The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Agenda

• Authentication and Authorization for BI 11g
• Architecture Overview
• Supported Configurations
• Authentication Mechanisms with and without SSO
• System Users and the Credential Store
• Troubleshooting and Logging
• Types of Security
Authentication and Authorization for BI EE 11g

For the purposes of comparing the approaches to authentication and authorization:

- Think of Authentication as the process of validating the userID and password and consequently setting the USER session variable in the BI EE session.

- Think of Authorization as the process of discovering the groups that the user is a member of, and then deriving which Application Roles (and associated permissions) the user should be granted. This results in setting the ROLES session variable in the BI EE Session. Refer to the slide ‘GROUP and ROLES Session Variables’
Authentication and Authorization for BI EE 11g

At a high level, there are two approaches to authentication and authorization into BI EE 11g.

- Firstly, new in 11.1.1.3, we integrated BI into Fusion Middleware and now make use of the Fusion Middleware security mechanisms built on the FMW security infrastructure (OPSS).
  - Authentication is via OPSS which in turn uses the Weblogic authentication mechanism (Authenticators defined in the Weblogic Security Realm). The resulting authenticated userID is used to set the USER session variable.
  - Authorization is via OPSS to retrieve group membership via Weblogic Authenticators. This works together with the Policy Store to derive a list of Application Roles for the user and the groups assigned to that user. This list of Application Roles is used to set the ROLES session variable.

- Secondly, the 10-g style Init Block mechanism for authentication and authorization is still available.
  - Authentication is via an Init Block that sets the USER session variable
  - Authorization is via an Init Block that sets the GROUP (or ROLES) session variable
Advice for customers on which Authentication and Authorization Mechanism to use

- Customers should not mix the two approaches. i.e. they should not attempt to authenticate users using FMW security and authorize users using Init Blocks.

- Not all use cases are currently supported by FMW security. Until such time that FMW security is able to support a particular use case, customers should continue to use the 10g-style Init Block approach for authentication and authorization.

- If you use FMW security in BI 11g then both users and group membership should be available via one or more BI EE certified Authenticators defined in WLS.

- FMW security in BI 11g is limited to BI EE certified WLS authenticators that work with the User Role API.
Upgrading from 10g and Backwards Compatibility

About the introduction of FMW Security to BI and Backwards compatibility of other authentication mechanisms:

• When introducing FMW security into BI, the aim was to provide as smooth an upgrade path, and as seamless backward compatibility, as possible.

• 10g systems built on init blocks should continue to work in the same way when upgraded to 11g.

About upgrading from 10g to 11g:

• If you upgrade 10g RPD users, they become Weblogic LDAP users in 11g (i.e. using FMW Security) so we no longer have RPD users. In this case, users and group membership for those users will be defined and maintained in the embedded Weblogic LDAP.

• On upgrade, all RPD groups are migrated to LDAP groups in the native Weblogic LDAP.

• Additionally, on upgrade, all RPD groups used to secure elements of the RPD are migrated to Application Roles in the file-based Policy Store.

• On upgrade, any element in the RPD that was secured by an RPD group will become secured by the Application Role with the same name (created during the upgrade process).

• The upgrade process does not do anything with Web Groups. Web Groups continue to exist in 11g, but customers are encouraged to replace them with Application Roles.
Use Case – Users in LDAP and Group Membership in Database – FMW Security or Init Block for Authentication?

• The most common use case for BI customers is to authenticate users in LDAP with group membership coming from a database query.

• If you have users in LDAP and Group Membership for those users defined in a database table, for BI EE 11.1.1.3.0, you should use Init Blocks to authenticate and authorize users. This approach has known issues when using BI Publisher.

• For BI 11.1.1.5.0, a FMW security solution for this use case is available via a patch (ARU 14523400). This solution involves an additional Authenticator that will allow authentication against LDAP and authorization (retrieving Groups) from a database. This is the best-practice approach for authentication against LDAP and authorization using SQL.

• The documented approach for integration with E-Business Suite continues to be based on Init Block authentication for BI EE 11.1.1.5.0.

• Security integration for BI Applications should follow the approaches in the BI Applications documentation.
Use Case – Security Integration with E-Business Suite

11g Customers can use one of the following approaches to secure their BI EE system when sourcing data from E-Business Suite

- Direct E-Business Suite to BI EE security integration using the ICX cookie method as described in the BI EE Integrator’s Guide
  - This is the only method able to secure data using the current responsibility of the user
  - This is the only method that allows Action Links back to E-Business Suite
  - This approach has known limitations with Delivers due to the integration with EBS Responsibilities
  - This approach has known issues with BI Publisher as this approach does not allow BI Publisher to impersonate a user
  - This approach does not work with BI Office or BI Mobile

- Shared Identity Store with E-Business Suite
  - If E-Business Suite is integrated with OID (and optionally OSSO), then BI EE can point to the same OID either via FMW security or via Init Blocks.
  - Init Blocks should not rely on the availability of an ICX cookie for the user

- Independent Identity Stores for BI and EBS
  - Some customers have a separate login for BI and maintain the EBS and BI user populations independently.
  - Init Blocks should not rely on the availability of an ICX cookie for the user

- Other approaches may be possible
Use Case – Browser SSO integration between BIEE and Hyperion EPM

• In BI 11.1.1.7.0 there is new functionality to embed BI into Workspace installed with EPM. This involves configuring BI to accept a CSS token as an SSO token through the browser. BI uses this to assert the user by validating the token against the version of the EPM Registry hosted by BI.

