SAP Business Objects Security

Pal Alagarsamy
President
Business Intelligence Practice
GloWiz Inc

GloWiz Inc

- GloWiz is an IT Staffing and Consulting company since 2005
- We focus on Business Intelligence, Data Warehouse, Project Management and Architects
- Our BI Practice, particularly BOE includes;
  - BOE Environment Assessment
  - Requirement Analysis
  - Installation and Configuration (R2, XI 3.x)
  - Dashboard Development
  - Report Development
  - System Administration and Support
  - Security Setup and Management
  - 5.x or 6.x or R2 to XI 3.x Migration
  - BI Implementation & Best Practices
  - BO Training

GloWiz Inc, 11801 Rockville Pike, Suite 403, Rockville MD 20852
P: (877) 456-9490 F: (877) 766-4240 Email: info@glowizinc.com Web: www.glowizinc.com

Agenda

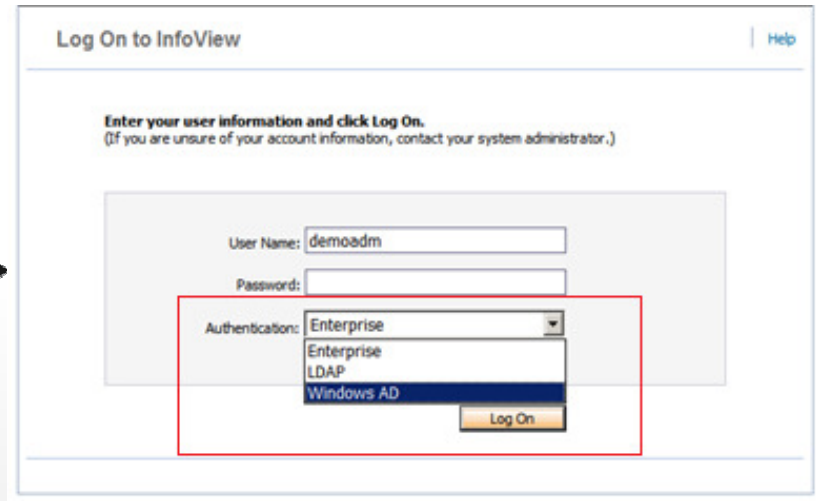
1. Business Objects Security Overview
2. Authentication and Authorization
3. Primary Authentication and SSO
4. Other BOE Security and Protections
5. Central Management Console (CMC)
6. Out of the Box Security
7. Security Best Practices

1. Business Objects Security Overview

- Business Objects Enterprise provides a framework for an increasing number of products within BOE family.
- This presentation explores how this framework enforces and maintains security
- More specifically this focuses on BOE XI 3.x version

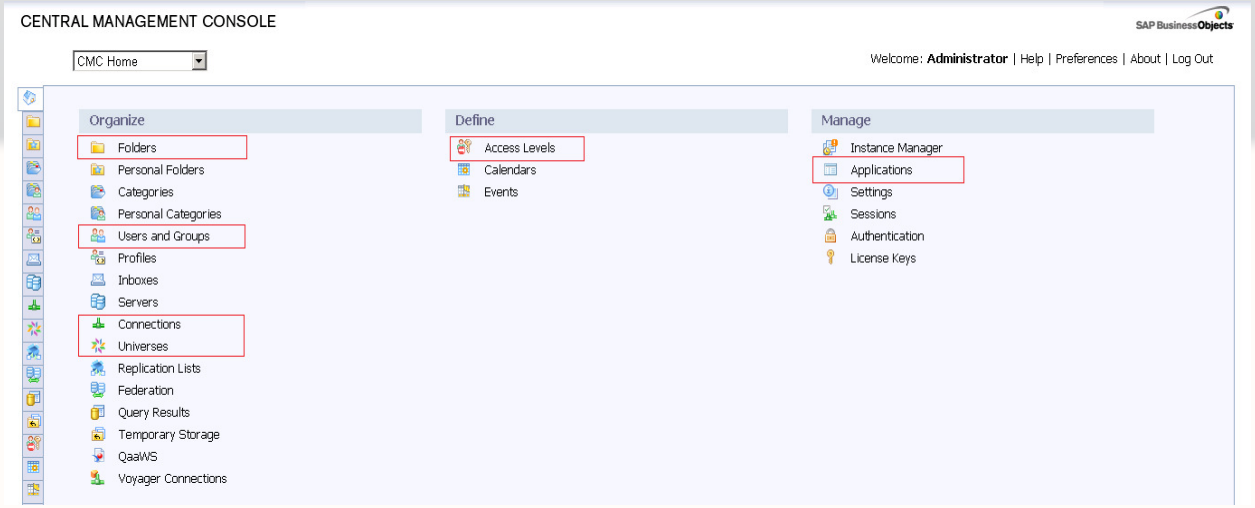
2. Authentication and Authorization

- Authentication is the process of verifying the identity of a user who attempts to use Business Objects Enterprise system.
- Authentication type can be Enterprise or Third Party Authentication such as LDAP or Windows AD.
- Authentication Flow: InfoView →SDK → Security Plug-In →CMS.



