EA209

Understanding Security and Rights in SAP BusinessObjects Business Intelligence 4.1

Greg Wcislo

September, 2013

Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Agenda

What security is available in BI4

- Authentication, Report, Application, Data
- Inheritance

Securing at the right layer

- BI Object security (report level)
- Universe security
- Data source security

Best practices for a low headache security model

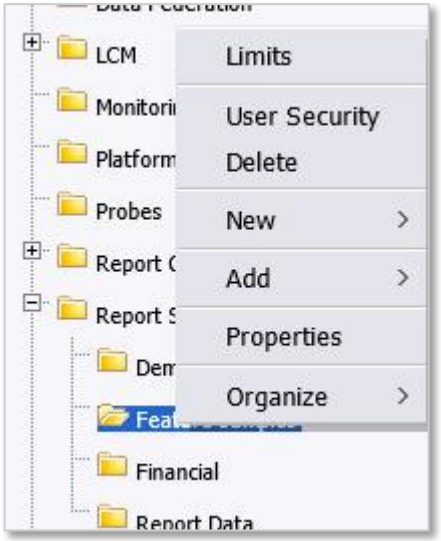
Security changes between 3.1 and 4.x

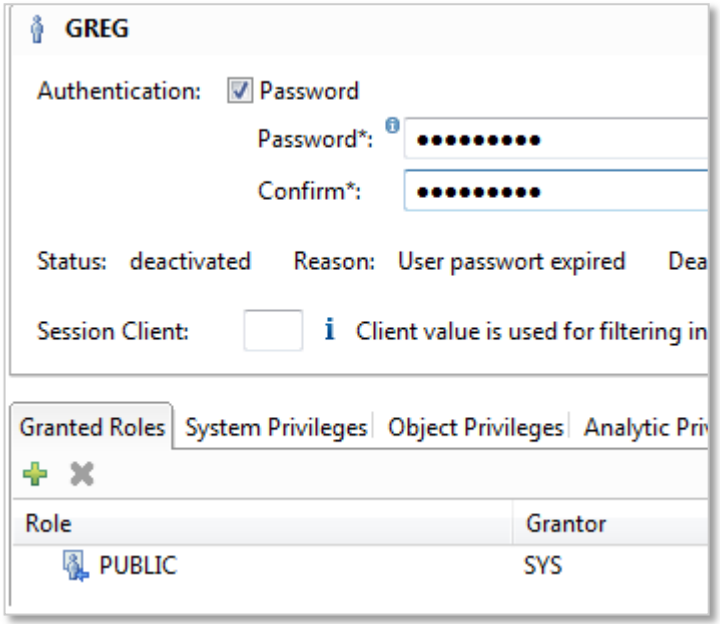
Different levels of security

Data Security

Data can be secured at:

- Folder/report level
- Universe level
- Database source level

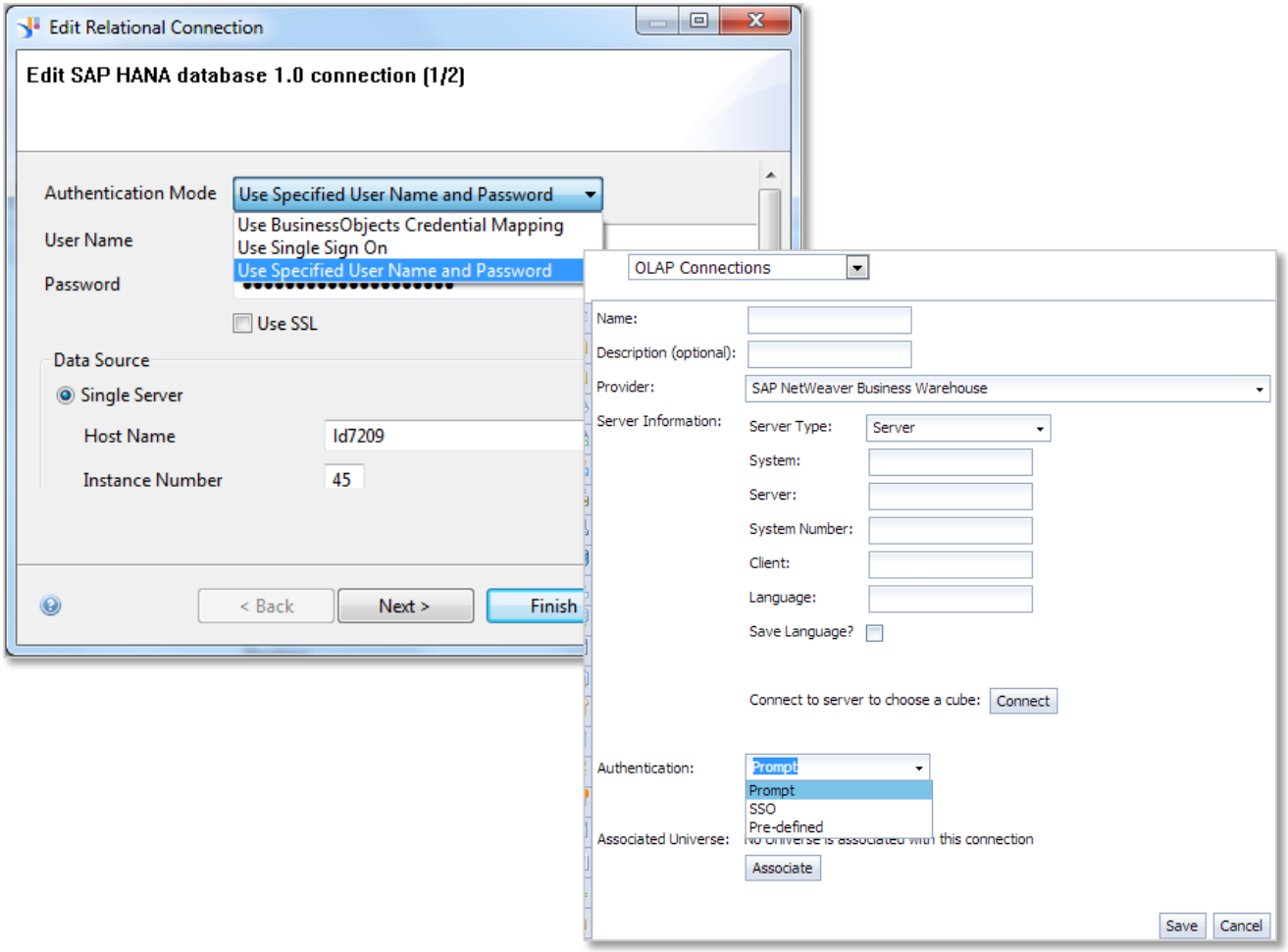




Considerations when creating Connections to data (shared)

Shared Connection

- All users logon to database with same shared user ID.
- Often referred to as “Technical User” or “System User”.
- Secure in BI system at report or universe level
- Pros:
  - No need to replicate users & manage security at database level
- Cons:
  - No differentiation of what users can see in the database*.



Considerations when creating Connections to data (SSO)

Use Single Sign On

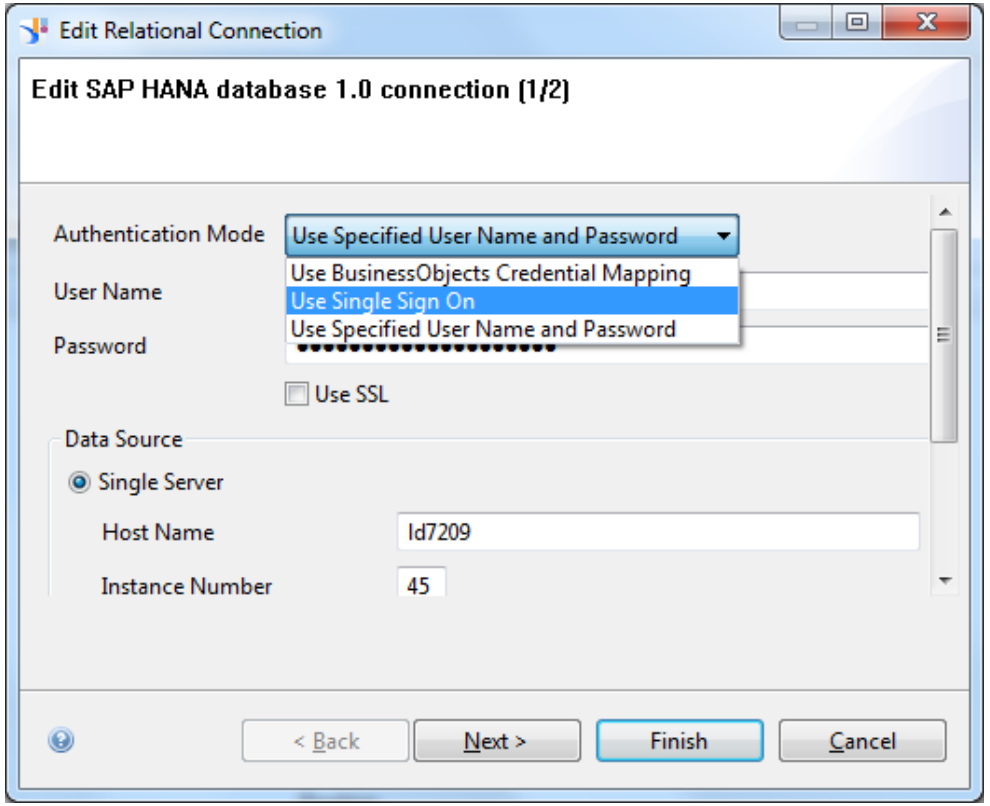
- Kerberos available for
  - MS SQL Server & Analsysis Services
  - Oracle
  - Teradata (as of 4.1 via ODBC)
  - HANA
- Trust Certificates*
  - HANA (internally SAML)
  - SAP