• BI still looks up the group, roles and permissions for the user against FMW security - not HSS. So it is not possible to point this to HSS Native groups.

• It is possible to point BI and EPM's HSS to the same (certified) LDAP. This functionality is documented in the Sys Admin guide.
Use Case – Authentication and Authorization integration between BIEE and Hyperion EPM

• It is not possible to point BI directly to a Hyperion EPM hosted HSS for authentication (setting/authenticating the User) or authorization (getting group membership).

• For authentication into BIEE if you want to use the same credentials as signing in to Hyperion products backed by HSS, you can either put a full SSO product (e.g. OAM) over the two systems, or you can point HSS and BIEE to the same Identity Store (usually LDAP) so both HSS and BIEE are actually authenticating against the same place.

• For authorization in BIEE, you can use the groups from the same external Identity Store (normally LDAP) used by HSS if there is one, but you cannot use the *native* groups from HSS. If this is a requirement, you will need to export or add these native HSS group memberships to a BI-certified Identity Store (e.g. database table using the BI SQL Group Provider). Oracle BI does not provide any specific functionality to perform this export and import.
Use Case – Security Integration with an Essbase data source

- Oracle Business Intelligence, includes functionality to generate a Hyperion (CSS) identity token that allows Oracle Business Intelligence Server to connect to Essbase data sources (both Essbase installed with Oracle Business Intelligence and Essbase installed with EPM) with the credentials of the end user. This approach is documented in the BI documentation.
- For this approach to be used, the Fusion Middleware approach to authentication and authorization needs to be used in BIEE.
- Since the CSS token is created based on the UserID for the BIEE user, this approach is designed to work when BIEE and Essbase/HSS are configured against the same underlying Identity Store (usually LDAP).
- Only specific versions of Essbase have been certified with this approach.
- It is necessary to synchronize the shared secret in BIEE that allows the BI Server to create the CSS token with the same shared secret in the EPM Registry.
- The CSS token is used by the BI Server to connect to Essbase and the connection will apply the appropriate filters for the user with the same name provisioned with filters in HSS.
- This functionality is independent of any front-end SSO solution. For example, an SSO solution based on OAM (or similar) can be used with any BI-certified authenticator to log in. Subsequently, when the user queries the Essbase data source, the BI Server connection pool can be configured to generate a CSS token for the end user.
Additional Information on Security Integration with Essbase data source hosted by BIEE

• There is new functionality in BI 11.1.1.7 where Essbase and related components can be installed with BI. In this case, these components use FMW security for authentication and authorization. These components cannot point to HSS when installed with BI.

• Essbase components installed using the Oracle Business Intelligence installer cannot use Native Essbase or Hyperion Shared Services (HSS) security. However, when you install Essbase with Oracle Business Intelligence, the Common Security Service (CSS) token-based identity assertion continues to be available and allows Oracle Business Intelligence to connect to the Essbase data sources installed with Oracle Business Intelligence with the credentials of the end user.

• HSS and CSS are not the same thing. BI does not install HSS so BI cannot use the HSS front-end to manage and provision security. However, BI does make use of CSS tokens for some elements of security when integrating with Essbase and related components.
Use Case – Custom SSO using a http Header or Cookie (Overview)

- There are currently two possible approaches for custom SSO solutions based on a http header or cookie that contains the UserID of the authenticated user.

- In both cases, make sure you are confident that the entry points into BI are adequately protected. Also ensure that the http header or cookie is secure so that tampering is not possible. Custom SSO implies and assumes that some form of SSO is protecting these resources, (i.e. BI does not protect the resources or the tokens). It is up to the custom SSO solution to protect the header or cookie and the resources. BIEE will just trust that the header or cookie contains the UserID of the authenticated user.
Use Case – Custom SSO using a http Header or Cookie - Method 1 (1 of 3)

- **Method 1**  
  Based on the BIEE 10g approach to SSO.
- This approach works with both FMW security or Init Block-based authentication and authorization.
- This approach is for BIEE only (i.e. not BI Publisher or RTD). BI Publisher has a similar mechanism.

