Expert Services

Apache LDAP Authentication - Integration with Qlikview Accesspoint

Version:	2
Date:	2010-11-24
Author(s)	RVA
QV9, 10	

Contents

1 Introduction

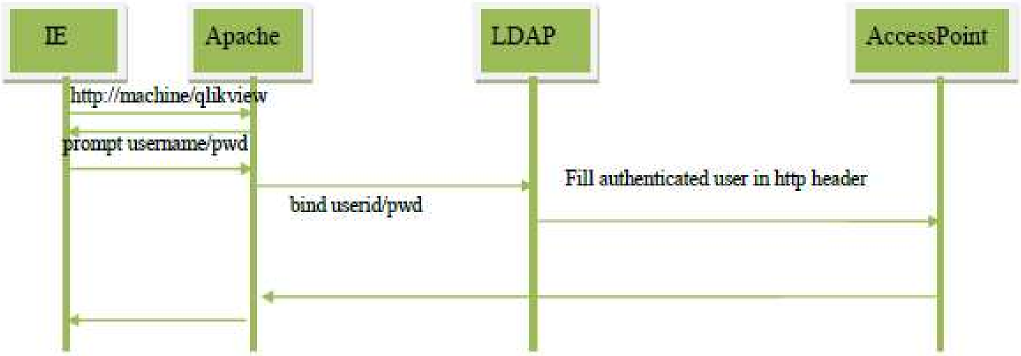
1.1 Background

Single Signon with “Non-Windows Integrated Security” systems into Qlikview Accesspoint requires that a “QVUSER” http header has been populated. Qlikview itself however is not responsible for configuring the WebServer to populate QVUSER field in any way. The customer must engage the WebServer Vendor to perform that integration.

Several Apache Modules are available that perform HTTP Basic Authentication. These cause the user to enter a Username and Password in a dialog window, which are then transmitted to the WebServer. The transmission of these credentials can only be protected if using SSL. Apache then typically validates the credentials against Flatfiles or LDAP.

This document describes two possible setups. First a Apache configuration is described using generic LDAP modules (mod_ldap) to do the authentication. The second approach describes how Oracles mod_osso can be used to configure Single Sign On with Qlikview Accesspoint.

While both scenarios have different technical implementation, the approach used from a Qlikview perspective is always the same, as shown in the figure below.



2 Setup Apache with mod_ldap

2.1 Configuration

Apache can do authentication with LDAP. However Apache’s authentication is only HTTP BASIC authentication. BASIC requires that the user send his username/password every request and that it is only BASE64 encoded, not encrypted. As this is not secure, in a productive environment Apache should use SSL for encryption.

The steps necessary to configure Apache with LDAP authentication and integration with Qlikview Accesspoint are:

1) Setup HTTP Authentication with BASIC.
2) Configure BASIC to use the LDAP server.
3) Setup a Reverse Proxy configuration for our URLs.
4) Block external access to our web server.
5) Configure the injection of the HTTP Header containing the name of the user.
6) (SSL configuration) << Not covered in this document

To configure Qlikview Accesspoint to read the http header field, please follow the instruction in the document “Qlikview Accesspoint SSO.pdf”.

After these steps the authenticated LDAP user is handed over to QV-Accesspoint. Then Qlikview Server, running in DMS-Mode, uses the authenticated LDAP user to authorize on Qlikview applications.