2. Authentication and Authorization…

- Authorization is the process of verifying the user has sufficient rights to perform the requested action upon a given objects.
- Action means to view, refresh, edit, schedule, etc. Object means folder, report, instance, universe, etc.
- Authorization is handled based on how the access level, application security, and content security such as users and groups, universe security, folder access, etc. are defined using CMC.



3. Primary Authentication and SSO

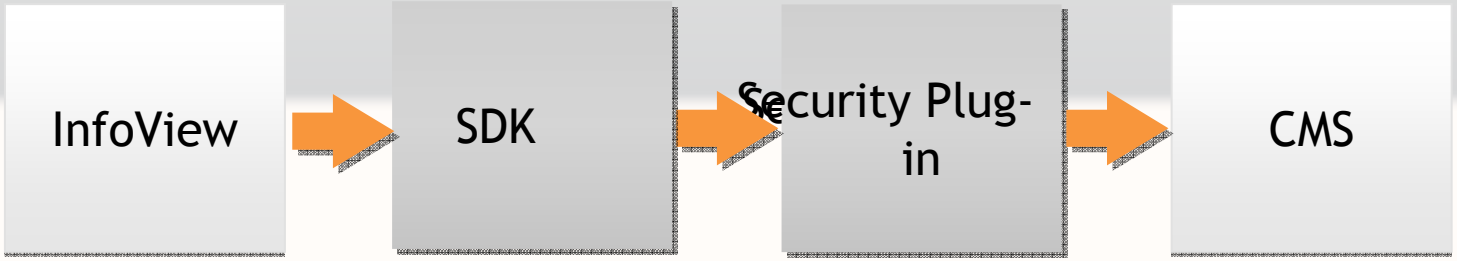
- Primary authentication occurs when the user first attempts to access Business Objects through InfoView or CMC.
- Single sign-on means once the user has entered his/her credentials to the Windows OS or LDAP, they can access Business Objects applications without having to enter the user credentials again.
- The following table describes out of the box methods of single sign-on support for InfoView and CMC.

Authentication Mode	Options	Comments
Windows AD	Windows AD with Kerberos only	Windows AD authentication to InfoView and CMC is available out of the box
LDAP	LDAP with SiteMinder only	LDAP authentication to InfoView and CMC is available out of the box. SSO requires SiteMinder
Enterprise	Trusted Authentication	Enterprise authentication to InfoView and CMC is available out of the box. SSO requires Trusted Authentication

3. Primary Authentication and SSO…

- Security plug-ins for the SSO is shipped out of the box and installed as part of BOE installation. These security plug-ins facilitates you to create and manage user accounts by allowing you to map users and groups from third party systems to BOE.

- Single Sign-on contexts can be 1. SSO to Enterprise, 2. SSO to Database, or 3. End to end SSO.



4. Other BOE Security and Protections

- Active trust relationship provides secured and seamless access to various applications within BOE through logon token and ticket mechanism.
- Session and session tracking using cookies and session variable.
- Environment protection between browser to web server and web server to BOE.
- Protection against malicious logon attempts through auditing web activities by logon restrictions, password restrictions, and user restrictions

5. Central Management Console (CMC)

- CMC is a web based tool helps you to perform day-to-day administrative tasks including user management, content management, and server management.

- Most of the authorization part is created, administered and maintained in CMC. This includes;
  - Access Levels and Inheritance
  - Application Security
  - Content Objects Security

6. Access Levels and Inheritance

- Access level is a set of rights that users frequently need.
- BOE comes with pre-defined out of the box access levels such as Administrator, Full Access, Schedule, View and View on Demand.
- However you can create and customize your own access levels.
- Rights are set on an object for a user in order to control the access to the specific objects. It is highly impractical to set this individually when there are hundreds of objects.
- Inheritance resolves this impractical situation by passing on the set of rights from a group to sub-group or from a folder to sub-folder.