The steps to configure this approach are:

1. Login to Enterprise Manager Fusion Middleware Control.  
   - Select Business Intelligence and go to the Security tab.  
   - Click “Lock and Edit”.  
   - In the SSO drop down, select Custom SSO.  
   - Click “Apply”.  
   - Click “Activate changes”.

2. Modify instanceconfig.xml file located at  
   mwhome/instances/instance1/config/OracleBIPresentationServicesComponent/coreapplication_obips1  
   Add/edit the following entry  
   Authentication>
   <!--This Configuration setting is managed by Oracle Business Intelligence Enterprise Manager-->  
   <EnabledSchemas>UidPwd,Impersonate,UidPwd-soap,Impersonate-soap,CustomSSO</EnabledSchemas>  
   </Authentication>
Use Case – Custom SSO using a http Header or Cookie – Method 1 (2 of 3)

• 3. Configure authenticationschemas.xml as follows:

• On your BI installation go to mwhome/Oracle_BI1/bifoundation/web/display
• Edit authenticationschemas.xml with the following changes:

  a> Add a line to the top part of the file (above the similar line for SSO if you intend this mechanism to be used in precedence to a generic SSO mechanism (e.g. Method 2 below).
  <!-- search key for custom sso authentication -->
  <SchemaKeyVariable source="httpHeader" nameInSource="Proxy-Remote-User" forceValue="CustomSSO"/>

  Replace Proxy-Remote-User with the username variable in the HTTPHeader as per your SSO implementation.

  b> Create an Authentication Schema definition for CustomSSO in the same file (somewhere within the <AuthenticationSchemas> tags, but not inside any existing <AuthenticationSchemaGroup> )

  <AuthenticationSchema name="CustomSSO" displayName="Custom SSO Schema" userID="IMPERSONATE" proxyUserID="NQ_SESSION.RUNAS" options="noLogoffUI noLogonUI"/>

  <RequestVariable source="credStoreUser" type="auth" nameInSource="oracle.bi.system/system.user" biVariableName="UID"/> 
  <RequestVariable source="credStorePwd" type="auth" nameInSource="oracle.bi.system/system.user" biVariableName="PWD" options="secure"/>
  <RequestVariable source="httpHeader" type="auth" nameInSource="Proxy-Remote-User" biVariableName="IMPERSONATE" options="required"/>

  Replace Proxy-Remote-User with the username variable in the HTTPHeader as per your SSO implementation.
Use Case – Custom SSO using a http Header or Cookie - Method 1 (3 of 3)

• 4. Restart Oracle BI Services
5. Navigate to http://[webserver:port]/analytics.

6. You should be given access to BI, but only if you have logged into the SSO mechanism protecting BI.

Please note that modifying the authenticationschemas.xml file is a customization that will be ignored by any patching or upgrade. There’s also a risk that the customization may not be possible in a future release. Like any customization, you are responsible for testing the solution to make sure it is secure and works as intended.

• Please note that Oracle BI does not support using URL parameters for authentication other than the standard &NQUSER &NQPASSWORD approach.
Use Case – Custom SSO using a http Header or Cookie - Method 2

- **Method 2**

Using a Custom Weblogic Asserter. You can use any Weblogic Asserter that works with a BI-certified Authenticator (technically, we only certify authenticators that work with the OPSS User/Role API).

You can create your own Weblogic Asserter by following the doc here: [http://docs.oracle.com/cd/E23943_01/web.1111/e13718/ia.htm#i1156163](http://docs.oracle.com/cd/E23943_01/web.1111/e13718/ia.htm#i1156163)

Then, in EM, configure BI for generic SSO.

The downside is that you need to code a bit of Java and it would be your code to support. The upside is that it works across the stack so long as you are using FMW security - not just BIEE.
Architecture Overview

WebLogic

- BI Publisher
- Analytics

Security Service
- OWSM

OPSS
- Identity Store
- Policy Store
- Credential Store

LDAP: WLS, OID, AD etc.

LDAP (OID) or File-based.

MDS

System User Connection

OBIS

Scheduler

OBIPS

OPSS

© 2013 Oracle Corporation
What security mechanisms do we support?


## What Authentication Mechanisms are supported in 11.1.1.6? –
Please Refer to Certification Matrix for the Actual List

<table>
<thead>
<tr>
<th>FMW Security</th>
<th>Init Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>![ ✔️ Supported ]</td>
<td>![ All 10g authentication mechanisms other than RPD users/groups ]</td>
</tr>
<tr>
<td>![ ✗ Not Available ]</td>
<td>![ Users in LDAP, group membership in database ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ Database Authentication ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ Custom Authenticators ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ *multiple AD Domains ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ EBS authentication ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ 64bit platforms ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ SiteMinder 6 or OAM as an Authenticator ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ Use of Asserters and Authenticators combined with Init Block Authentication ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ BI Publisher Limitations ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ RTD ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ Delivers Limitations when using EBS authentication ]</td>
</tr>
<tr>
<td>![     ]</td>
<td>![ Hyperion CSS integration ]</td>
</tr>
</tbody>
</table>