Pros:

- User's account & security applied at data source level (most secure)

Cons:

- No Kerberos SSO for scheduling
- User acounts must exist on both systems

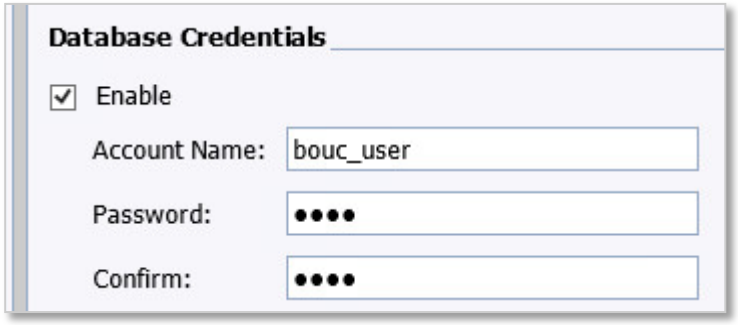


Refer to http://scn.sap.com/docs/DOC-33875 for full list of SSO options

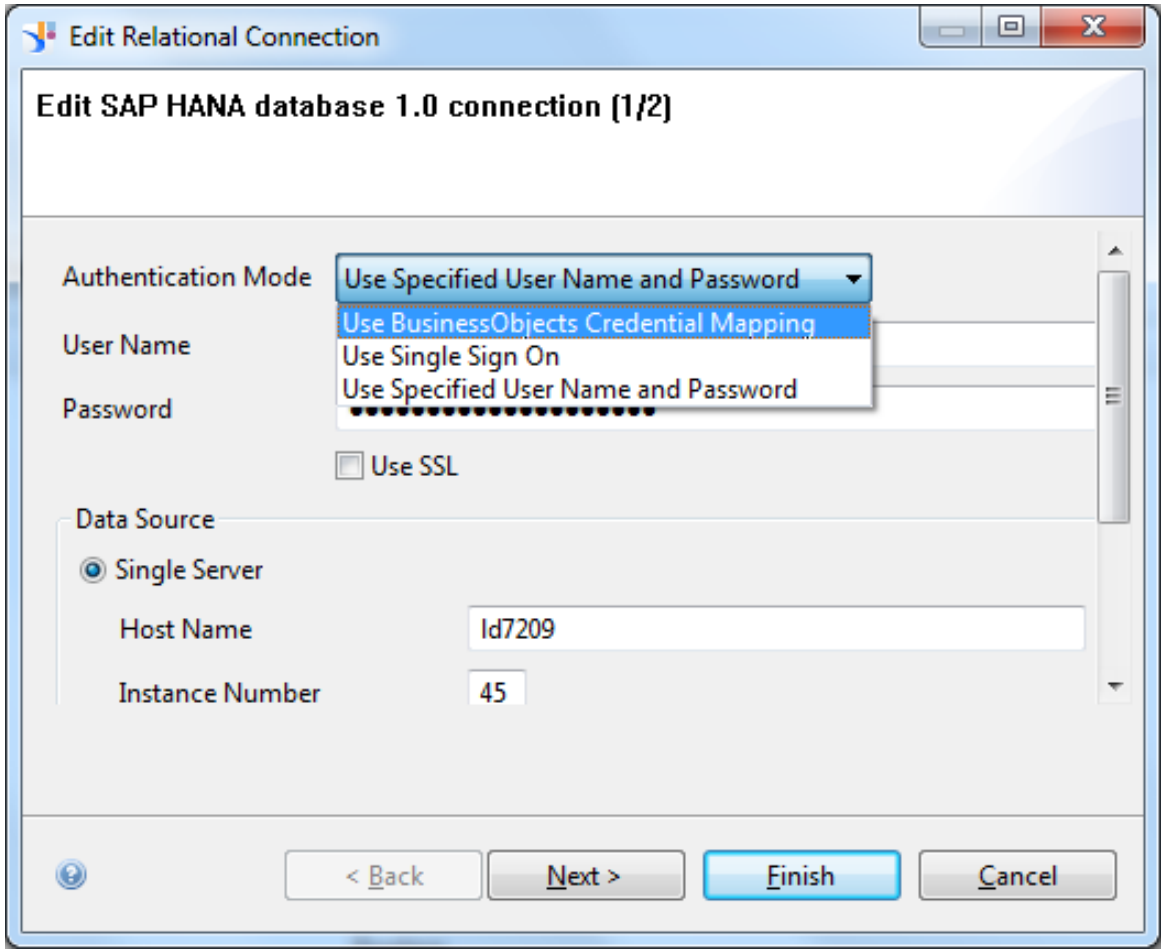
Considerations when creating Connections to data (save password)

Credential Mapping

- User's database credentials hardcoded and saved in BI4 system
- Password capture/replication required
- A user can only have one of these in the system.



- Capture during logon if no SSO or set via SDK



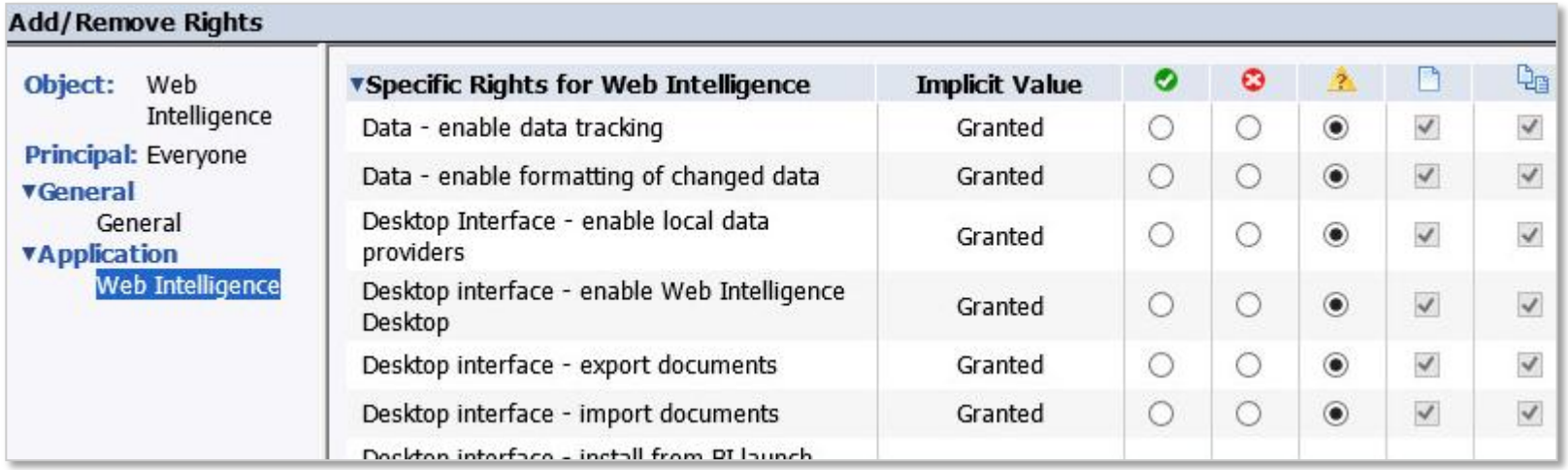
Some help deciding where to secure

- Report objects are still going to be listed if only database is secured
- Consider where your main user management is, take user federation into consideration
- Consider your overall landscape (not just BI). Do you have other applications accessing your DB?