2.2 Httpd.config Example

On the following pages you find the httpd.config for this scenario. Please take notice of the comments for each configuration.

```
#Apache listens on 8081. The url a user types in their browser
is http://myserver:8081/qlikview. Our web server listens on
port 80 and we block in the firewall external access. We could
of course swap these ports.
Listen 8081


#BASIC authentication
LoadModule auth_basic_module modules/mod_auth_basic.so
#Works with mod_ldap to lookup attributes of the user in the
LDAP
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
#Maybe not needed. But we do need to add a header based on
environment variables so …
LoadModule env_module modules/mod_env.so
#To add the header
LoadModule headers_module modules/mod_headers.so
#Basic LDAP activities including binding with an admin account
and searching for a username.
LoadModule ldap_module modules/mod_ldap.so
#Basic proxy server functionality
LoadModule proxy_module modules/mod_proxy.so
#Proxy server for HTTP (Apache can also proxy ftp and Tomcat’s
AJP protocol)
LoadModule proxy_http_module modules/mod_proxy_http.so
#To set a header based on the existence of a variable
LoadModule setenvif_module modules/mod_setenvif.so


#This is not a Forward Proxy.
#This is important to have because a forward proxy can go to
any web server.
#If not there, it is easy to hijack this server to carry out
attachs on the internet.
ProxyRequests Off
#The static content of AccessPoint
ProxyPassMatch (?i)^/qlikview(.*)
http://localhost:80/qlikview$1
```

```
#The static content for AJAX client and Dynamic AJAX, AccessPoint, GetTicket, DocList, AccessPointSettings and QvsStatus pages (V10)
ProxyPassMatch (?i)^/qvajaxzfc(.*) http://localhost:80/qvajaxzfc$1
#The static content for Plugin client
ProxyPassMatch (?i)^/qvplugin(.*) http://localhost:80/qvplugin$1
#There is also /QvClients/settings.js for Plugin without AccessPoint but we don’t care for this client
#There is also /QvPrint for v9 AJAX Export to Excel etc.

#Shouldn't be any redirects except from /qlikview to /qlikview/index.htm but here anyway
ProxyPassReverse /qlikview http://localhost:80/qlikview
ProxyPassReverse /qvajaxzfc http://localhost:80/qvajaxzfc
ProxyPassReverse /qvplugin http://localhost:80/qvplugin

#This is v10. In V9 it is /QvAJAXZfc/AccessPoint.aspx at least
<Location /QvAJAXZfc/Authenticate.aspx>
#Authentication based on BASIC
AuthType basic
#Tell browser the realm is “test” so it remembers the password based on the URL space and realm
AuthName "test"
#Tell Apache to use LDAP to verify the username/password
AuthBasicProvider ldap
#The user ID in the LDAP is uid
AuthLDAPRemoteUserAttribute uid
#We first bind as an admin and search for the LDAP node for the user. If found we disconnect and rebind using his password. So this is the admin DN
AuthLDAPBindDN uid=admin,ou=system
#This is the admin Password
AuthLDAPBindPassword secret
#This is the URL to find the LDAP server and also to determine what attributes are returned from searches
AuthLDAPURL "ldap://localhost:10389/ou=system?uid"
```

```
#Authorization – we let them through if we found a valid user. We could have other rules here
Require valid-user
</Location>

#Pass the user’s ID to AccessPoint in the QVUSER variable
RequestHeader add QVUSER "%{AUTHENTICATE_uid}e"
```

3 Apache with Oracle SSO mod_osso

To integrate Qlikview Accesspoint with Oracle SSO the module mod_osso needs to be configured. The following chapter describes a possible configuration.

3.1 Apache Configuration

3.1.1 Reverse proxy configuration

In order to access Qlikview from a separate Apache, add the following in the Apache config. All endusers will communicate through the reverse proxy Apache with the Qlikview Server. This can be simplified if using `ProxyPassMatch` as shown in Chapter 2.

```
ProxyPass /qlikview/ http://swXXXXX/qlikview/
ProxyPass /qlikview http://swXXXXX/qlikview/
ProxyPass /QvPrint/ http://swXXXXX/QvPrint/
ProxyPass /QvAjaxZfc/ http://swXXXXX/QvAjaxZfc/
ProxyPass /QvAJAXZfc/ http://swXXXXX/QvAJAXZfc/
ProxyPassReverse /qlikview/ http://swXXXXX/qlikview
ProxyPassReverse /qlikview http://swXXXXX/qlikview
ProxyPassReverse /QvAjaxZfc/ http://swXXXXX/QvAjaxZfc
ProxyPassReverse /QvAJAXZfc/ http://swXXXXX/QvAJAXZfc
ProxyPassReverse /QvPrint/ http://swXXXXX/QvPrint
```

The proxy pass for the QvAjaxZfc is entered twice due to case sensitivity issues in Qlikview 9.

3.1.2 Oracle SingleSignOn mod_osso configuration

To secure the Qlikview Server with SSO enter the following in the mod_osso.config. Whenever an enduser tries to access Qlikview Accesspoint, the user is redirected to the Oracle SSO page if not authenticated already.