### Supported

- Users and Groups in LDAP
- **Users in LDAP and group membership in Database**
- Users and Groups in Database

**Certified/Supported LDAP versions as listed in published matrix:**
- OID (OID Authenticator)
- OVD (OVD Authenticator)
- AD (AD Authenticator)
- OpenLDAP (OpenLDAP Authenticator)
- Sun Java System Directory Server version 6.3 and ODSEE 11.1.1.3+ (iPlanet Authenticator)
- eDirectory 8.8. (NovellAuthenticator)

**Additional supported Authenticators:**
- Native Weblogic LDAP (Default Authenticator)
- SQL Authenticator *2
- ReadOnlySQLAuthenticator *2
- BISQLGroupLookup Provider

### Not Available

- SiteMinder 6 or OAM as an Authenticator
- *3Any ‘Authenticator’ other than those listed above.

### Notes

- * - Not tested
- *2 - Unless the user passwords are available in the underlying database to authenticate against, these Authenticators can only be used with an SSO mechanism.
- *3 - Only those Authenticators related to Identity Stores that have an appropriate implementation of the OPSS UserRole API may be used. OBIEE restriction only (BIP and RTD can use multiple authenticators).
- *4 - Using the BI SQL Group Lookup Provider
## What Authentication Mechanisms are supported in 11.1.1.7? – Please Refer to Certification Matrix for the Actual List

<table>
<thead>
<tr>
<th>Supported</th>
<th>Init Block</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FMW Security</strong></td>
<td>All 10g authentication mechanisms other than RPD users/groups</td>
</tr>
<tr>
<td>![Checkmark] Yes</td>
<td></td>
</tr>
<tr>
<td>• Users and Groups in LDAP</td>
<td>• Users in LDAP, group membership in database</td>
</tr>
<tr>
<td>• Users in LDAP and group membership in Database*4</td>
<td>• Database Authentication</td>
</tr>
<tr>
<td>• Users and Groups in Database</td>
<td>• Custom Authenticators</td>
</tr>
<tr>
<td><strong>Certified/Supported LDAP versions as listed in published matrix:</strong></td>
<td>• *multiple AD Domains</td>
</tr>
<tr>
<td>• OID (OID Authenticator)</td>
<td>• EBS authentication</td>
</tr>
<tr>
<td>• OVD (OVD Authenticator)</td>
<td>• 64bit platforms</td>
</tr>
<tr>
<td>• AD (AD Authenticator)</td>
<td></td>
</tr>
<tr>
<td>• OpenLDAP (OpenLDAP Authenticator)</td>
<td></td>
</tr>
<tr>
<td>• Sun Java System Directory Server version 6.3 and ODSEE 11.1.1.3+ (iPlanet Authenticator)</td>
<td></td>
</tr>
<tr>
<td>• eDirectory 8.8. (NovellAuthenticator)</td>
<td></td>
</tr>
<tr>
<td><strong>Additional supported Authenticators:</strong></td>
<td></td>
</tr>
<tr>
<td>• Native Weblogic LDAP (Default Authenticator)</td>
<td>• Use of Asserters and Authenticators combined with Init Block Authentication</td>
</tr>
<tr>
<td>• SQL Authenticator *2</td>
<td>• BI Publisher Limitations</td>
</tr>
<tr>
<td>• ReadOnlySQLAuthenticator *2</td>
<td>• RTD</td>
</tr>
<tr>
<td>• BISQLGroupLookup Provider</td>
<td>• Delivers Limitations when using EBS authentication</td>
</tr>
<tr>
<td>![Cross] Not Available</td>
<td>• Hyperion HSS integration (see SSO slide for Hyperion CSS integration)</td>
</tr>
<tr>
<td>• SiteMinder 6 or OAM as an Authenticator</td>
<td></td>
</tr>
<tr>
<td>• *3Any ‘Authenticator’ other than those listed above.</td>
<td></td>
</tr>
</tbody>
</table>

---

* - Not tested
*2 - Unless the user passwords are available in the underlying database to authenticate against, these Authenticators can only be used with an SSO mechanism.
*3 - Only those Authenticators related to Identity Stores that have an appropriate implementation of the OPSS UserRole API may be used. OBIEE restriction only (BIP and RTD can use multiple authenticators).
*4 - Using the BI SQL Group Lookup Provider
What SSO Mechanisms are supported in 11.1.1.6? – Please Refer to Certification Matrix for the Actual List

