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

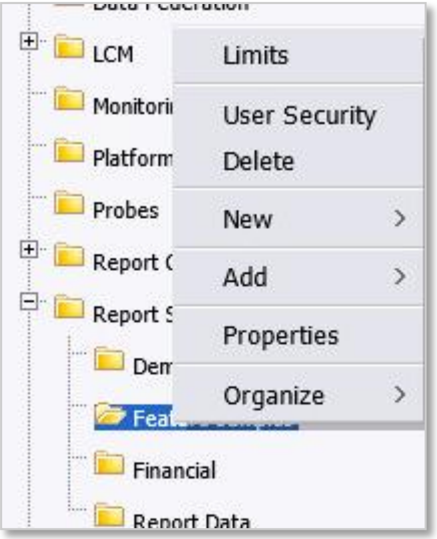
Security changes between 3.1 and 4.x

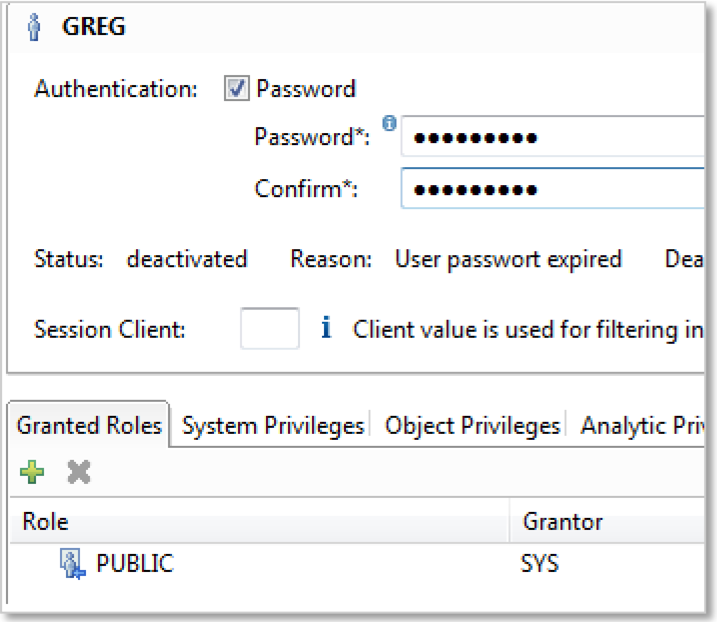
Different levels of security

Data Security

Data can be secured at:

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




GREG

Authentication: ☑ Password

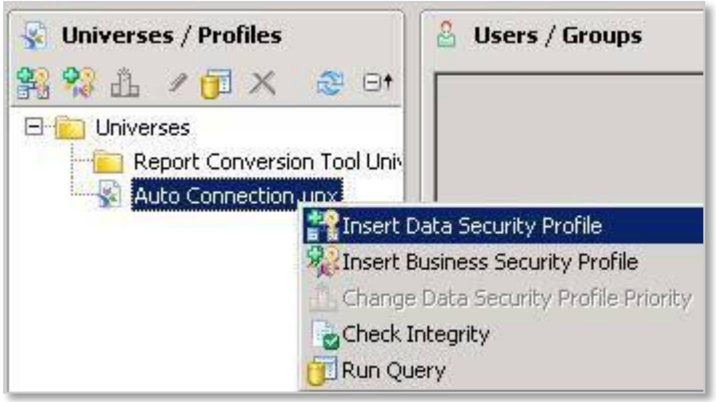
Password*: ●●●●●●●●●

Confirm*: ●●●●●●●●●

Status: deactivated Reason: User password expired Dea

Session Client: i Client value is used for filtering in

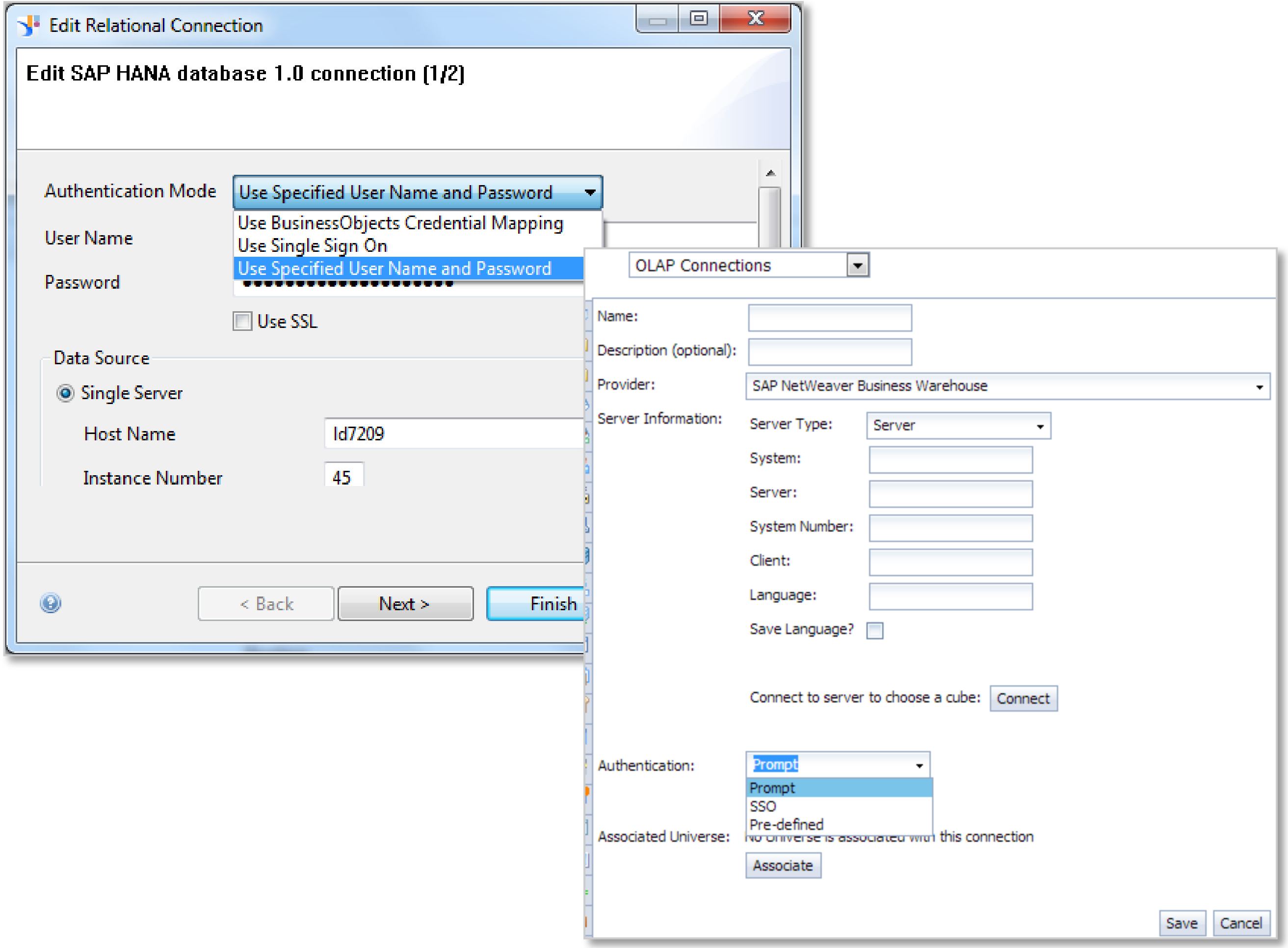
Role	Grantor
PUBLIC	SYS


Universes / Profiles
Users / Groups
Universes
Report Conversion Tool Univ
Auto Connection.unx
Insert Data Security Profile
Insert Business Security Profile
Change Data Security Profile Priority
Check Integrity
Run Query

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*.



Edit Relational Connection

Edit SAP HANA database 1.0 connection (1/2)

Authentication Mode: Use Specified User Name and Password
- Use BusinessObjects Credential Mapping
- Use Single Sign On