7. Applications Security

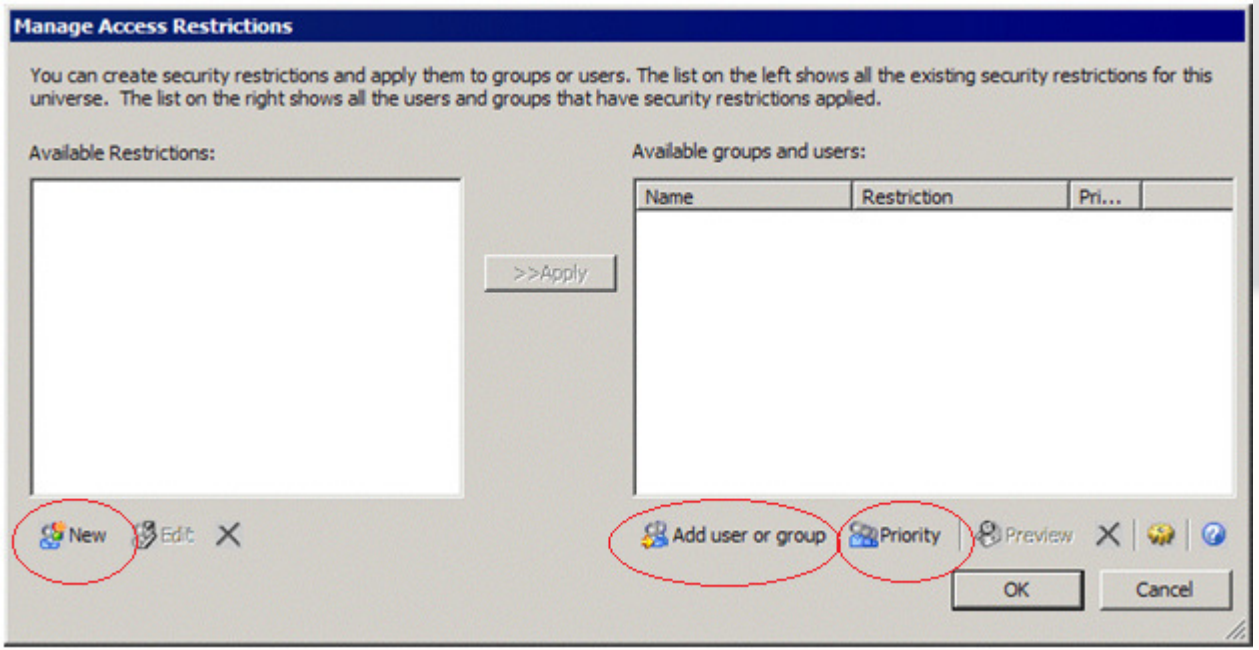
- CMC allows you to control the appearance and features of tools such as,
  - InfoView
  - Desktop Intelligence
  - Web Intelligence
- You can use user rights to control the user access of certain features in Business Objects applications.

8. Users and Groups

- CMC is your one stop shop for user and group management whether you use Enterprise or third party authentication type with or without SSO.
- By default, the BOE out of the box comes with two users, Administrator and Guest.
- Group is a collection of users who share the same account privileges. A group can have sub-groups which may share the same or a sub-set of the parent group privileges.
- Users can be added to a group or sub-group or more than one groups or sub-groups.
- When groups with different access levels are enabled to other contents such as folders, categories, universe or connections, the users from the group automatically inherit the rights.

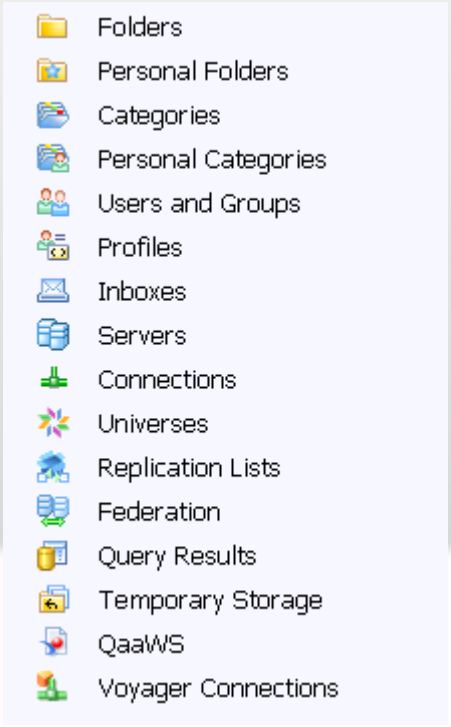
9. Universe and Connection Security

- Universe security is managed at two levels CMC and Universe Designer.
- From CMC restrictions such as access level, users and groups, and usage rights can be applied and stored in CMS.
- From Universe Designer restrictions such as Connection, Query Controls, SQL Generation, Object Access, Row Access, Alternate Table Access can be defined.
- Restriction is a powerful security feature. You can apply restrictions to a selected user or group for a universe.