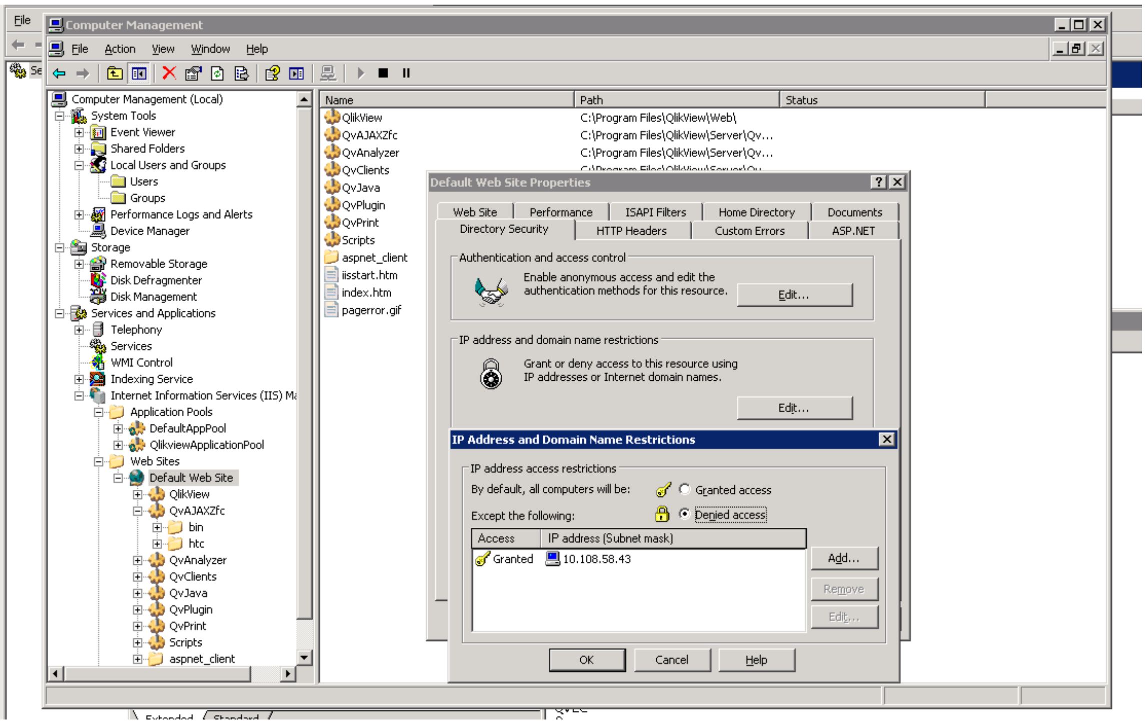
```
<Location /qlikview>
    require valid-user
    AuthType Basic
</Location>
<Location /qlikview*>
    require valid-user
    AuthType Basic
</Location>

<Location /QvAJAXZfc>
    require valid-user
    AuthType Basic
</Location>
<Location /QvAJAXZfc*>
    require valid-user
    AuthType Basic
</Location>
<Location /QvAjaxZfc>
    require valid-user
    AuthType Basic
</Location>
<Location /QvAjaxZfc*>
    require valid-user
    AuthType Basic
</Location>
```

The entry for QvAjaxZfc is again entered twice due to case sensitivity.

3.2 IIS IP Restriction

As IIS hosting the Qlikview Accesspoint should only be reachable from the Reverse Proxy, add a IPRestriction that only grants access via your Reverse Proxy.



Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

IP Address and Domain Name Restrictions

IP address access restrictions

By default, all computers will be: ○ Granted access ● Denied access

Except the following:

Access	IP address (Subnet mask)
Granted	10.108.58.43

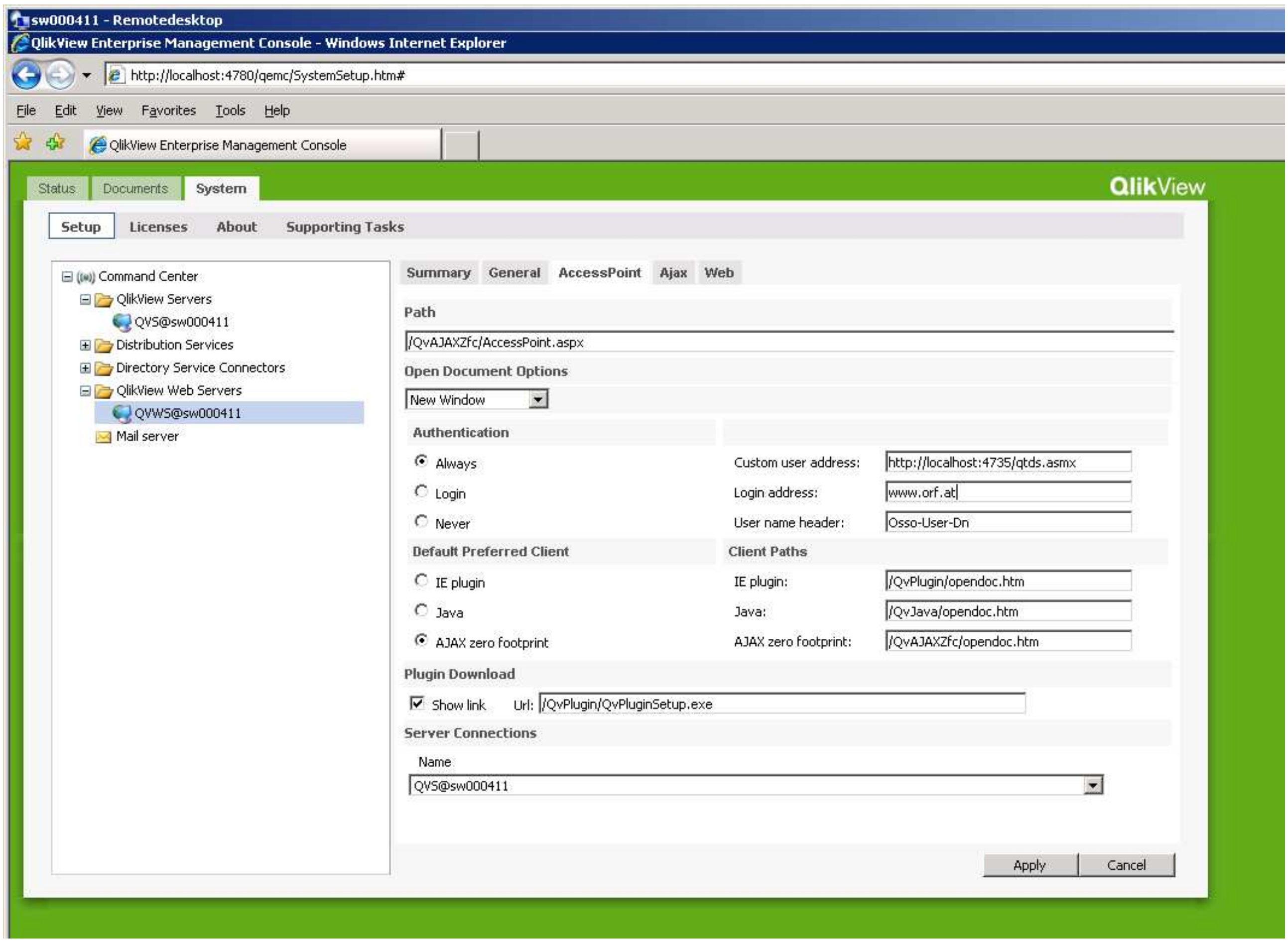
3.3 Accesspoint Configuration

To use Oracle SingleSignOn the Qlikview Accesspoint needs to retrieve the authenticated username from the OSSO HTTP Header field “Osso-User-Dn”.

Authenticate: Always

User name header: Define the HTTP Header field name. We used “Osso-User-DN” from Oracle SSO. Other fields tested: “Osso-User-Guid” returns a hexstring GUID for the user.

