507 Demystifying Authentication and SSO Options in Business Intelligence

Greg Wcislo
• We will not go into detailed how-to, however links to multiple how-to whitepapers will be provided.

• Some familiarity with general SAP Business Intelligence suite will be assumed.
This is the majority of report consumption, using either the BI Portal, or direct document access using OpenDoc.

- The following major logon methods are supported, with various methods of SSO:
  - Windows AD
    - SSO achieved through Kerberos, using Quest Vintela plugin.
    - Web application server can run on any platform, however the Central Management server MUST be on a windows system.
  - LDAP
    - SSO is supported with integration through CA Siteminder
  - SAP
    - SSO achieved by configuring SAP SSO tickets.
  - Enterprise
    - Native BI authentication model. SSO can be achieved through ‘Trusted Authentication’.
Involves the following steps

- Setup system account on Domain controller
- Configure the CMC
- Modify SIA

- Modify krb5.ini and bscLogon.conf files
- Modify global.properties, BIIlaunchpad.properties, OpenDocument.
  - make sure this is done in “Custom” folder, so settings are not removed in patch
- Modify your application server settings to reference krb5.ini, bscLogon.conf

- AD SSO to BI makes it possible to SSO all the way down to database*

See https://websmp230.sap-ag.de/sap/support/notes/1631734 for how-to whitepaper
AD SSO into the BI portal, or manually logging in with AD username & password allows for SSO to database, however there are a few limitations to keep in mind:

1) Scheduling a report will not carry forward the Kerberos ticket (no SSO), even if you choose to ‘schedule now’.

2) It is not possible to setup Kerberos SSO for offline scheduling.

3) The CMS and processing servers must be on Windows

View time refresh will perform AD SSO.
- LDAP SSO can be attained using Siteminder
- Incoming ‘ticket’ from Siteminder cannot be used for any further SSO to database, front door entry only
  - Secondary Credentials or mix with SAP SSO methods for data access
- Integrate BI content into SAP NetWeaver Enterprise Portal

- Configure SAP authentication in CMC

- **Configure properties files**

```
[siteminder properties - WordPad]

siteminder.enabled=false
# Set to true to enable other single sign on.
sso.enabled=true

[bilaunchpad.properties - WordPad]

# You can specify the default Authentication types here.
secEnterprise, secIDP2, secWinAD, secSAPR3
authentication.default=secSAPR3

[OpenDocument.properties - WordPad]

# You can specify the default Authentication types here.
secEnterprise, secIDP2, secWinAD, secSAPR3
authentication.default=secSAPR3
```

*SSO can be configured right down to BW data source*
Setting up web services SSO for Windows Active Directory is required to enabled SSO for the following clients:

- LiveOffice
- Query as a Web Services
- BI Widgets
- Crystal Reports for Enterprise
- Dashboard Designer

Setup is similar to configuring BI Launchpad, see SAP note 1646920
- With BI’s native Enterprise authentication, it is possible to enable trusted authentication.

- With “Trusted” authentication, BI is TRUSTING underlying application server to perform the authentication.

- The application server passes a shared secret, and a user ID to BI. If the user ID exists in the BI system, a logon session for that user is created.

- This allows most other authentication methods to be used to logon to BI, such as X.509, SAML, SecureID, SAP Netweaver SSO etc.
Configuring Trusted Authentication

You must secure the web application - `webapps\BOE\WEB-INF\web.xml`:

```xml
Add the follow entry before </web-app>:
<security-constraint>
  <web-resource-collection>
    <web-resource-name>OnJava Application</web-resource-name>
    <url-pattern>/</url-pattern>
  </web-resource-collection>
</security-constraint>
```

A number of ways to pass user information in trusted authentication:
- Web Session
- HTTP Header
- URL Query
- User Principal (new method using JAAS authentication)
- Remote User (new method using JAAS authentication)
- Cookies *not recommended, supported for legacy

Modify `global.properties`:

- `sso.enabled=true`
- `trusted.auth.user.retrieval=USER_PRINCIPAL`
- `trusted.auth.user.namespace.enabled=true` (optional if you want to map external user name to a different BOE user name)

It is possible to bind a different incoming user id to an existing user in the BI system using `trusted.auth.user.namespace.enabled`.

Example: User “gregw” exists in BI, user “gregwcislo” authenticates to web app server.
What if I have more than 1 method of SSO?

- Q: Can I have some users doing SSO with AD and others with SAP?
- A: No. The BI web application can only be setup for one at a time.
- Workaround: You can setup multiple web application servers and direct the users appropriately.
Review the Clients

Visualize data for better decision making
Answer ad hoc questions and interact with information
Determine trends from complex historical data and make possible better forecasts
Find immediate answers to business questions

Crystal Reports
Dashboards
Web Intelligence
OLAP Analysis
Explorer

Access and transform corporate data into highly formatted reports for greater insight
New Semantic Layer Connectivity (.unx)

Kerberos SSO – CMS Must be on Windows.
MS SQL Server
Oracle DB
SAP HANA

Security Token Service (STS)
SAP BW

Applicable to the following clients:
Crystal Reports for Enterprise
Web Intelligence
Dashboards
Explorer
OLAP Analysis
Legacy Semantic Layer (.unv)

- **Kerberos SSO** – CMS Must be on Windows.
  - MS SQL Server
  - Oracle DB

- **Server SNC**
  - SAP BW

- **Stored User credentials**
  - all other databases

- Applicable to the following clients:
  - Crystal Reports 2011
  - Web Intelligence
Both are exposed in the CMC. The new STS method is available under the options tab. STS is generally used by newer BI clients.