- Use Specified User Name and Password

User Name

Password: ••••••••••••••••••••••

□ Use SSL

Data Source

● Single Server

Host Name: ld7209

Instance Number: 45

OLAP Connections

Name:

Description (optional):

Provider: SAP NetWeaver Business Warehouse

Server Information: Server Type: Server

System:

Server:

System Number:

Client:

Language:

Save Language? □

Connect to server to choose a cube:

Authentication: Prompt
- Prompt
- SSO
- Pre-defined

Associated Universe: No universe is associated with this connection

Considerations when creating Connections to data (SSO)

Use Single Sign On

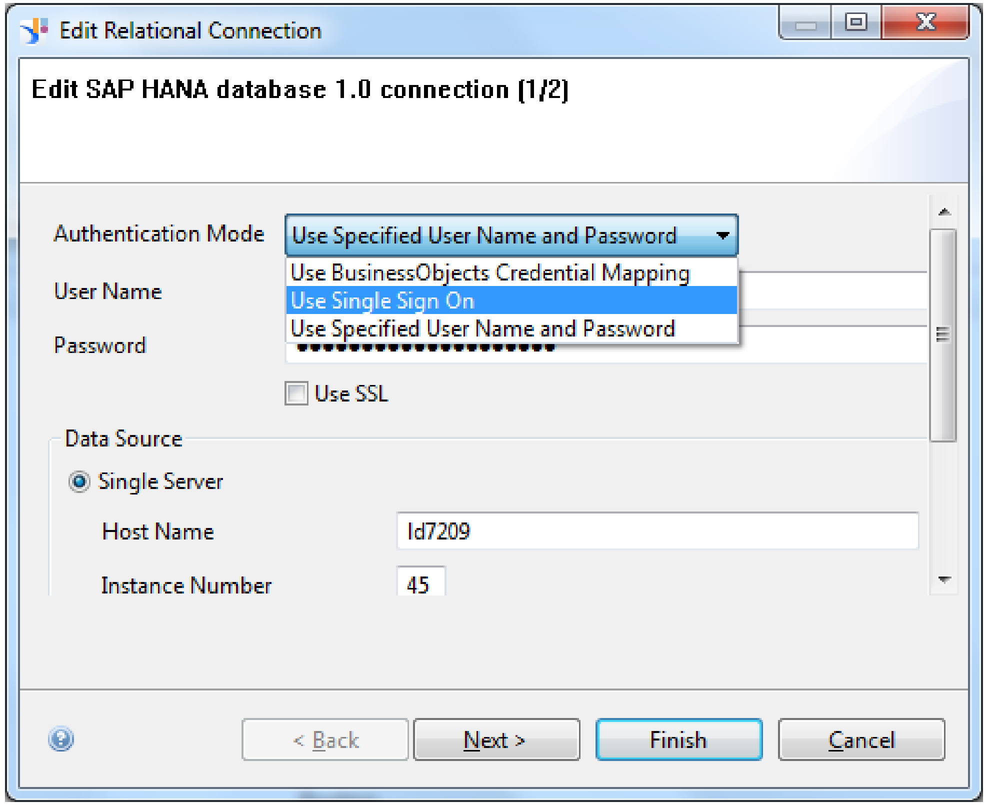
- Kerberos available for
  - MS SQL Server & Analsysis Services
  - Oracle
  - Teradata (as of 4.1 via ODBC)
  - HANA
- Trust Certificates*
  - HANA (internally SAML)
  - SAP