10. Content Objects Security

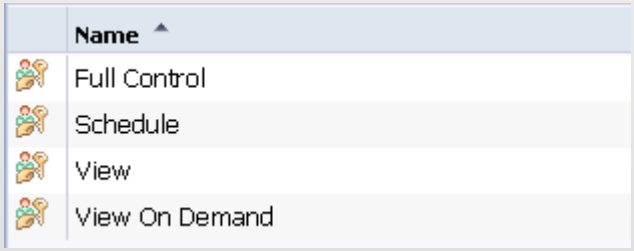
- User security can be defined at the most granular level for the following content objects.
  - Folders and sub-folders
  - Reports
  - Categories
  - Events
  - Program Files
  - Publications



- Content level security is helpful to when users have different level of access across applications.

11. Out of the Box Security

- BOE comes with following out of the box security.
- Access Levels
  - Full Control
  - Schedule
  - View
  - View on Demand



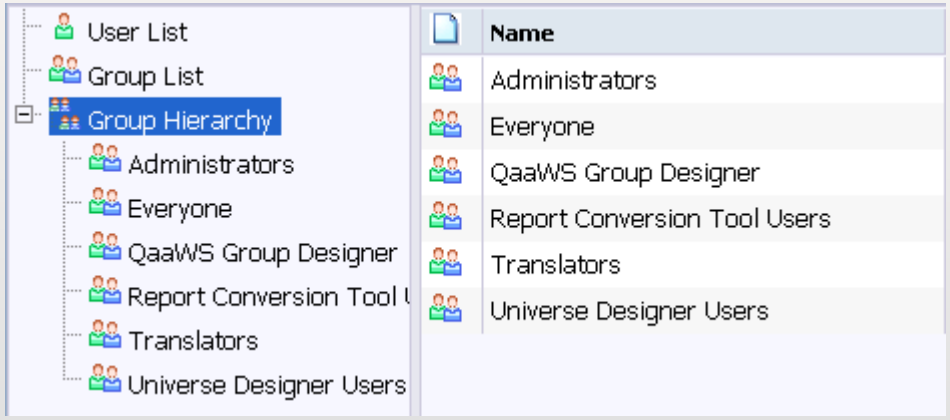
	Name
	Full Control
	Schedule
	View
	View On Demand

- Application Security
  - Content
  - Designer
  - Web Intelligence
  - CMC, etc.

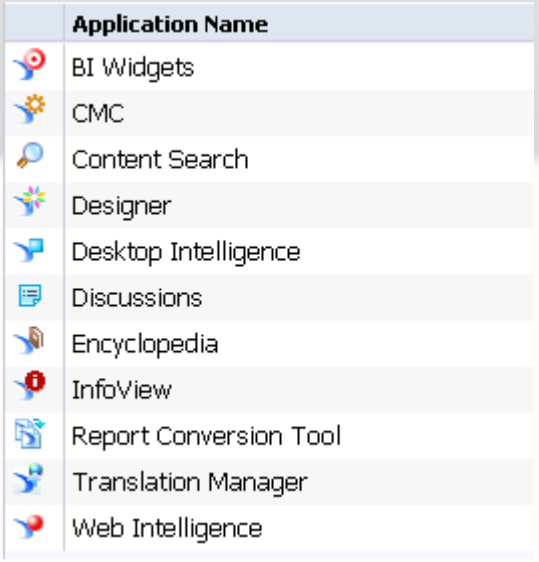
Collection	Type	Right Name	Status
Application	BI Widgets	Log on to the BI Widgets and view this object in the CMC	
Application	BI Widgets	Edit this object	
Application	BI Widgets	Modify the rights users have to this object	
Application	BI Widgets	Securely modify rights users have to objects.	
Application	BI Widgets	Use Explorer	
Application	BI Widgets	Use Alert Inbox	
Application	BI Widgets	Use Search	
Application	CMC	Log on to the CMC and view this object in the CMC	
Application	CMC	Edit this object	
Application	CMC	Modify the rights users have to this object	
Application	CMC	Securely modify rights users have to objects.	
Application	CMC	Allow access to Security Query	
Application	CMC	Allow access to Relationship Query	
Application	CMC	Allow access to Instance Manager	
System	Connection	Data Access	
System	Connection	Use connection for Stored Procedures	
Application	Content Search	View	
Application	Content Search	Edit this object	

11. Out of the Box Security…

- Users and Groups
  - Administrators
  - Everyone
  - Universe Designer Users



- Applications (Default Settings)
  - CMC
  - InfoView
  - Web Intelligence
  - Desktop Intelligence, etc.



12. Security Best Practices

- Create a security matrix for each of your application
- Leverage out of the box access levels. Create new access level only when necessary.
- Use common naming convention for your application across report folder, universe folder, user groups, and access levels.
- Follow universe development best practices particularly connection, control, SQL generation, and restrictions.

12. Security Best Practices…

- Leverage the use of Inheritance while defining folder, sub-folder, user and group security.
- Simplify the security model. Complex model may cause performance issue especially when SSO is implemented.

THANK YOU!

Pal Alagarsamy
pal@glowizinc.com