Application rights

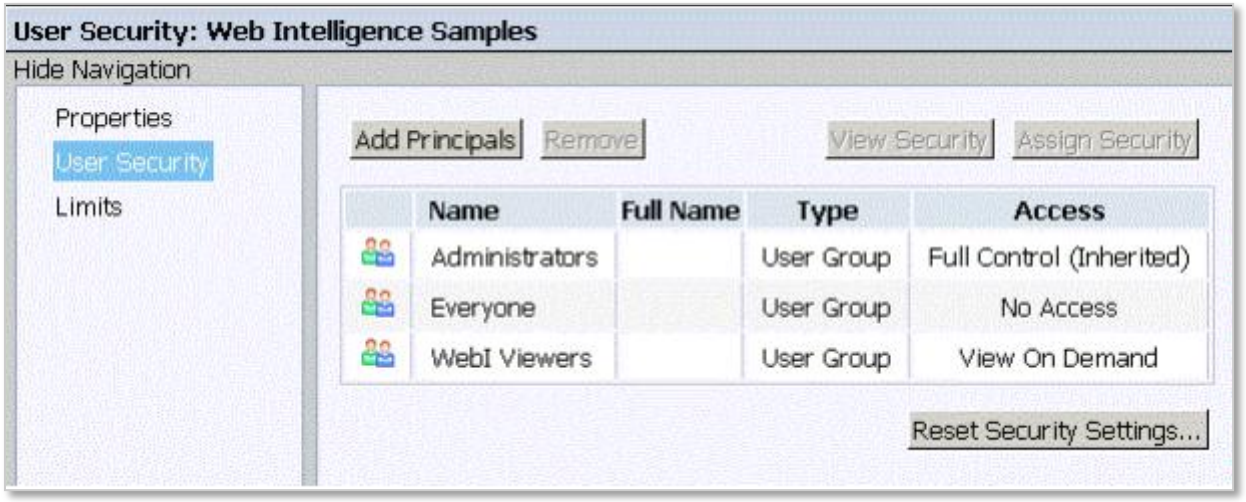
Set what user can do in system

Example Webi report edit panel, logon to CMC



Access Control List

- Access Control List (ACL) is the list of principals who have access to an object .
- Principals are the users and groups.



Access Levels

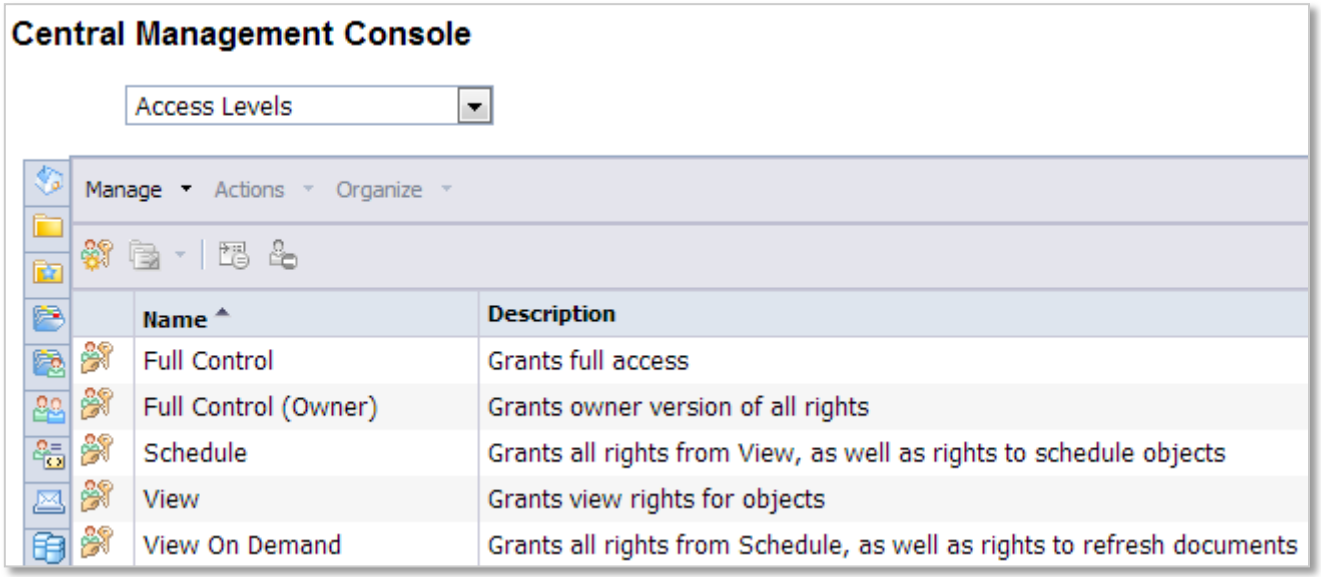
Many rights in the system

Do not assign individual rights

- Not reproducible, high maintenance

Use Access levels which are collections of rights

- Assign to groups, not individual users
- Build up from minimum rights and increment
- Minimize explicit denies
  - Grant + Deny = Deny

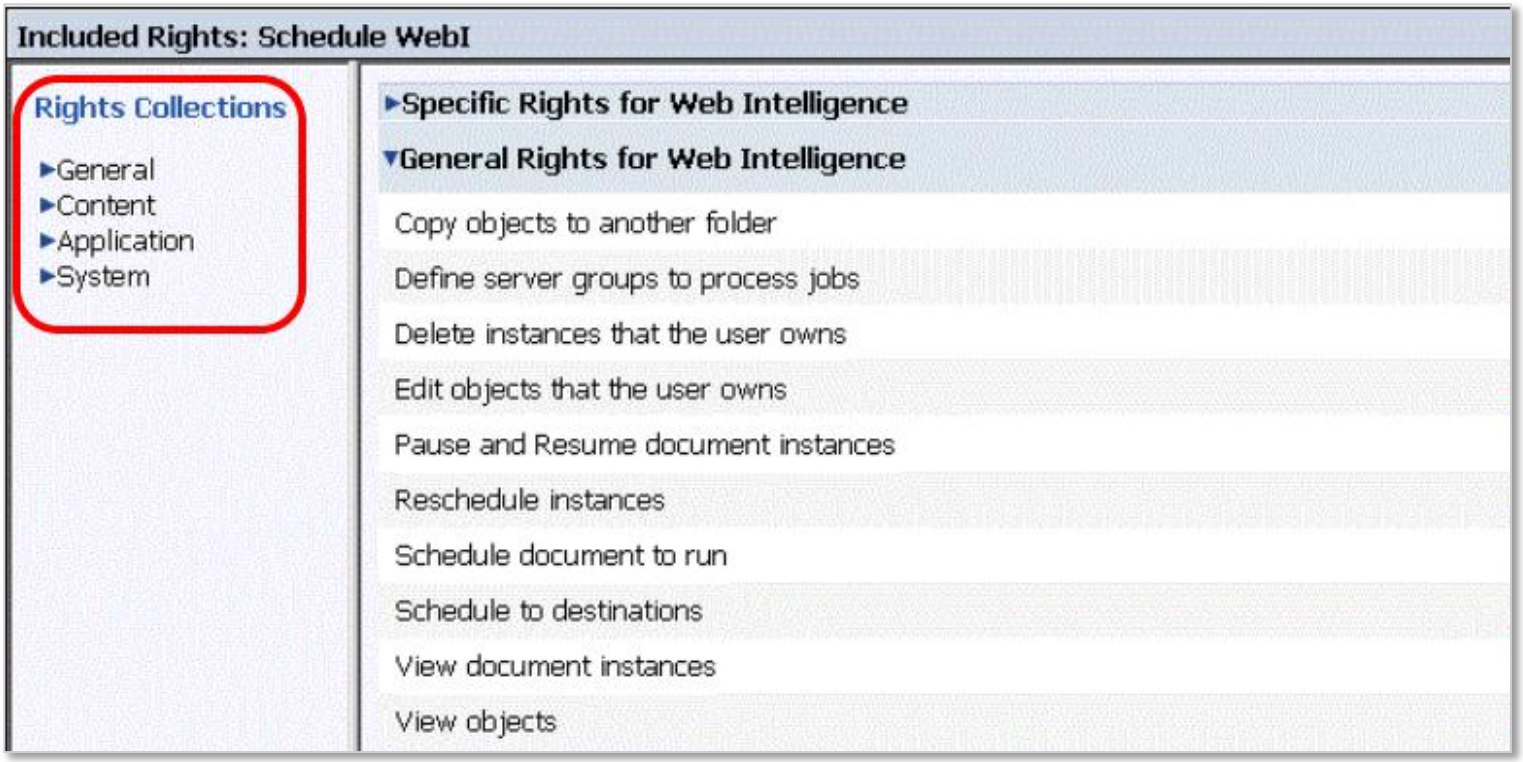


Rights

General rights can be overridden by content specific rights.