<table>
<thead>
<tr>
<th>FMW Security</th>
<th>10g-Style SSO</th>
</tr>
</thead>
</table>
| **Supported** | • SSO via http header or cookie – ie. where the SSO product provides the authenticated User via an http header or cookie (requires customization of BI Config)  
• E-Business Suite ICX Cookie mechanism*²  
• Windows Authentication using IIS (uses http header)  
• Siteminder 6 via http header  
• &NQUSER/&NPASSWORD URL parameters via get or post |
|  | • Use of Asserters and Authenticators combined with Init Block Authentication  
• SSO via URL parameter other than when using &NQUSER/&NPASSWORD  
• Hyperion CSS Token  
• BI Office and Client tools and BI session-based web services are not able to use SSO, but will still work using UID/Password |
| **Not Available** | • Use of Asserters and Authenticators rather than directly to the underlying LDAP Identity Store*³  
• BI Office and Client tools and BI session-based web services are not able to use SSO, but will still work using UID/Password |

* - Not all Asserters have been tested against.

*² - Both BI and E-Business Suite must appear to be in the same Internet Domain.

*³ - OBIEE restriction only (BIP and RTD can use additional authenticators)
## What SSO Mechanisms are supported in 11.1.1.7? – Please Also Refer to Certification Matrix

<table>
<thead>
<tr>
<th>FMW Security</th>
<th>10g-Style SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported</strong></td>
<td><em><em>Use of most Asserters delivered in Weblogic</em> when combined with a supported Authenticator as listed on the previous slide.</em>*</td>
</tr>
<tr>
<td></td>
<td>This includes:</td>
</tr>
<tr>
<td></td>
<td>• OAM Asserter (but not Authenticator)</td>
</tr>
<tr>
<td></td>
<td>• OSSO Asserter</td>
</tr>
<tr>
<td></td>
<td>• Default Asserter (for Client Certificate Authentication)</td>
</tr>
<tr>
<td></td>
<td>• NegotiateIdentityAsserter (for Windows Native Authentication without IIS)</td>
</tr>
<tr>
<td></td>
<td>• SAML2IdentityAsserter (but not Authenticator)</td>
</tr>
<tr>
<td></td>
<td><strong>SSO via http header or cookie – ie. where the SSO product provides the authenticated User via an http header or cookie (requires customization of BI Config)</strong></td>
</tr>
<tr>
<td></td>
<td>• E-Business Suite ICX Cookie mechanism*²</td>
</tr>
<tr>
<td></td>
<td>• Windows Authentication using IIS (uses http header)</td>
</tr>
<tr>
<td></td>
<td>• Siteminder 6 via http header</td>
</tr>
<tr>
<td></td>
<td>• &amp;NQUSER/&amp;NQPASSWORD URL parameters via get or post</td>
</tr>
<tr>
<td></td>
<td><strong>Hyperion CSS Token</strong></td>
</tr>
<tr>
<td><strong>Not Available</strong></td>
<td><strong>Use of Asserters and Authenticators against SSO products rather than directly to the underlying LDAP Identity Store*³</strong></td>
</tr>
<tr>
<td></td>
<td>• BI Office and Client tools and BI session-based web services are not able to use SSO, but will still work using UID/Password</td>
</tr>
<tr>
<td></td>
<td>• <strong>BI Mobile is only supported with OAM for SSO</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Use of Asserters and Authenticators combined with Init Block Authentication</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SSO via URL parameter other than when using &amp;NQUSER/&amp;NQPASSWORD</strong></td>
</tr>
<tr>
<td></td>
<td><strong>BI Office and Client tools and BI session-based web services are not able to use SSO, but will still work using UID/Password</strong></td>
</tr>
<tr>
<td></td>
<td><strong>BI Mobile and SmartView are not supported to use 10g-style SSO</strong></td>
</tr>
</tbody>
</table>

* - Not all Asserters have been tested against.

*² - Both BI and E-Business Suite must appear to be in the same Internet Domain.

*³ - OBIEE restriction only (BIP and RTD can use additional authenticators)
Fusion MiddleWare Security Model

Part 1 – Without SSO
What happens when a User Logs In?

Simple Version 1 - Default Authenticator/Asserter

User enters UserID and Password to /analytics Login Form

1. Enter UserID and Password to /analytics Login Form

2. BI Server calls Security Service to Authenticate User Credentials

3. Security Service returns an object to BI Server with attributes for user profile data, application roles and permissions. The BI Session is now authenticated.

4. BI Server calls Security Service to Authenticate User Credentials

5. UserID and Password posted to Presentation Services

6. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service

7. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service

8. Security Service returns an object to BI Server with attributes for user profile data, application roles and permissions. The BI Session is now authenticated.