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



Edit Relational Connection

Edit SAP HANA database 1.0 connection (1/2)

Authentication Mode: Use Specified User Name and Password

- Use BusinessObjects Credential Mapping
- Use Single Sign On
- Use Specified User Name and Password

User Name

Password

□ Use SSL

Data Source

● Single Server

Host Name: ld7209

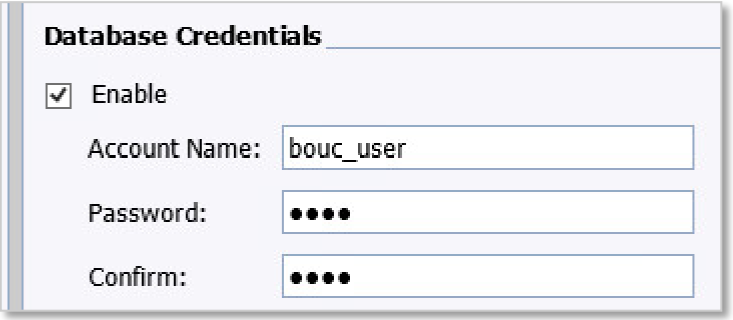
Instance Number: 45

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.



Database Credentials

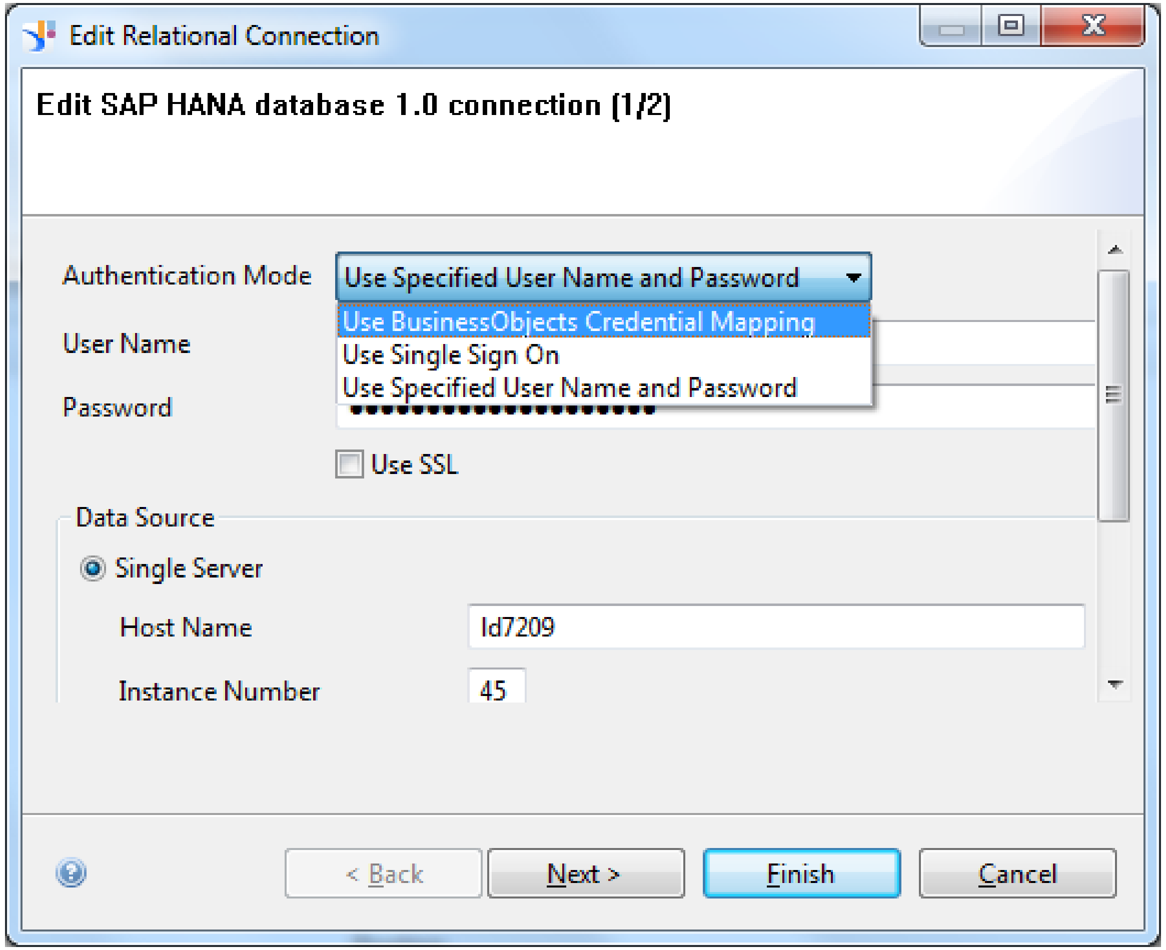
☑ Enable

Account Name: bouc_user

Password: ●●●●

Confirm: ●●●●

- Capture during logon if no SSO or set via SDK



Edit Relational Connection

Edit SAP HANA database 1.0 connection (1/2)