Server SNC – available as it was in xir3, used by .unv
More about STS

- It is based on trust, between the BW server and the BI system
- Requests processed by BI’s Adaptive Processing Server
- You can configure multiple SAP systems for access in BI. Based on the system that a connection is established to, an SSO ticket will be automatically generated by the BI system.

Security Consideration

- Beware that the system is based on trust. The BI Administrator can technically assign any BW account without requiring the password to that account and query data.
  - More on this in the user aliasing section.
Using STS versus SNC

Both methods can coexist in the BI system.

<table>
<thead>
<tr>
<th></th>
<th>NONE</th>
<th>SNC</th>
<th>STS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBI UNV SSO</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEBI UNX SSO</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>WEBI BICS SSO</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>PORTAL SSO</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>CR 2011</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>SAP LOGINS</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>IDT</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>BO MOBILE</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>CR FOR ENTERPRISE</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>HARDCODED USER</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Yes, you can setup multiple SAP systems. Valuable note: Refer to user aliasing slides later in presentation.
- Mobile is currently username & password only.
- The username & password can be saved locally on the device.
If you are running BI4 on Windows:

- Setup Windows SSO to BI Portal, or manually logon using AD credentials
- SSO at view time using Exploration view, Semantic Layer (Web Intelligence, Crystal Reports), OLAP Analysis.
- Still no scheduling SSO using Kerberos – but it is FAST so why schedule? 😊

- If you are running on Linux:
  - Configure LDAP connectivity for MS AD
  - Enable Kerberos authentication from your LDAP authentication plugin.
  - Manual logon, then SSO to database possible.

Any platform, all clients:

- Setup user database credentials Direct DB authentication, exposed through CMC
- Can be scripted
New option to configure HANA SSO

- Accessible under Applications, “HANA Authentication”
- Based on trust configured between BI and HANA
- Less work to setup than kerberos
- User ID’s must match between HANA & BI system
- Works with any type of authentication to BOE: Enterprise, AD, LDAP, SAP, and supports all platforms.
- Based on system trust. HANA trusts BI to do the authentication. Once a user is authenticated to BI, BI creates SAML assertions on behalf of users to pass to HANA for SSO
- Dashboard Designer and A-Office ETA SPI
- Enter HANA server details
- Generate a certificate on the BI side to import into the HANA server. (copy & paste)
- Once both systems are setup, user can test connection from CMC directly to validate setup.
Tips: Validate your certificate online

- http://www.redkestrel.co.uk/cgi/decodeCert.cgi is just one sample online tool.
- Format should look something like this

Validate your format by using HANA UI:
After configuring BI, HANA side is next

- Using the HANA Studio run this SQL command to enabled BOE as the id provider. The SUBJECT and ISSUER can be seen in the previous screen.

```
CREATE SAML PROVIDER GREGMBOE WITH SUBJECT 'C=CA, ST=BC, O=SAP, OU=BOE, CN=GREGMBOE' ISSUER 'C=CA, ST=BC, O=SAP, OU=BOE, CN=GREGMBOE'
```

- “CN=GREGMBOE” is the id entered in the CMC (can also be done via UI)

- Configuration on HANA requires to import certificate generated in the CMC into the ..ssl/trust.pem file on the HANA server.

- HANA side users must be granted rights to be impersonated via SAML
SAP Business Objects and SAP HANA support identity forwarding for scenarios where authorization enforcement in SAP HANA is required.

User authenticates against BOE server with one of the mechanisms supported by BOE.

1. BOE securely forwards the user identity to SAP HANA with one of the following methods:
   - **User name/password**
     - SAP HANA database user name/password stored in BOE server
     - Manual synchronization
   - **Kerberos** (As of SP4)
     - Users must log on to BOE server using Active Directory authentication
     - BOE server must run on Linux or Microsoft Windows
   - **Trust (SAML) NEW with 4.1**
     - BOE server acts as identity provider
     - BOE server generates SAML ticket for the user, sends it to the SAP HANA database to validate -> if valid session will be established for this user
       - Protocol (SAML) is irrelevant here. Just think of trust between systems.
     - Using SSL transport security between BOE and HANA is highly recommended
Reporting on HANA Client and connectivity options using Kerberos SSO

- Crystal Reports for Enterprise
- Dashboards
- Web Intelligence
- Semantic Layer (relational universe UNX)
- Explorer
- JDBC
- ODBC

