USER DOCUMENTATION (ALEPHINO 5.0)

Single-Sign-On

The bridge to knowledge

Table of Contents

The Alephino WEB-Opac supports a simple Single-Sign-On, which the customer can use without a special configuration.

1 Mode of operation

If variable **REMOTE_USER** of HTTP-Header Code is equal to the patrons barcode or registration number the patron is signed on without asking about the password.
He has immediately access to his personal features.
But this is only available with Microsoft Browser "Internet Explorer" because of the proprietary protocol.
Other Browser needs a new sign on at the first invocation.

2 Windows domain user

The method allows to “carry” the already made proprietary Windows authentication to the web sites visited. As a result said REMOTE_USER is then occupied with the login name (prefixed with domain).
The first time "entering" a protected site with Internet Explorer, no separate authentication is required, however other browsers require on first call of the protected area a fresh Windows authentication and hence a login screen is displayed.
By editing parameter ***network.automatic-ntlm-auth.trusted-uris*** it is possible bringing Mozilla Firefox to a similar behaviour as known for Internet Explorer.
For this simply use URL ***about:config*** to enter the internal configuration dialog.
Search the aforementioned parameter and add the address of the OPAC to its value. When specifying multiple URLs they are to be separated by commas.

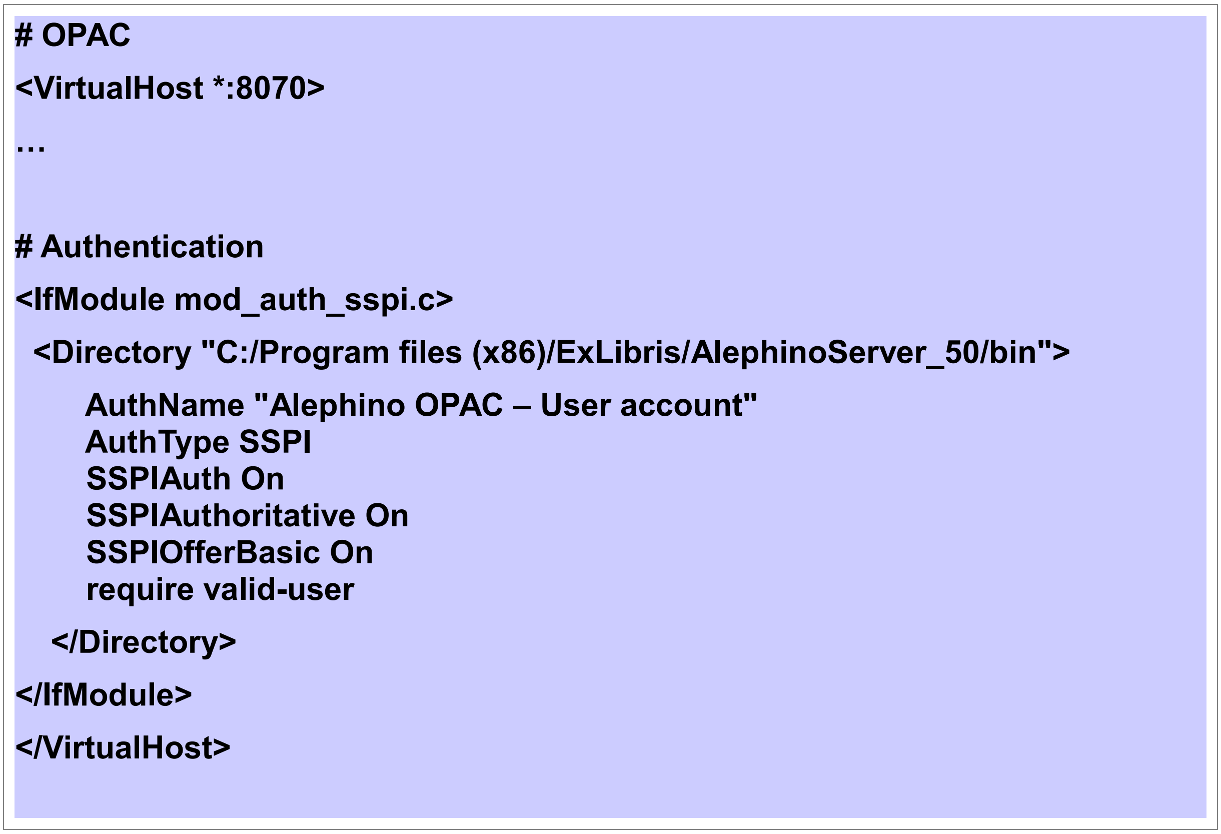
2.1 Configuration example for Apache http server