9. Session and Session Variables for User & Roles returned to Presentation Services

10. Oracle BI Server

11. BI Session returned to Oracle BI Presentation Services

12. BI Session returned to browser cookie
What happens when a User Logs In?

Simple Version 2 - Default Authenticator/Asserter

1. Enter UserID and Password to /analytics Login Form
2. BI Server calls Security Service to Authenticate User Credentials
3. User ID and Password used in Connection string to BI Server (ODBC)
4. Security Service returns an object to BI Server with attributes for user profile data, application roles and permissions. The BI Session is now authenticated
5a. Security Realm
5b. Application Server (Weblogic domain)
6a. Embedded LDAP (system-jazn-data.xml)
6b. Policy Store
5c. OPSS
6c. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service
7a. BI Session returned to Presentation Services
7b. Session and Session Variables for User & Roles returned to Presentation Services
8. Security Realm
9. Oracle BI Server
10. Oracle BI Presentation Services
11. BI Session returned
12. BI Session returned to browser cookie

Enter UserID and Password to /analytics Login Form

OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service

BI Server calls Security Service to Authenticate User Credentials

Security Service returns an object to BI Server with attributes for user profile data, application roles and permissions. The BI Session is now authenticated

Session and Session Variables for User & Roles returned to Presentation Services

BI Session returned to browser cookie

© 2013 Oracle Corporation
What happens when a User Logs In?
Simple Version 3 - Default Authenticator/Asserter

1. User enters UserID and Password to /analytics Login Form.
2. BI Server calls Security Service to Authenticate User Credentials.
3. Security Service calls OPSS API to request Permissions for the Subject.
4. Security Service calls OPSS API to Authenticate the User.
5. Security Service calls OPSS API to retrieve User/Role information.
6. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service.
7. Security Service returns an object to BI Server with attributes for user profile data, application roles and permissions. The BI Session is now authenticated.
8. BI Server calls Security Service to Authenticate User Credentials.
9. User ID and Password used in Connection string to BI Server (ODBC).
10. Session and Session Variables for User & Roles returned to Presentation Services.
11. BI Session returned.
12. BI Session returned to browser cookie.

Security Realm
- Embedded LDAP
- Policy Store (system-jazz-data.xml)

OPSS
- 5a Security Realm
- 6a Managed Server
- 6b Web Browser
- 6c Security Realm
- 5b Application Server (Weblogic domain)
- 6d Security Realm
- 7b Oracle BI Server
User Profile Information
User Profile Information

• What attributes do we look for?
• Where do we get it from?
User Profile Information

- User Profile information such as Displayname, Locale, Timezone, email comes from the following locations:
  - LDAP Attributes via FMW security
  - SA System Subject Area
  - Webcat Profile
  - Init Blocks

- GUID is part of the user profile
  - If using FMW security User GUID is mandatory
Authentication and Authorization from multiple Identity Stores
Virtualization (New in 11.1.1.5)

- Enables Authentication chaining for BI
- Federates the lookup of user profile information across multiple Identity Stores
- Required if using SQL Authenticator or Read Only SQL Authenticator
- Also used to configure native Weblogic LDAP for HA
Virtualization

- Follow 7.3.2.2 Configuring the Service for Multiple LDAP using Fusion Middleware Control in this doc:

http://download.oracle.com/docs/cd/E21764_01/core.1111/e10043/idstoreadm.htm#CIAIDIFI
Fusion MiddleWare Security Model

Part 2 – Including SSO
Single Sign On (SSO)

SSO enables a user to log in once and gain access to all systems without being prompted to log in again at each of them. If SSO is enabled then Oracle Business Intelligence will not challenge the user for authentication and will assume the user has already been authenticated by SSO.

- Enable SSO
  - Custom
  - Oracle SSO
  - Oracle SSO plus Fusion Applications
  - Oracle Access Manager
  - Oracle Access Manager plus Fusion Applications

Security Realm
- Go to the Oracle CA SiteMinder and manage the WebLogic security realm.

Application Policy
- Configure and manage Application Policies
- Configure and manage Application Roles
What happens in Instanceconfig.xml when you turn on SSO?

<Authentication>
<!--This Configuration setting is managed by Oracle Business Intelligence Enterprise Manager-->
<EnabledSchemas>UidPwd,Impersonate,UidPwd-soap,Impersonate-soap,SSO-Siteminder</EnabledSchemas>
</Authentication>
What happens when a User Logs In?

Pre-Authenticated Via SSO with Users and Groups available via an Authenticator defined in the Security Realm

1. User navigates to /analytics having previously authenticated against a supported SSO mechanism.

2. J2EE Container works through the list of Asserters in the Security Realm in order to assert the user based on a token of some sort from SSO. Following assertion, the list of Authenticators is worked through in order to lookup the User. As a result, the JAAS Principal is populated with the UserID and becomes available via a call to getRemoteUser.

3. BI Server calls Security Service to Assert User Credentials. UserID retrieved from J2EE Container via call to getRemoteUser() used in Connection string to BI Server (ODBC).