SAP HANA Database
## HANA SSO overview

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Internal (Direct)</th>
<th>External (Kerberos Delegated)</th>
<th>TRUST (SAML) (4.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explorer</td>
<td>Y</td>
<td>Y (I)</td>
<td>Y</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Y</td>
<td>Y (I)</td>
<td>Y</td>
</tr>
<tr>
<td>Web Intelligence</td>
<td>Y</td>
<td>Y (I)</td>
<td>Y</td>
</tr>
<tr>
<td>Crystal Reports 2011</td>
<td>Y</td>
<td>Y (I)</td>
<td>Y</td>
</tr>
<tr>
<td>Crystal Reports for Enterprise</td>
<td>Y</td>
<td>Y (I)</td>
<td>Y</td>
</tr>
<tr>
<td>Analysis, Edition for Office</td>
<td>Y</td>
<td>Y (I)</td>
<td>Y</td>
</tr>
<tr>
<td>Analysis, Edition for OLAP</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

(1) Support on Linux and Windows platforms only
## Security

<table>
<thead>
<tr>
<th>Client</th>
<th>Crystal Reports</th>
<th>Web Intelligence</th>
<th>SBOP Dashboards</th>
<th>Design Studio</th>
<th>Analysis, edition for Microsoft Office</th>
<th>Analysis, edition for OLAP</th>
<th>SBOP Explorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Yes (1)</td>
<td>Yes (3)</td>
<td>Yes (3)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes (3)</td>
</tr>
<tr>
<td>SAML</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secured Connection (SSL)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

(1) Crystal Reports for Enterprise via a Universe (UNX)  
(2) Crystal Reports 2011 only  
(3) Support on Linux and Windows platforms only

### More Information
Storing User Credentials

- It is possible to save database credentials to use for “SSO”, using the database’s native authentication.

- These can be automatically captured if user manually logs on through a configuration option in the authentication plugin.
It is possible to match aliases from various identity providers, to a single user profile. For example, matching an AD + SAP account, to provide AD SSO to BI, and BW SSO data.
More on user Aliasing

- But there is an easier way to match SAP & AD accounts

Registry key will allow you to strip out the SAP system name, and automatically match user based on user ID alone:

```
HKLM\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\Enterprise\Auth\Plugins\secSAPR3\SimpleUsernameFormat
"SimpleUsernameFormat" = "Yes"
```

This method requires planning of SAP and AD users. User IDs have to be identical in SAP and AD.
The SAP alias SID~CLNT/USER01 and AD alias DOMAIN\USER01 will be automatically mapped to the matching BO USER01 when SAP user ID and AD user ID are identical.
Web Intelligence – review your options

Reporting from SQL Server, Oracle DB
- Kerberos SSO (windows only)
- Saved Credentials (all platforms)
- Predefined credentials (shared user) – (all platforms)

Reporting from HANA
- Kerberos SSO (windows/linux only, using
- Saved Credentials (all platforms)
- Predefined credentials (shared user) – (all platforms)

Reporting from SAP BW
- STS (all platforms – .unx)
- SNC (all platforms – .unv)
- Saved credentials
  - if logging onto BI with SAP credentials, these can be used for view time refresh (SSO)
Analysis Office options

Reporting from Microsoft Analysis Services
- Kerberos SSO (windows only) – requires user to logon manually using AD or to have SSO set up.
- Saved Credentials (all platforms)
- Predefined credentials (shared user) – (all platforms)

https://websmp230.sap-ag.de/sap/support/notes/1688079

Reporting from SAP BW
- STS (all platforms)
Sample SAP authentication workflow

- Logon to BI Launchpad using SAP authentication

  *Enter your user information, and click "Log On".*
  If you are unsure of your account information, contact your system administrator.

  - System: AUTOCHAIN-VM18:6400
  - SAP System: r79
  - SAP Client: 800
  - User Name: user1
  - Password: ********

- Access a report containing data for an SAP system
  - Even if you have not configured SNC or STS, the saved credentials for the duration of this session will be used to access data
KEY LEARNINGS

• How to use SAP authentication with other authentication methods

• Understand what is possible for Single Sign On based on your environment.

• Understand HANA integration options
Follow @ASUG365 and ASUG CEO Bridgette Chambers @BChambersASUG on Twitter to keep up to date with everything at ASUG.

Follow the ASUGNews team of Tom Wailgum: @twailgum and Courtney Bjorlin: @cbjorlin for all things SAP.
THANK YOU FOR PARTICIPATING

Please provide feedback on this session by completing a short survey via the event mobile application.

SESSION CODE: 0310

For ongoing education on this area of focus, visit www.ASUG.com
Learning Points

- List 1-3 key points that attendees will take away from your session.
Return on Investment

- If applicable, highlight any aspect of your presentation that can contribute to a significant ROI. Omit slide from presentation if necessary.
Best Practices

- List 1 or more practices that can be obtained specific to your topic area.
Key Learnings

- Highlight/summarize 3-5 key learning points from your presentation
Thank you for participating.

Please provide feedback on this session by completing a short survey via the event mobile application.

507:

Learn more year-round at www.asug.com