Using Apache http-Server you can implement it with REMOTE_USER and the module mod_auth_sspi

httpd.conf:

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so
```

vhost.alephino:



```
# OPAC
<VirtualHost *:8070>
…


# Authentication
<IfModule mod_auth_sspi.c>
  <Directory "C:/Program files (x86)/ExLibris/AlephinoServer_50/bin">
        AuthName "Alephino OPAC – User account"
        AuthType SSPI
        SSPIAuth On
        SSPIAuthoritative On
        SSPIOfferBasic On
        require valid-user
    </Directory>
</IfModule>
</VirtualHost>
```

3 Configuration for Microsoft Internet Information Server

The interaction between IIS and "Internet Explorer" allows it to "carry" the already made proprietary Windows authentication to the web sites visited a very simply way.

3.1 *IIS 6.0 (Windows Server 2003)*

With the configuration dialog choose options:

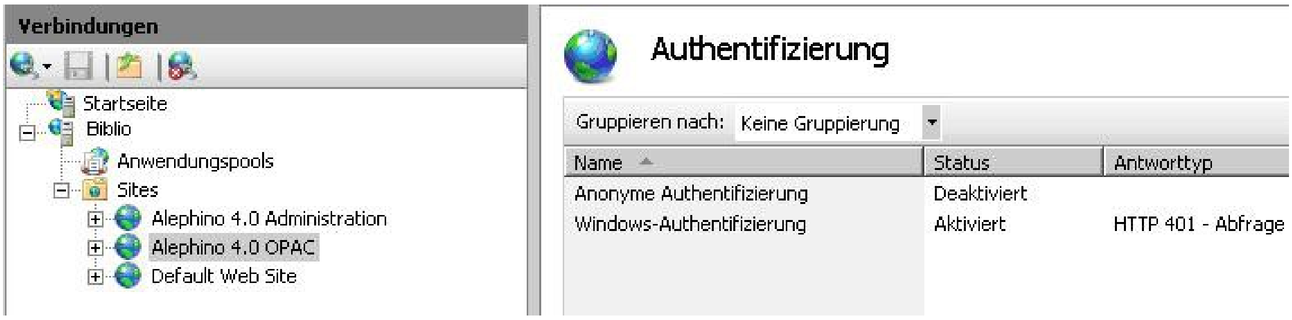
„Basic authentication“

and

„Enable Integrated Windows authentication“.

3.2 *IIS 7.0 (Windows Server 2008)*

Condition: Feature "Authentification" must be installed.
Choose Site **OPAC**, switch to Features and click on Authentification. Windows-Authentification must be activated.
(Anonymus Authentification must be deactivated).

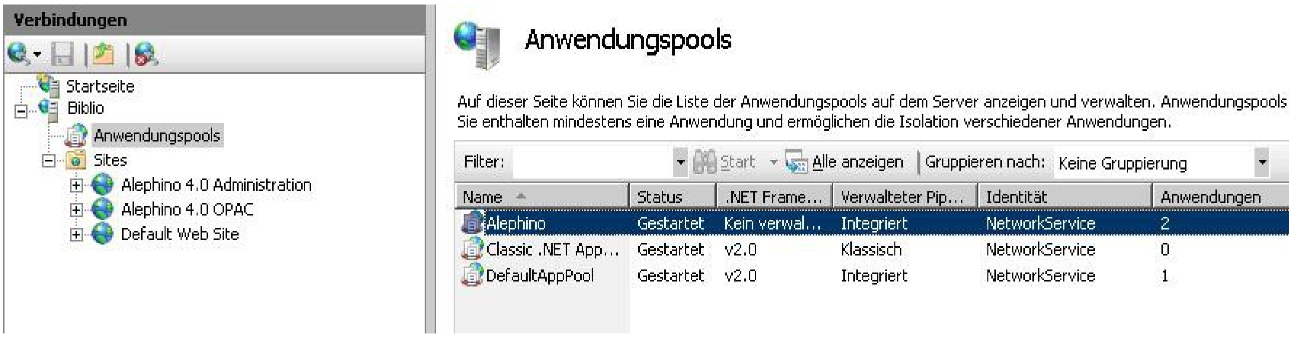


Authentifizierung

Gruppieren nach: Keine Gruppierung

Name	Status	Antworttyp
Anonyme Authentifizierung	Deaktiviert	
Windows-Authentifizierung	Aktiviert	HTTP 401 - Abfrage

Under **Application Pools > Advanced Settings > Process model** must be shown the identity „**NetworkService**“:



Anwendungspools

Auf dieser Seite können Sie die Liste der Anwendungspools auf dem Server anzeigen und verwalten. Anwendungspools Sie enthalten mindestens eine Anwendung und ermöglichen die Isolation verschiedener Anwendungen.

Filter: Start Alle anzeigen | Gruppieren nach: Keine Gruppierung

Name	Status	.NET Frame...	Verwalteter Pip...	Identität	Anwendungen
Alephino	Gestartet	Kein verwal...	Integriert	NetworkService	2
Classic .NET App...	Gestartet	v2.0	Klassisch	NetworkService	0
DefaultAppPool	Gestartet	v2.0	Integriert	NetworkService	1

3.3 SSO with Shibboleth

Shibboleth is a procedure for distributing authentification and authorization for WEB Application and WEB Services. The concept of Shibboleth is that Users has to authentificate himself once to use other services from different providers. The infrastructure is based on Security Assertion Markup Language (SAML).
http://en.wikipedia.org/wiki/Shibboleth_(Internet2)

In basic configuration Shibboleth can provide Authentication for REMOTE_USER.

httpd.conf:

```
LoadModule mod_shib /usr/lib/shibboleth/mod_shib_22.so

Alias /shibboleth-sp/main.css /usr/share/doc/shibboleth/main.css
Alias /shibboleth-sp/logo.jpg /usr/share/doc/shibboleth/logo.jpg
```

vhost.alephino:

```
# OPAC
<VirtualHost *:8070>
…
# Authentication
 <Directory "C:/Programme/ExLibris/AlephinoServer_50/bin">
     AuthName "Alephino OPAC – User area"
     AuthType shibboleth
     ShibRequireSession On
     require valid-user
  </Directory>
</VirtualHost>
```

3.4 SSO with LDAP

The Lightweight Directory Access Protocol is a data exchange protocol that allows the retrieval and modification of information. The communication between the LDAP directory service and each client is via the TCP / IP protocol.
The structure stated by the LDAP is called LDAP directory.
In order to enable authentication via LDAP the modules listed below need to be installed. Example: authentication against LDAP-compatible Windows directory service (Active Directory).

httpd.conf:

```
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
```

vhost.alephino:

```
<Directory "C:/Programme/ExLibris/AlephinoServer_50/bin" >

  AuthType Basic
  AuthName "Alephino OPAC – User area"
  AuthBasicProvider ldap
  AuthzLDAPAuthoritative off
  AuthLDAPURL ┐
ldap://myldapserver:389/ou=users,ou=Germany,dc=corp,dc=exlibrisgroup,
dc=com?sAMAccountName

  AuthLDAPBindDN "Harry Hurtig"
  AuthLDAPBindPassword "topsecret“
  AuthLDAPRemoteUserAttribute sAMAccountName
  Require valid-user

</Directory>
```

Notes:

- Since anonymous access to the directory service is usually not possible access data of a representative user must be stored for authentication of the query. For this purpose the directives AuthLDAPBindDN and AuthLDAPBindPassword have to be used.
- The sAMAccountName attribute of an AD directory service is typically identical to the Windows login name of the user. This will initially be used as an attribute element in the directive AuthLDAPURL. It is thus determined that this attribute must match the login name sent by the browser.
- The directive AuthLDAPRemoteUserAttribute ensures that the environment variable REMOTE_USER, as expected from Alephino, is occupied. In our case also with the login name of the user. If you want to use another attribute available in the directory service as REMOTE_USER, this must also be included in the (comma-separated) list of attributes in AuthLDAPURL.