Authentication Mode: Use Specified User Name and Password

- Use BusinessObjects Credential Mapping
- Use Single Sign On
- Use Specified User Name and Password

User Name

Password: ●●●●●●●●●●●●●●●●●●●●

□ Use SSL

Data Source

● Single Server

Host Name: ld7209

Instance Number: 45

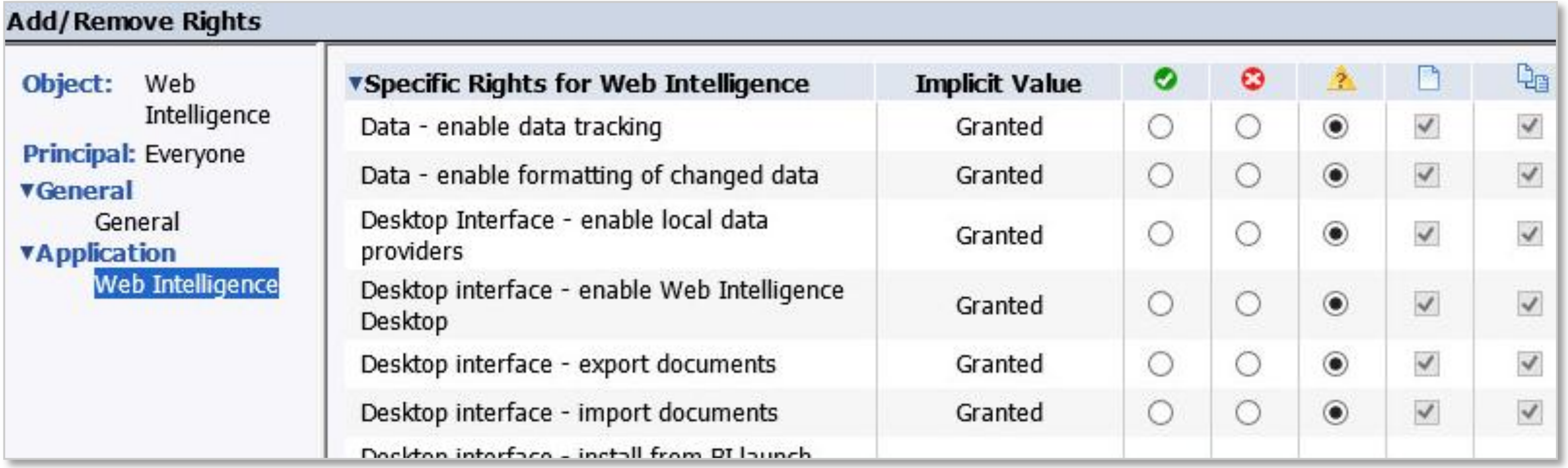
Some help deciding where to secure

- 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



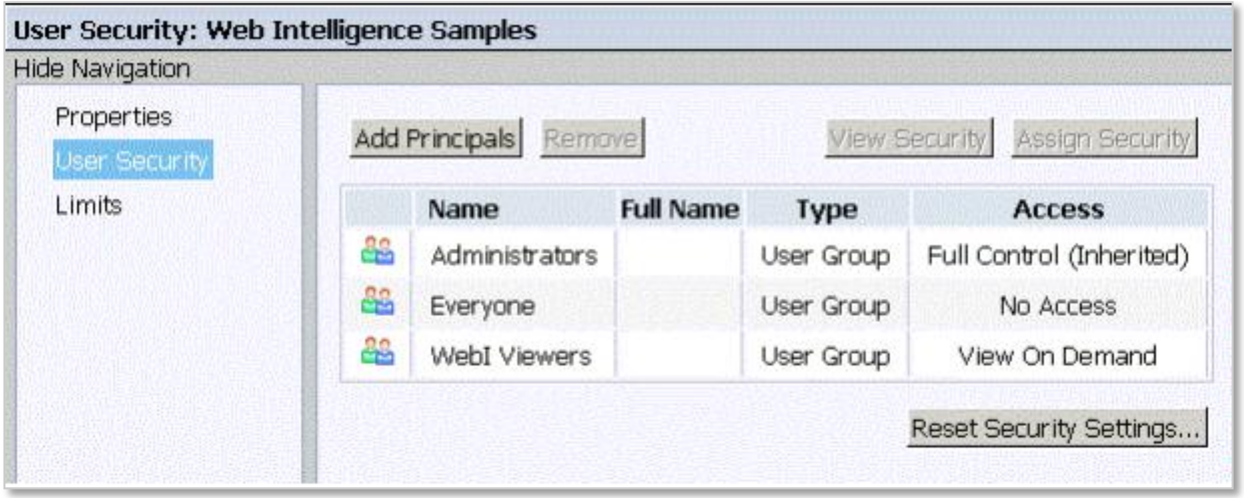
Add/Remove Rights

Object: Web Intelligence
Principal: Everyone
▼**General**
General
▼**Application**
Web Intelligence