Login address: redirect if HTTP Header is not presented to Qlikview Accesspoint. This should be the SSO login page in the productive environment.


sw000411 - Remotedesktop
QlikView Enterprise Management Console - Windows Internet Explorer
http://localhost:4780/qemc/SystemSetup.htm#
File Edit View Favorites Tools Help
QlikView Enterprise Management Console
Status Documents System
QlikView
Setup Licenses About Supporting Tasks
Command Center
QlikView Servers
QVS@sw000411
Distribution Services
Directory Service Connectors
QlikView Web Servers
QVWS@sw000411
Mail server
Summary General AccessPoint Ajax Web
Apply Cancel

Path: /QvAJAXZfc/AccessPoint.aspx

Open Document Options: New Window

Authentication

● Always
○ Login
○ Never

Custom user address: http://localhost:4735/qtds.asmx
Login address: www.orf.at
User name header: Osso-User-Dn

Default Preferred Client

○ IE plugin
○ Java
● AJAX zero footprint

Client Paths

IE plugin: /QvPlugin/opendoc.htm
Java: /QvJava/opendoc.htm
AJAX zero footprint: /QvAJAXZfc/opendoc.htm

Plugin Download

☑ Show link Url: /QvPlugin/QvPluginSetup.exe

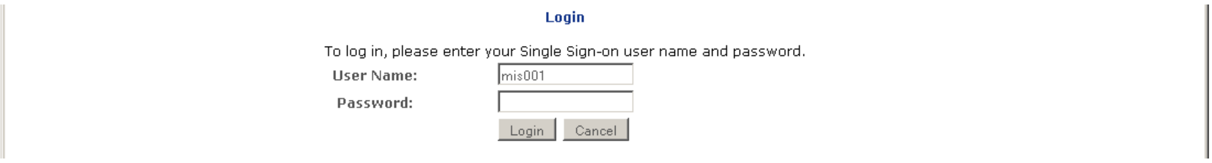
Server Connections

Name: QVS@sw000411

3.4 Enduser walkthrough

To access Qlikview Accesspoint enter the URL https://swXXXXX:4443/qlikview

The user will then be redirected to the Oracle Single Sign on Login Page



Login

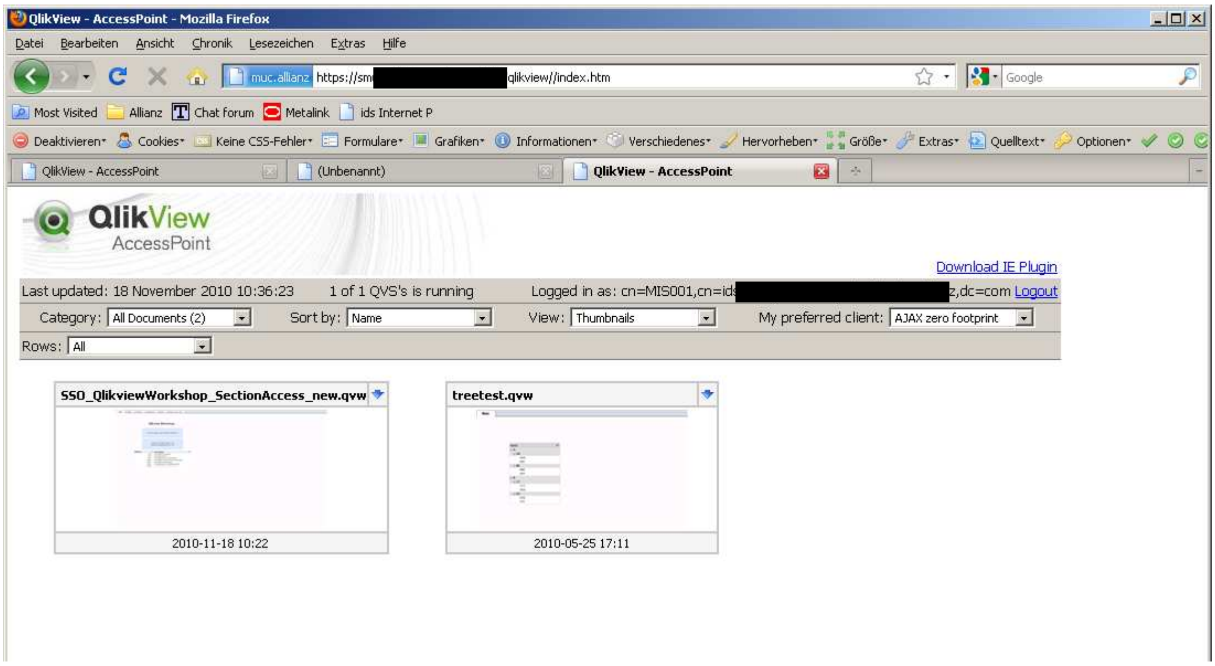
To log in, please enter your Single Sign-on user name and password.