4. User ID and Impersonator ID (BISystemUser) used in Connection string to BI Server (ODBC).

5. BI Session returned to Presentation Services.

6a. OPSS looks up the UserID against the Embedded Weblogic LDAP. OPSS retrieves a Subject containing the User's Username and Groups.

6b. Security Service calls OPSS API to retrieve User/Role information.

6c. OPSS retrieves Permissions for the Subject from the Policy Store.

6d. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service.

7a. Security Service calls OPSS API to Assert the User.

7b. Security Service looks up the UserID against the Embedded Weblogic LDAP. OPSS retrieves a Subject containing the User's Username and Groups.

7c. OPSS looks up the UserID against the Embedded Weblogic LDAP. OPSS retrieves a Subject containing the User's Username and Groups.

8a. OPSS retrieves Permissions for the Subject from the Policy Store.

8b. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service.

9. OPSS sends Subject containing UserID, Roles, Profile information and Permissions to bimiddleware service.

10. Security Service returns an object to BI Server with attributes for user profile data, application roles and permissions. The BI Session is now authenticated.

11. BI Session returned to browser cookie.

12. BI Session returned to Oracle BI Presentation Services.

13. BI Session returned to browser cookie.

Pre-Authenticated Via SSO with Users and Groups available via an Authenticator defined in the Security Realm.
BI 10g Security Model
GROUP and ROLES Session Variables

- The GROUP session variable existed in 10g and held the list of Groups that the user was assigned to.
- The GROUP session variable exists in 11g and now holds the list of Application Roles that the user is assigned to.
- A new session variable ‘ROLES’ was created in 11g as a more appropriately named variable for holding the list of Application Roles the user is assigned to.
- When the user logs in, the BI Server has logic to synchronize the GROUP and ROLES session variables. So both should hold identical values.
- This synchronization ensures backwards compatibility for RPDs that include Init Blocks setting GROUP rather than ROLES and RPDs that refer to the GROUP session variable explicitly in other areas (e.g. Subsequent Init Blocks, formulae or security filters).
- If using Init Block security, greenfield sites from 11.1.1.5 onwards should aim to set ROLES rather than GROUP in order to get people thinking in terms of securing by Application Role rather than (LDAP) groups. The intention is to deprecate the GROUP session variable at an appropriate point in time.
How to Use the Init Block Security Model in BI EE 11g

• In Oracle BI 11g, Init Blocks to set USER and GROUP (or ROLES) will only fire when the user trying to authenticate is not found via an Authenticator configured in the WebLogic security Realm. Therefore, you should not configure any authenticators which reference a user that you want to authenticate using Init Block authentication.

• If the intention is for all BI users to authenticate using Init Blocks, an authenticator still needs to be configured and should contain the BI System User and the OracleSystemUser and related group. By default, this would be the default authenticator.

• When using an Init Block to set the GROUP (or ROLES) session variable, the values of this variable should be set to match by name against one or more Application Roles configured via Enterprise Manager Fusion Middleware Control, for example, “BIConsumer”. A user will be assigned these Application Roles and associated permissions during authentication.

• Please refer to the documentation in Oracle Fusion Middleware Security Guide for Oracle Business Intelligence for information about Application Roles and how to add a new Application Role.

• When using init blocks to set USER and GROUP (or ROLES), the association of groups to Application Roles is performed using the logic described above. Assignment of users and groups to Application Roles in the policy store is not used in this case.

• Any values of the GROUP (or ROLES) variable that do not match an Application Role will be matched by name against the available Web Groups in the BI Presentation Services Web Catalog. The user will be assigned these Web Groups and associated privileges.

• Any value of GROUP (or ROLES) that does not match an Application Role or a Web Group will be ignored.
System Users and the Credential Store
**System Users**

- **BISystemUser**
  - By default called BISystemUser, but can be any user
  - Used for inter-bi-component communication
  - Used for Impersonation
  - Referenced via an ‘Authenticator’ (the Default Authenticator unless changed)
  - Credentials stored in the Credential Store under oracle.bi.system – system.user
  - Does not need Group membership, but does need the Weblogic Global Role called ‘Admin’.
    - Note this is not an ‘Application Role’.
    - By default BISystemUser is a member of an LDAP Group called ‘Administrators’ which is assigned to the Weblogic Global Admin Role.