▼Specific Rights for Web Intelligence	Implicit Value	✓	✗	⚠	🗋	🗐
Data - enable data tracking	Granted	○	○	●	☑	☑
Data - enable formatting of changed data	Granted	○	○	●	☑	☑
Desktop Interface - enable local data providers	Granted	○	○	●	☑	☑
Desktop interface - enable Web Intelligence Desktop	Granted	○	○	●	☑	☑
Desktop interface - export documents	Granted	○	○	●	☑	☑
Desktop interface - import documents	Granted	○	○	●	☑	☑
Desktop interface - install from BI launch						

Access Control List

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



	Name	Full Name	Type	Access
	Administrators		User Group	Full Control (Inherited)
	Everyone		User Group	No Access
	WebI Viewers		User Group	View On Demand

Access Levels

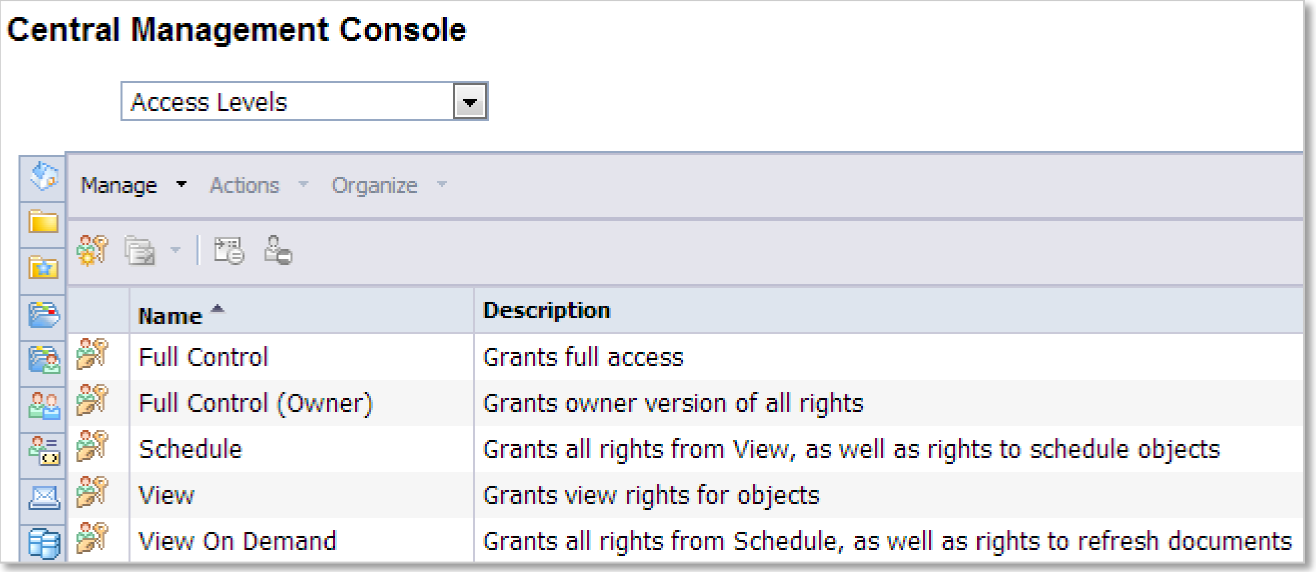
Many rights in the system

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



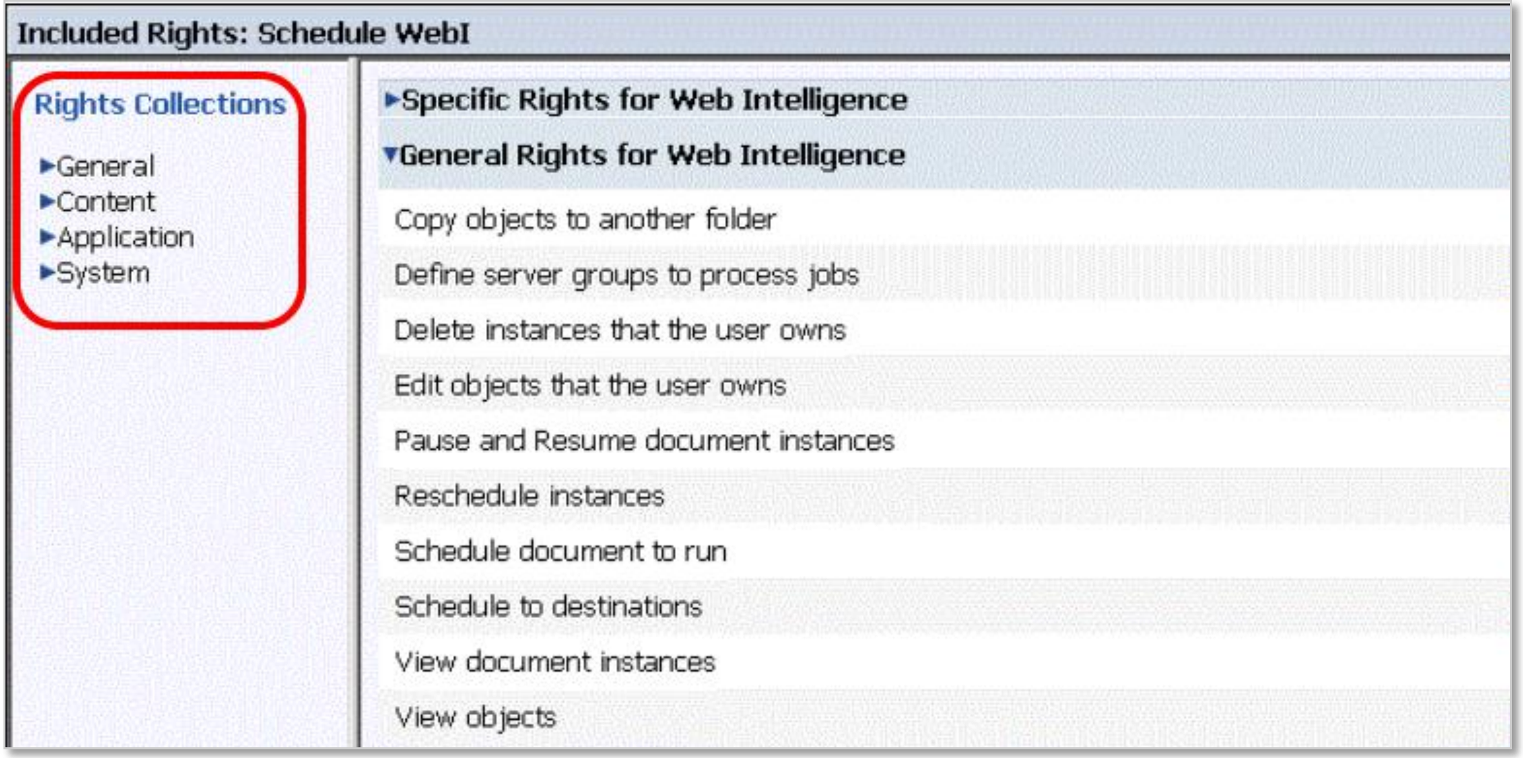
Name	Description
Full Control	Grants full access
Full Control (Owner)	Grants owner version of all rights
Schedule	Grants all rights from View, as well as rights to schedule objects
View	Grants view rights for objects
View On Demand	Grants all rights from Schedule, as well as rights to refresh documents