User Name: mis001

Password:

Enter the password as normal and the user will be redirected to the Accesspoint page of Qlikview with a list of accessible applications (they were enabled for the user in the QEMC).

The username is also displayed as Logged in. The Accesspoint will show the unique name of the user in the LDAP directory as provided by Oracle Single Sign On.



QlikView - AccessPoint - Mozilla Firefox

muc.allianz https://sm[redacted]qlikview/index.htm

Last updated: 18 November 2010 10:36:23 1 of 1 QVS's is running Logged in as: cn=MIS001,cn=ids[redacted]z,dc=com Logout

Category: All Documents (2) Sort by: Name View: Thumbnails My preferred client: AJAX zero footprint

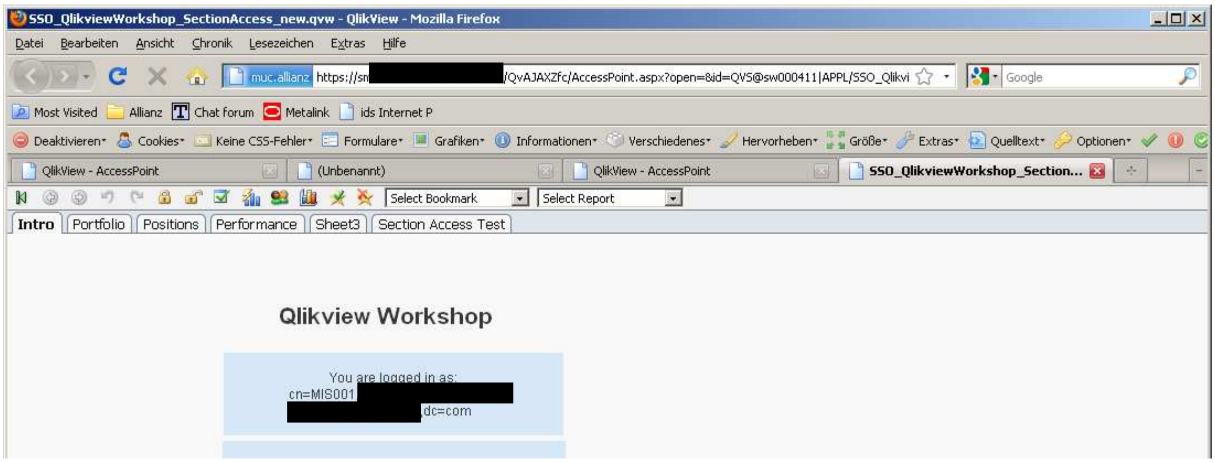
Rows: All

SSO_QlikviewWorkshop_SectionAccess_new.qvw 2010-11-18 10:22

treetest.qvw 2010-05-25 17:11

When the user clicks on the first application for example, they are taken into the application without being asked for an additional login as the user who has authenticated in the SSO is handed over to the application and the repository. This is done by using the Osso-User-Dn HTTP Header field delivered from the Oracle SSO and configured in Qlikview.

Qlikview Section access restricts the user MIS001 to only see limited data!


SSO_QlikviewWorkshop_SectionAccess_new.qvw - QlikView - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
muc.allianz
Google
Most Visited Allianz Chat forum Metalink ids Internet P
Deaktivieren Cookies Keine CSS-Fehler Formulare Grafiken Informationen Verschiedenes Hervorheben Größe Extras Quelltext Optionen
QlikView - AccessPoint
(Unbenannt)
QlikView - AccessPoint
SSO_QlikviewWorkshop_Section...
Select Bookmark
Select Report
Intro Portfolio Positions Performance Sheet3 Section Access Test

https://sm[redacted]/QvAJAXZfc/AccessPoint.aspx?open=&id=QVS@sw000411|APPL/SSO_Qlikvi

Qlikview Workshop

You are logged in as:
cn=MIS001 [redacted] dc=com