Example: Right to Add object granted, right to add Webi object denied.

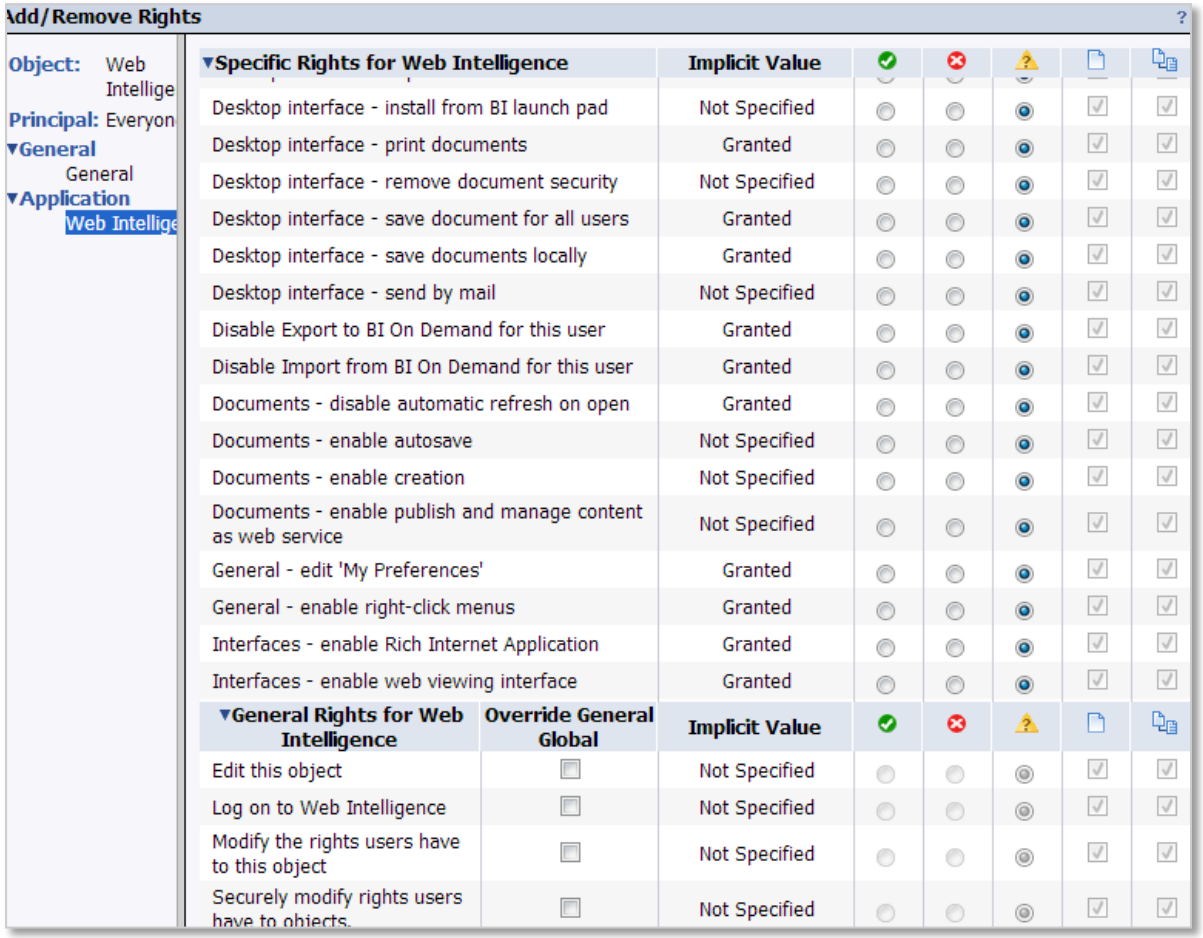
Application rights – example: right to use the webi application



Example of Application rights

Dictates what you can do with the application

You must have rights to the actual object (webi document in this case) to perform actions



Granted, Denied, Not Specified, not sure…?

- **Granted & Denied should be clear, what is not specified?**
  Denied > Granted > Not Specified

- **If a right setting is “Not Specified”, it is denied.**
  - ‘Not permitted unless I say otherwise’

- **Apply to current level or all sublevels**

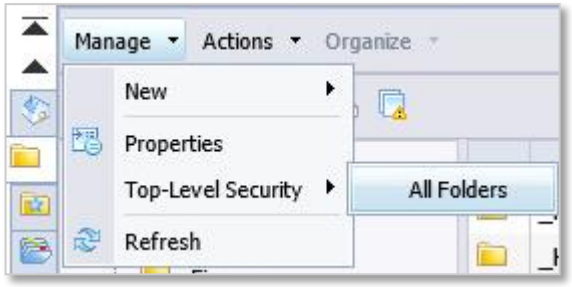
- **Trumping rights**
  - Ex 1: Set grant rights on folder, but explicitly deny right on a single report or subfolder
  - Ex 2: Deny rights on folder, but explicitly grant right on single report or subfolder

Multiple folders for departments, basic permissions

Root public folder is denied by default (secure by default).

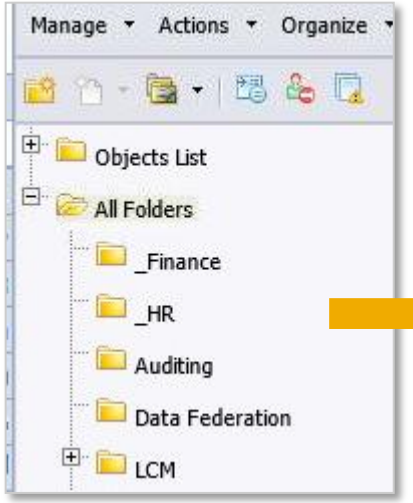
“I have 20 department folders. For each department group, I have to deny permission on 19 folders and grant permission on the single folder. Times 20…”

Example, how do we actually set this up:

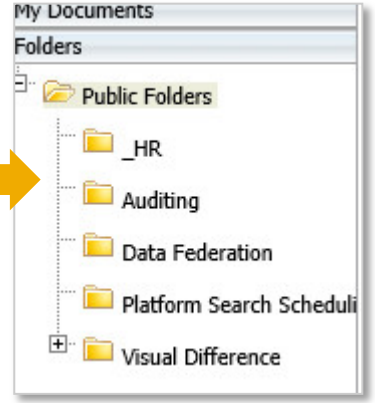


Grant view object but not subjobjects

General Rights for Folder	Override General Global	Implicit Value					
View objects	☑	Not Specified	◉	○	○	☑	☐
View objects that the user owns	☑	Not Specified	◉	○	○	☑	☐



Seen By Administrator



Seen By HRUser

Create access levels from minimal rights to full control

Multiple departments? Consider multi-tenancy tool

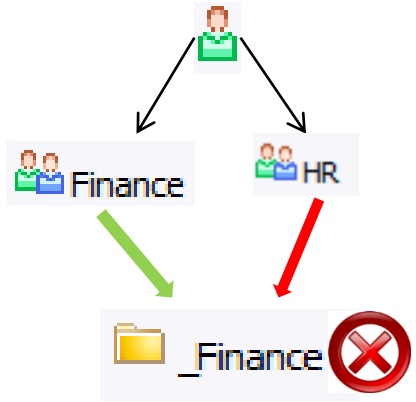
Common roles:

- **Viewers/Consumers**
- **Report creators/Editors**
  - Sometimes split into “Analyst” – user who create or edit reports an “Report Editor” who can publicly edit & modify all reports
- **Report Publisher – scheduling & publishing**

2 Level of inheritance

Groups & Folders

What happens if user is member of 2 groups, one explicitly permits, one explicitly denies?