- **OracleSystemUser**
  - Used by OWSM
  - By default called OracleSystemUser and a member of the OracleSystemGroup
  - User name can be changed, but need to follow FMW documentation
  - By default created in the native Weblogic LDAP and referenced via the Default Authenticator. This can be changed.
The Credential Store

• BI uses it to hold:
  • BISystemUser credential
  • Actions/OWSM credentials
  • SSL credentials and certificates
  • RPD credentials
  • Web Services for SOA browsing credential
Troubleshooting and Logging
Introducing the BI Security Diagnostics Helper

The Oracle BI Security Diagnostics Helper is a JEE application that helps diagnose possible configuration issues which may prevent your users from being able to log in to your Oracle BI system.

```
Business Intelligence Diagnostics

User id: 
Password: 
Managed Server Host: slc01nfv.us.oracle.com 
Managed Server Port: 7001 
Test Authentication

Testing container-only authentication ✓
Testing full BI authentication ✓
Testing BI Web Service authentication ✓

Successfully authenticated user Subject: Principal: BIAuthors Principal: ApplicationRolePrincipal: BIConsumer,uname:example
Principal: ApplicationRolePrincipal: BIAuthor,uname:example
Principal: ApplicationRolePrincipal: BIAdministrator,uname:example
Private Credential: Subject: Principal: weblogic Principal: Administrator (full BI logon)

User authenticated successfully to the BI System: weblogic
User authenticated successfully to the BI System via Web Service

<- Previous (Tests for BISystemUser) ^ Main index
```
Creating a Clean Set of Logs

**Process**

Doc ID 1434514.1

- Set appropriate log levels, stop all processes, clear logs then re-start and re-produce the error
- Collect config.xml and jps-config.xml and adapters.os_xml (if using multiple Authenticators i.e. virtualize=true)
- Work through the logs in the following order:
  - OBIPS (saw.log)
  - OBIS (NQServer.log)
  - Managed Server .out (Admin Server if using a Simple Install from 11.1.1.5)
  - Managed Server .log (Admin Server if using a Simple Install from 11.1.1.5)
  - Managed Server diagnostic log (Admin Server if using a Simple Install from 11.1.1.5)
  - Domain and Admin Server logs for MDS errors
- Identify error with timestamps and cross-reference between log files (maybe via EM ECID)
- Identify the root cause error
BI Security Troubleshooting Guide

Doc ID 1359798.1

Or

BI Security Guide
Types of Security
Types of Security (other than Authentication)

• SSL
• J2EE Perimeter
• App Roles for Authorization
• Web Groups for Authorization
• Data Level Security
SSL Everywhere

- SSL Configuration in Oracle Business Intelligence

- One-way SSL easy to configure.
Perimeter Security

• J2EE Security
  • Authenticate (and authorization) into the J2EE container can be inherited by the J2EE applications within that container
  • Weblogic container uses Asserters and Authenticators
Application Roles

These role types are used by security-aware applications that are specific to the application. These role types are being used to secure access to the BI application.

Application Roles, Policies and Permissions in the Policy Store

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Members</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BISystem</td>
<td>BISystem, User</td>
<td></td>
</tr>
<tr>
<td>BIAdministrator</td>
<td>BIAdministrators</td>
<td></td>
</tr>
<tr>
<td>BIAuthor</td>
<td>BIAuthors, BIAdministrator</td>
<td></td>
</tr>
<tr>
<td>BIController</td>
<td>BIControllers, Users, dabling, BIAuthor, authoring</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>BIControllers, BIAuthors</td>
<td></td>
</tr>
<tr>
<td>Anonymous</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An alternative – simpler view
BI Application Role Model Summary – Permissions and Privileges in the RPD
BI Application Role Model Summary - Permissions and Privileges in the webcat

<table>
<thead>
<tr>
<th>Access</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Dashboards</td>
<td>E1Consumer</td>
</tr>
<tr>
<td>Access to Answers</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to Delivers</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to Briefing Books</td>
<td>E1Consumer</td>
</tr>
<tr>
<td>Access to Administration</td>
<td>E1Administrator</td>
</tr>
<tr>
<td>Access to Segments</td>
<td>E1Consumer</td>
</tr>
<tr>
<td>Access to Segment Trees</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to List Formats</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to Metadata Dictionary</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to Oracle BI for Microsoft Office</td>
<td>E1Consumer</td>
</tr>
<tr>
<td>Access to Conditions</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to KPI Builder</td>
<td>E1Author</td>
</tr>
<tr>
<td>Access to Scorecard</td>
<td>E1Consumer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Navigate Actions</td>
<td>E1Consumer</td>
</tr>
<tr>
<td>Create Invoke Actions</td>
<td>E1Author</td>
</tr>
<tr>
<td>Save Actions containing embedded HTML</td>
<td>E1Administrator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin Catalog</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Permissions</td>
<td>E1Author</td>
</tr>
<tr>
<td>Toggle Maintenance Mode</td>
<td>E1Administrator</td>
</tr>
<tr>
<td>Manage Sessions</td>
<td>E1Administrator</td>
</tr>
<tr>
<td>Manage Dashboards</td>
<td>E1Author</td>
</tr>
<tr>
<td>See sessions IDs</td>
<td>E1Administrator</td>
</tr>
</tbody>
</table>
Data-level Security

- The same as 10g
- Plus new Essbase functionality