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



Included Rights: Schedule WebI

Rights Collections

- ▶General
- ▶Content
- ▶Application
- ▶System

▶Specific Rights for Web Intelligence

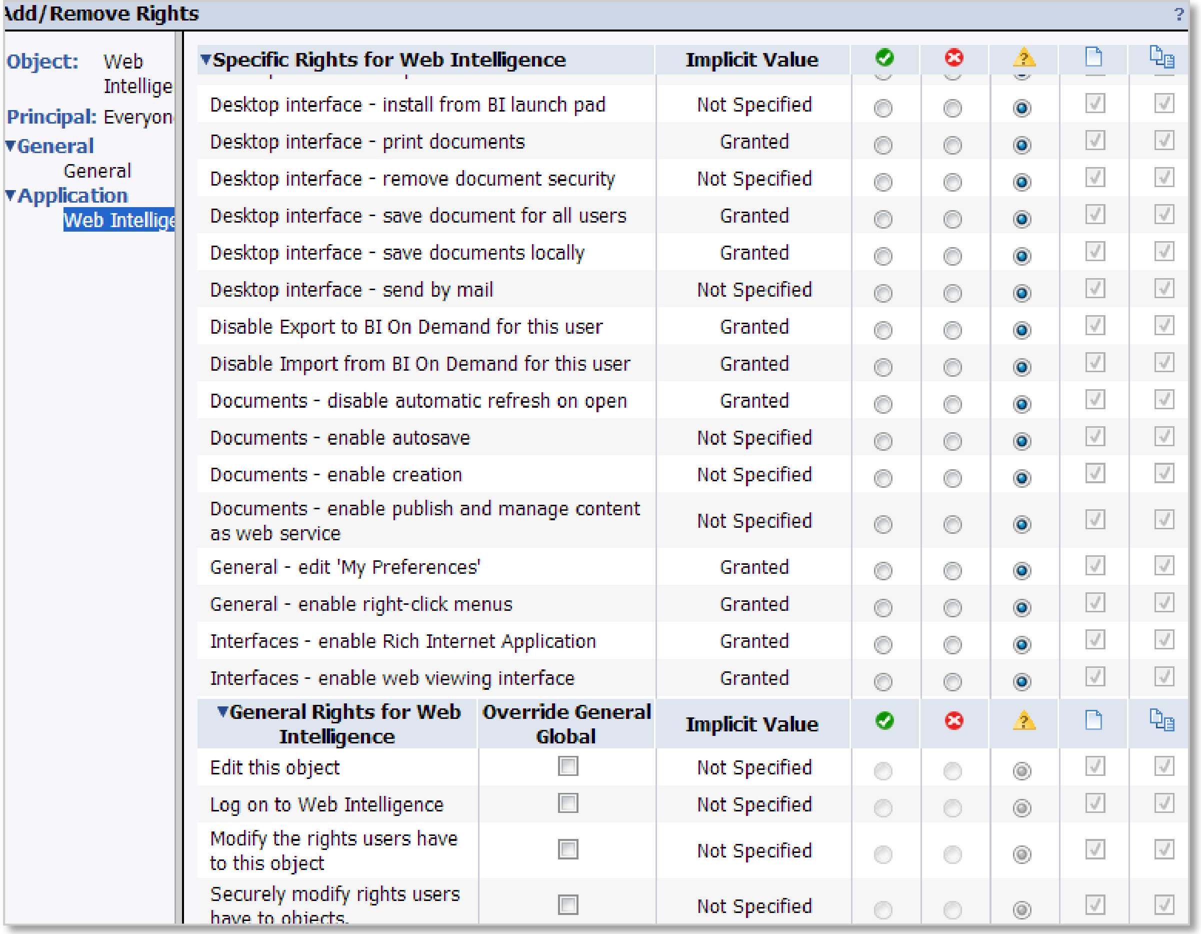
▼General Rights for Web Intelligence

- Copy objects to another folder
- Define server groups to process jobs
- Delete instances that the user owns
- Edit objects that the user owns
- Pause and Resume document instances
- Reschedule instances
- Schedule document to run
- Schedule to destinations
- View document instances
- View objects

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



Add/Remove Rights

Object: Web Intellige

Principal: Everyon

▼**General**

General

▼**Application**

Web Intellige

▼Specific Rights for Web Intelligence	Implicit Value	✓	✗	⚠	🗎	🗐
Desktop interface - install from BI launch pad	Not Specified	○	○	●	☑	☑
Desktop interface - print documents	Granted	○	○	●	☑	☑
Desktop interface - remove document security	Not Specified	○	○	●	☑	☑
Desktop interface - save document for all users	Granted	○	○	●	☑	☑
Desktop interface - save documents locally	Granted	○	○	●	☑	☑
Desktop interface - send by mail	Not Specified	○	○	●	☑	☑
Disable Export to BI On Demand for this user	Granted	○	○	●	☑	☑
Disable Import from BI On Demand for this user	Granted	○	○	●	☑	☑
Documents - disable automatic refresh on open	Granted	○	○	●	☑	☑
Documents - enable autosave	Not Specified	○	○	●	☑	☑
Documents - enable creation	Not Specified	○	○	●	☑	☑
Documents - enable publish and manage content as web service	Not Specified	○	○	●	☑	☑
General - edit 'My Preferences'	Granted	○	○	●	☑	☑
General - enable right-click menus	Granted	○	○	●	☑	☑
Interfaces - enable Rich Internet Application	Granted	○	○	●	☑	☑
Interfaces - enable web viewing interface	Granted	○	○	●	☑	☑

▼General Rights for Web Intelligence	Override General Global	Implicit Value	✓	✗	⚠	🗎	🗐
Edit this object	□	Not Specified	○	○	●	☑	☑
Log on to Web Intelligence	□	Not Specified	○	○	●	☑	☑
Modify the rights users have to this object	□	Not Specified	○	○	●	☑	☑
Securely modify rights users have to objects.	□	Not Specified	○	○	●	☑	☑

Granted, Denied, Not Specified, not sure…?

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

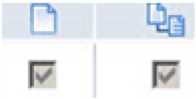
✓ = granted

✗ = denied

⚠ = 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**



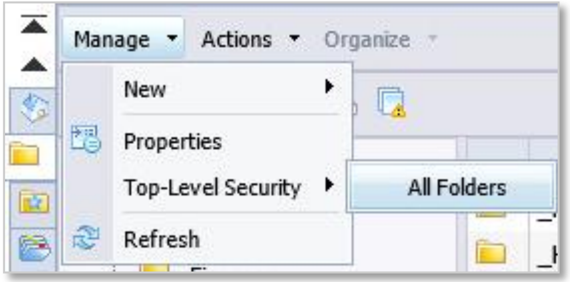
- **Trumping rights**
  - Ex 1: Set grant rights on folder, but explicitly deny right on a single report or subfolder
  - Ex 2: Deny rights on folder, but explicitly grant right on single report or subfolder

Multiple folders for departments, basic permissions

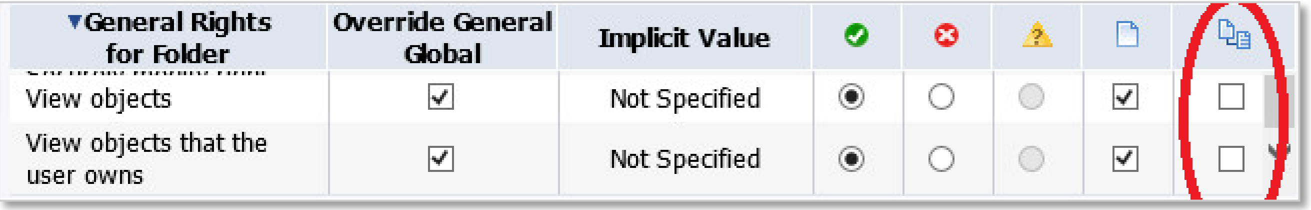
Root public folder is denied by default (secure by default).