DENY > GRANT > NOT SPECIFIED

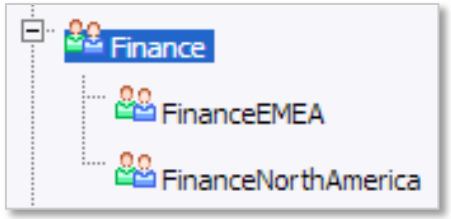
Cheat Sheet:
G + NS = Grant

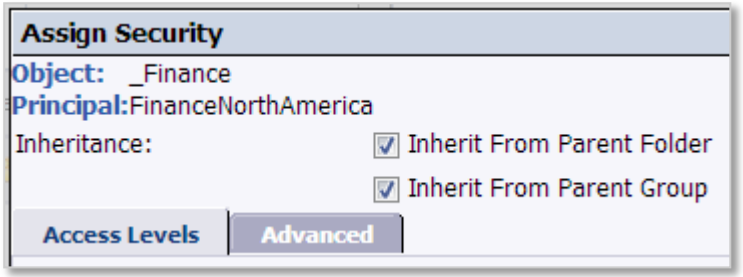
G + D = Deny

G + D + NS = Deny

D + NS = Deny

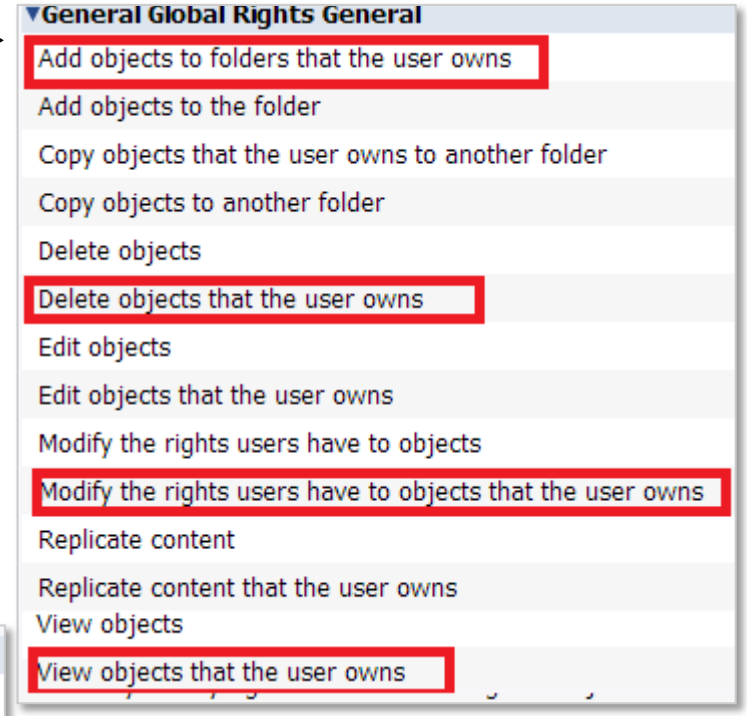
Users & groups also have inheritance





What has changed between 3.x and 4.x

New Owner Right



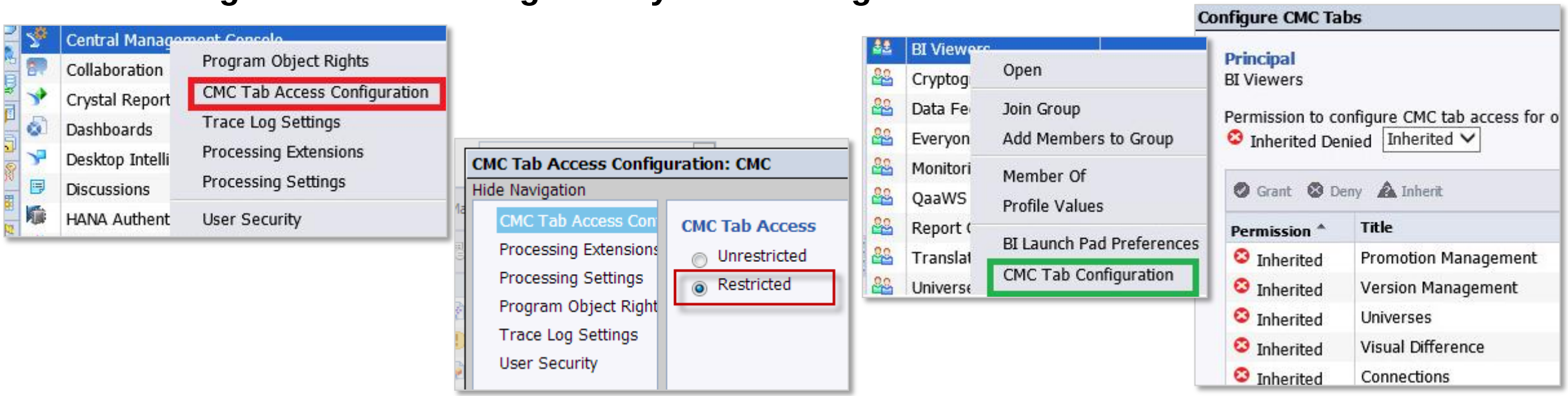
Webi Rights changes/renames
http://wiki.scn.sap.com/wiki/display/BOBJ/WEBI+security+rights+changes+between+XI3.1+and+BI4.x

Connection Download right

CMC tab access

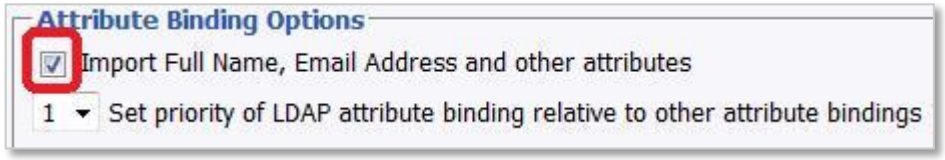
Useful for delegated administration.
http://scn.sap.com/docs/DOC-41311
- Important to note, this is not actual security.

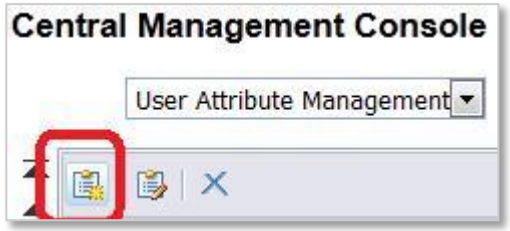
The UI is hidden, but if you do not actually configure rights, a skilled user could still use the SDK to manage & access settings if they have the rights to do so.

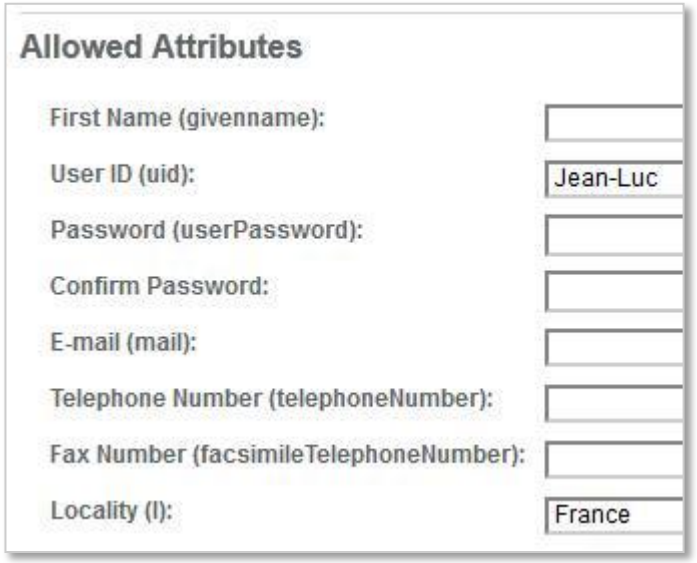


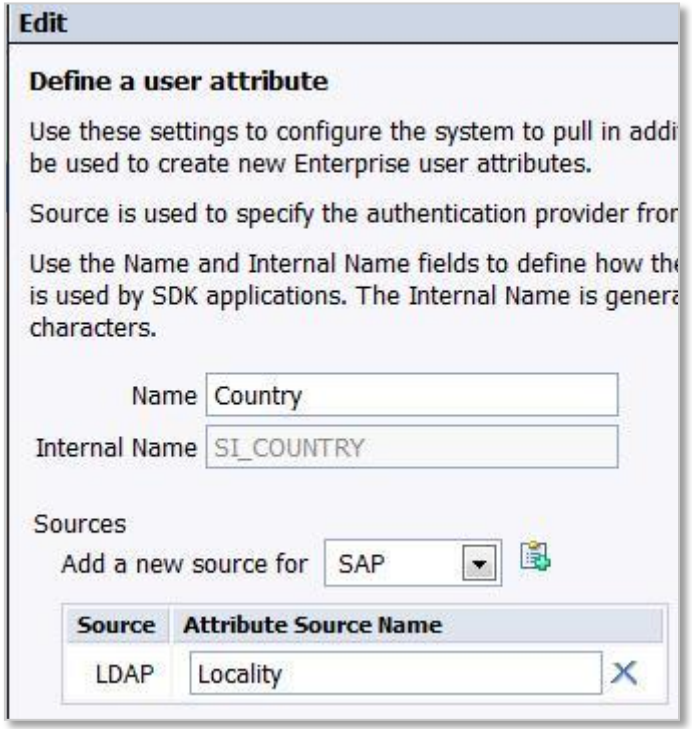
More on universe rights, User attribute mapping 1/2

Custom user attributes can be used to further secure universe

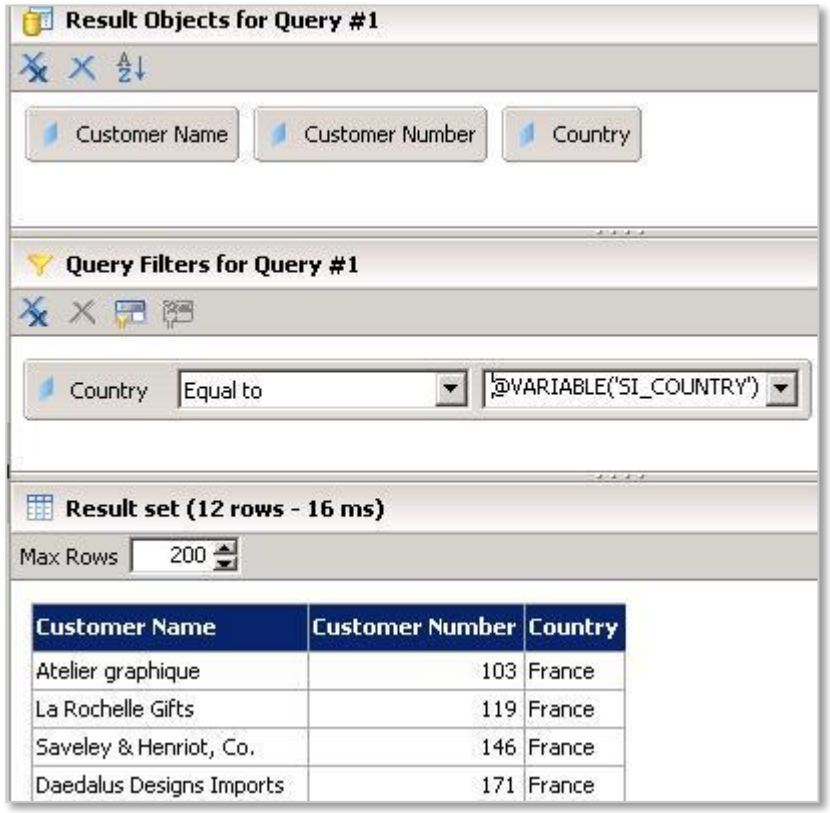


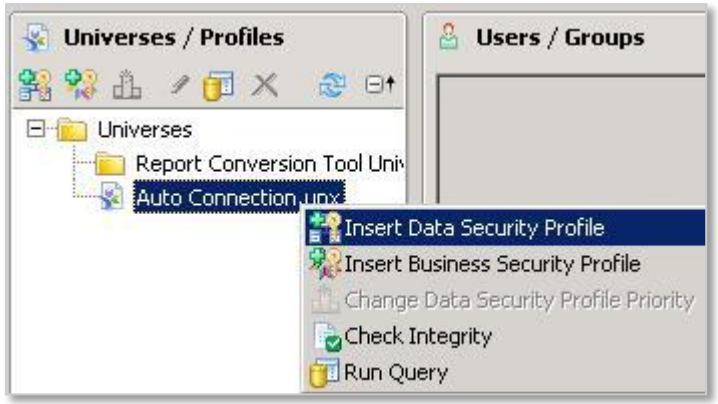


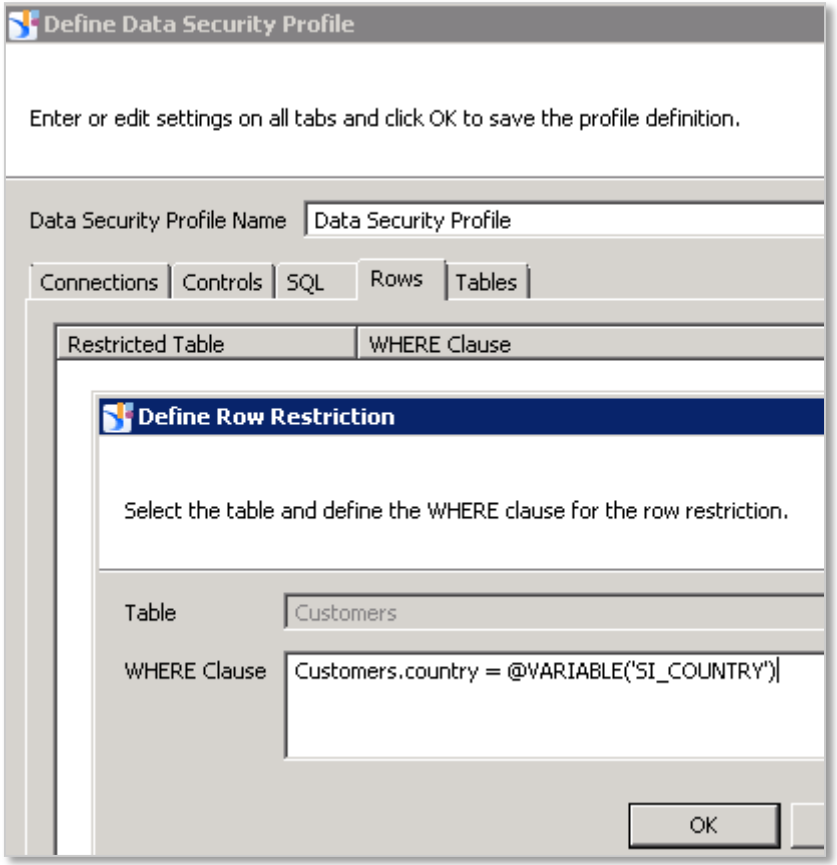




More on universe rights, User attribute mapping 2/2

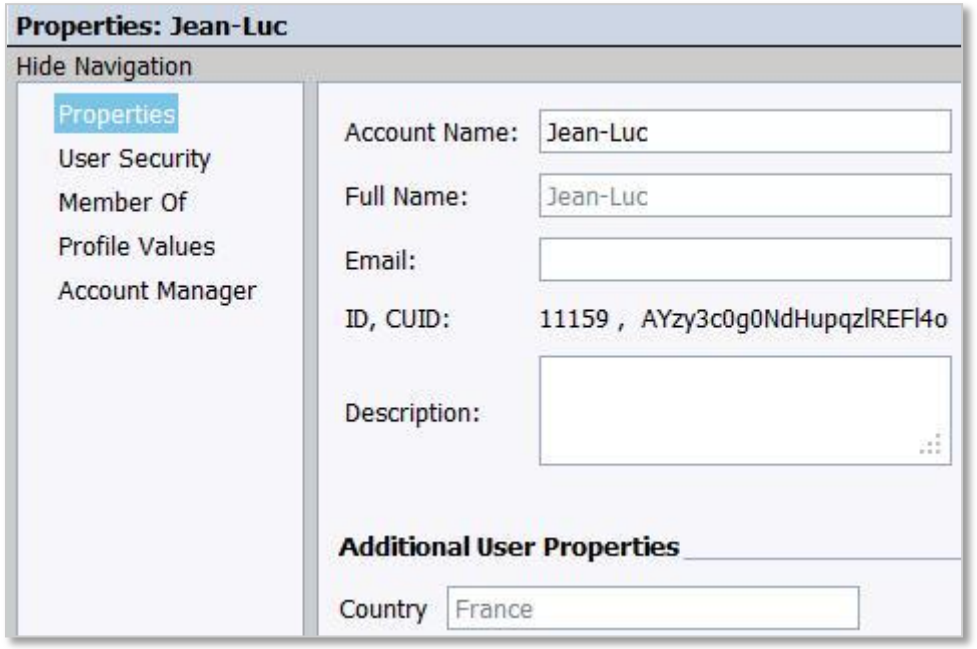


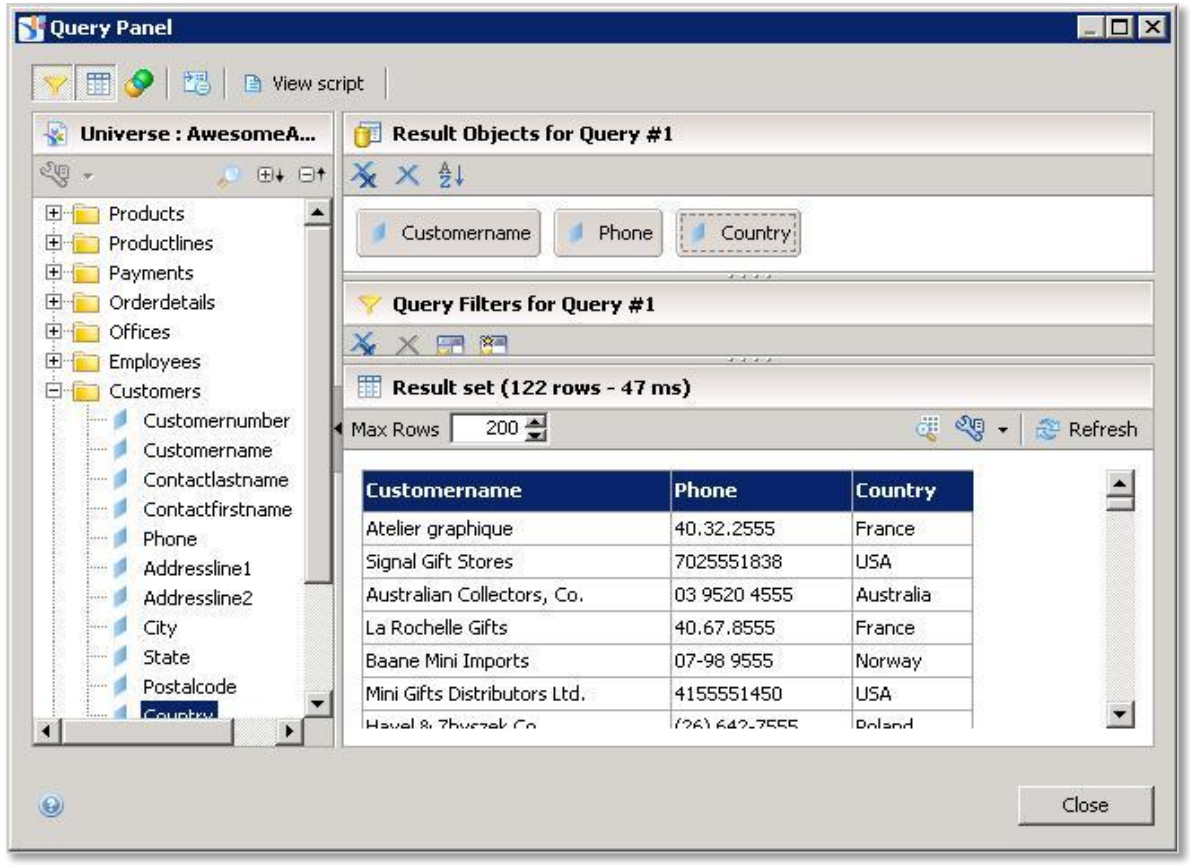




See SCN article on complete how to. http://scn.sap.com/community/bi-platform/blog/2012/07/05/user-attribute-mapping-in-bi4

More on universe rights, User attribute mapping 2/3



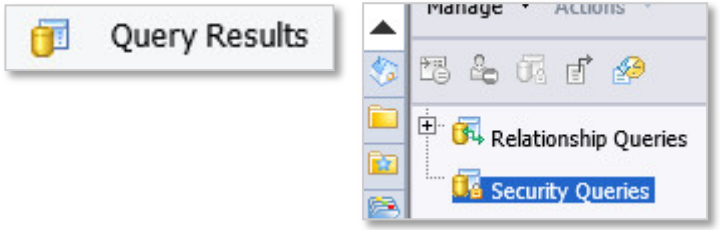


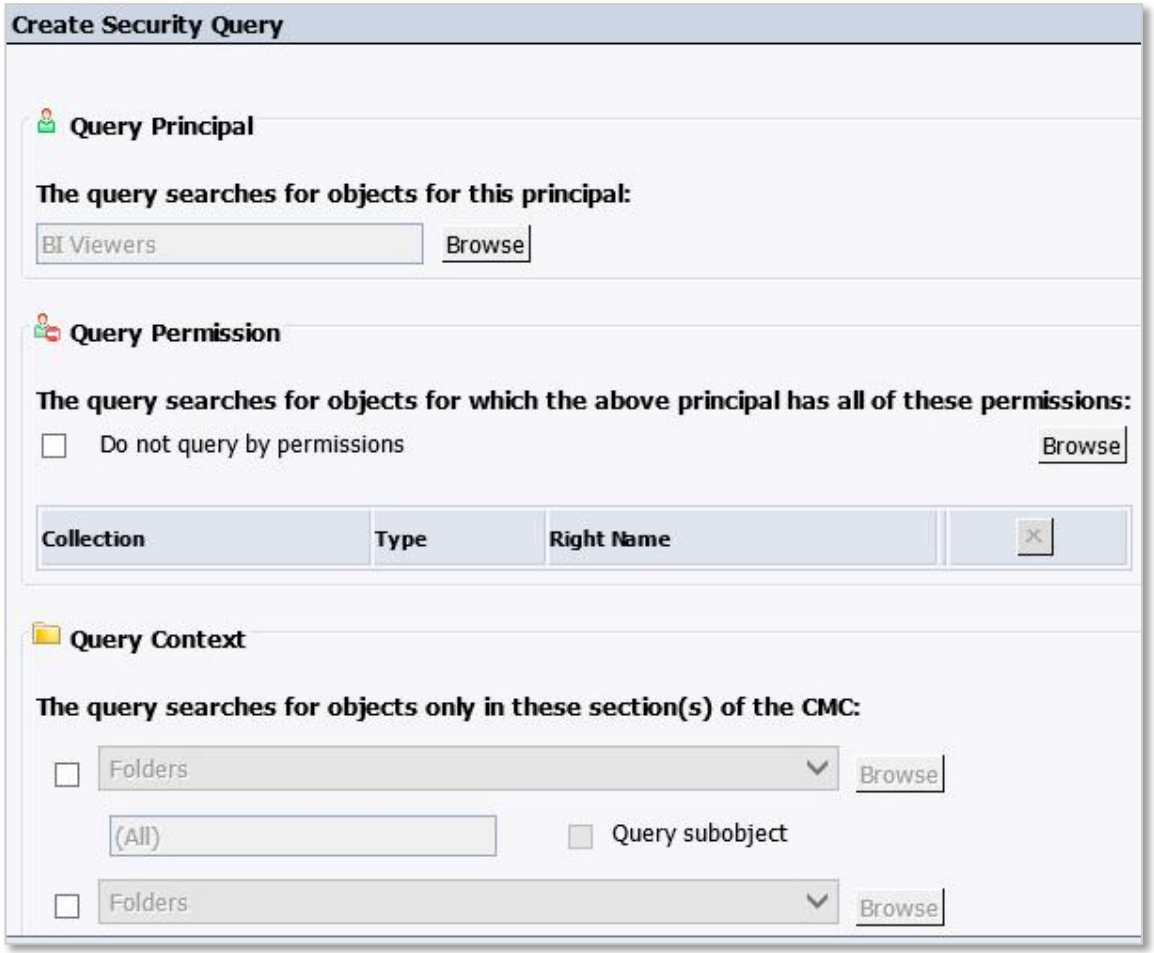
Full how to at:
http://scn.sap.com/community/bi-platform/blog/2012/07/05/user-attribute-mapping-in-bi4

Security Query Tool

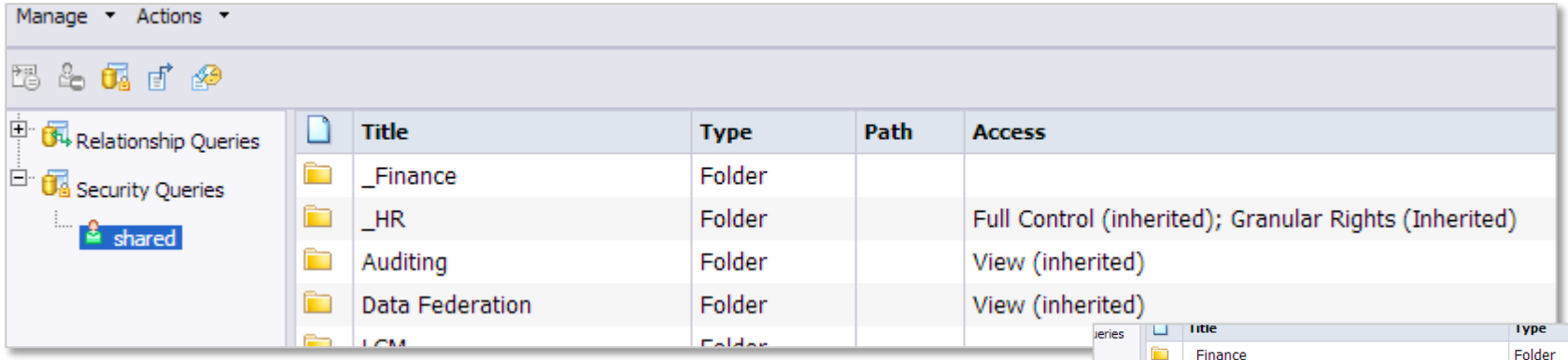
You can see a full listing of rights for a principal (single user or group)

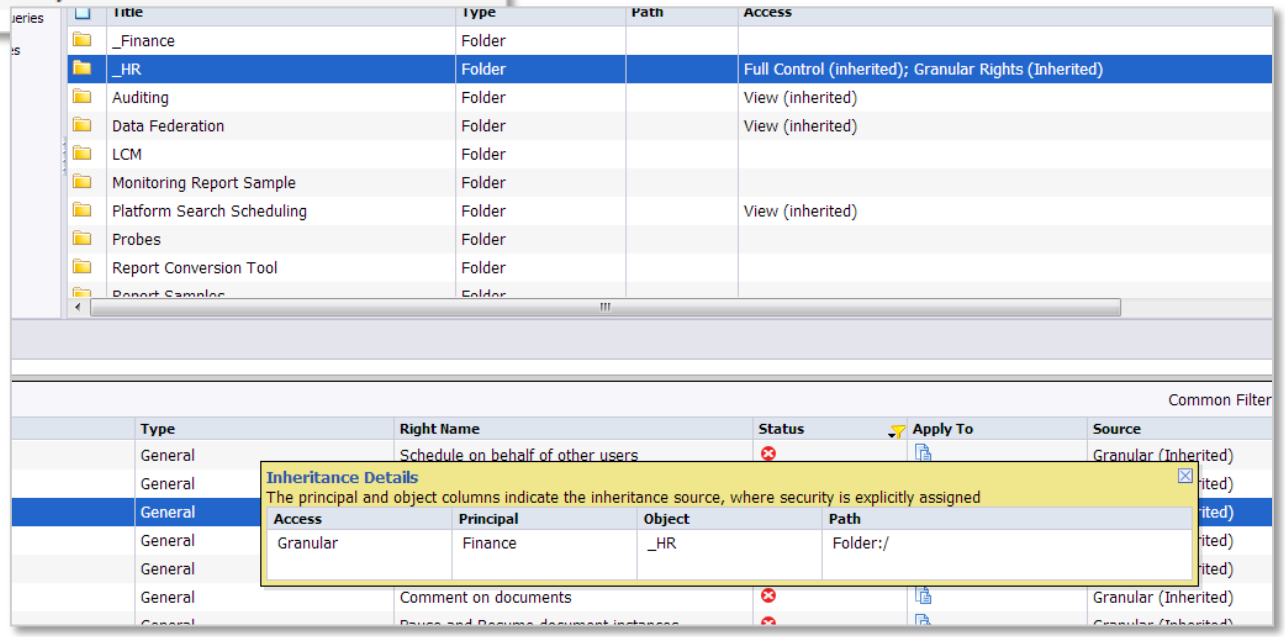
- Useful for debugging
- Export to CSV for compliance
- Can be scripted for more users, there are partners who expose more





Security Query Tool Results





Output lets you drill down (select HR folder, select right, see where the source of the right setting is.

Further Information

SAP Public Web

scn.sap.com

http://scn.sap.com/community/bi-platform/blog/2012/07/05/user-attribute-mapping-in-bi4

http://scn.sap.com/docs/DOC-33875

http://scn.sap.com/docs/DOC-41311

http://wiki.scn.sap.com/wiki/display/BOBJ/WEBI+security+rights+changes+between+XI3.1+and+BI4.x

SAP Education and Certification Opportunities

www.sap.com/education

Watch SAP TechEd Online

www.sapteched.com/online

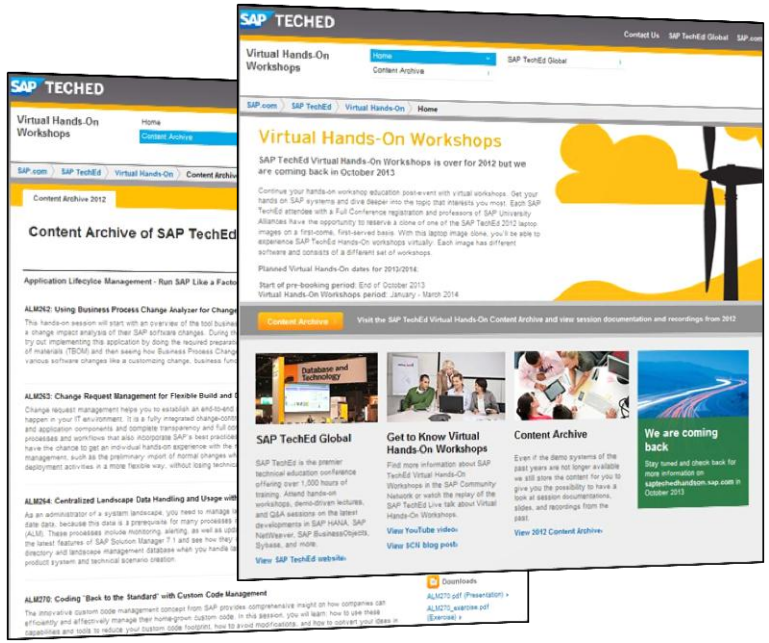
SAP TechEd Virtual Hands-on Workshops and SAP TechEd Online

Continue your SAP TechEd education after the event!

SAP TechEd Virtual Hands-on Workshops

- Access hands-on workshops post-event
- Available January – March 2014
- Complementary with your SAP TechEd registration

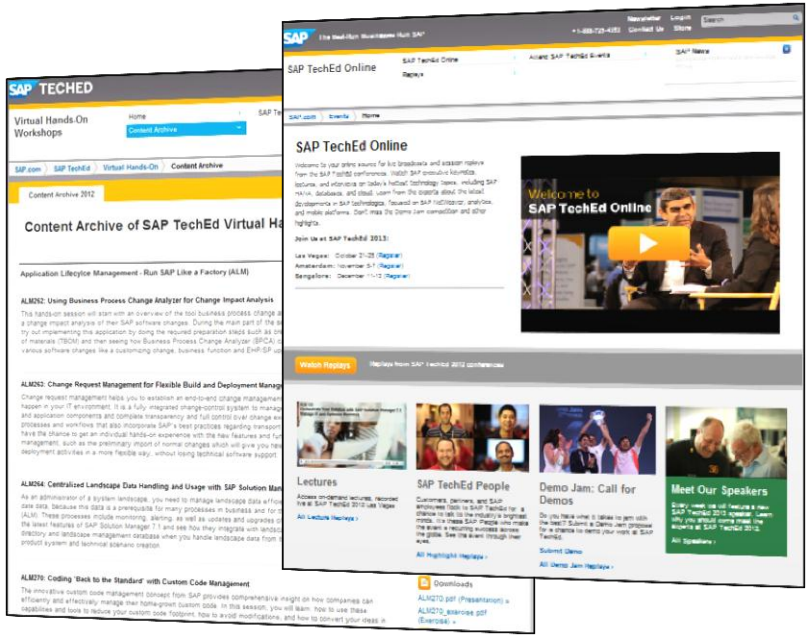
http://saptechedhandson.sap.com/



SAP TechEd Online

- Access replays of keynotes, Demo Jam, SAP TechEd LIVE interviews, select lecture sessions, and more!
- View content only available online

http://sapteched.com/online



Feedback

Please complete your session evaluation for EA209.

Thanks for attending this SAP TechEd session.

© 2013 SAP AG or an SAP affiliate company. All rights reserved.