“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…”

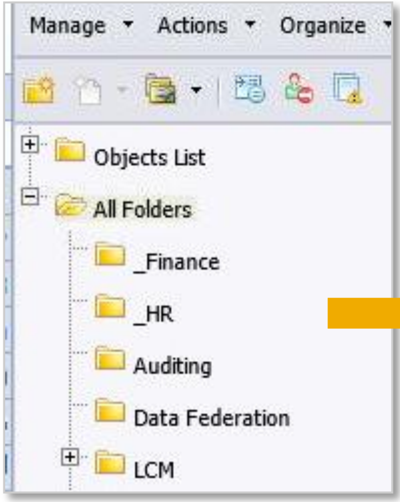
Example, how do we actually set this up:



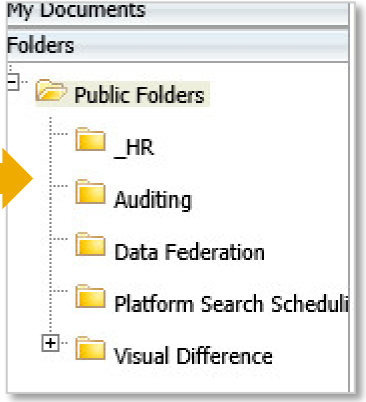
Grant view object but not subjobjects



▾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

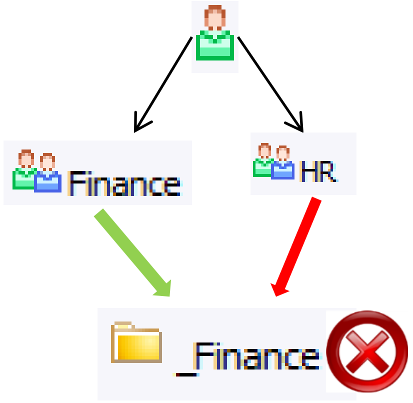
Common roles:

- **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

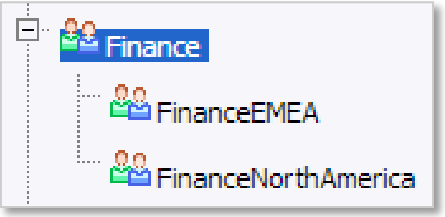
Cheat Sheet:
G + NS = Grant

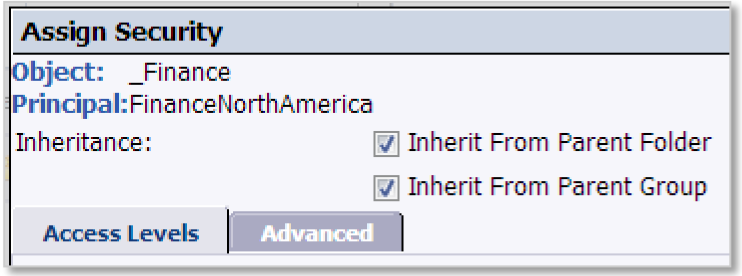
G + D = Deny

G + D + NS = Deny

D + NS = Deny

Users & groups also have inheritance





Assign Security

Object: _Finance

Principal: FinanceNorthAmerica

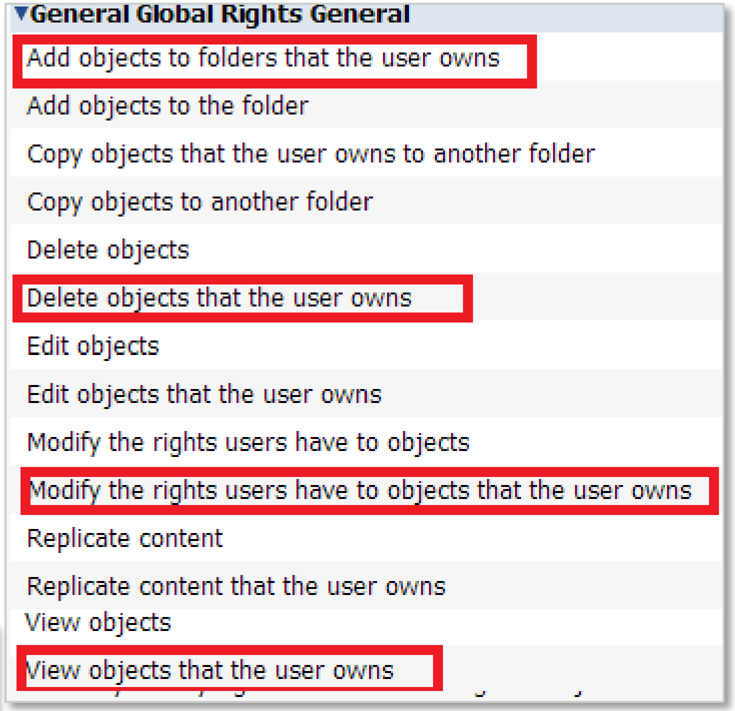
Inheritance: ☑ Inherit From Parent Folder

☑ Inherit From Parent Group

What has changed between 3.x and 4.x

New Owner Right

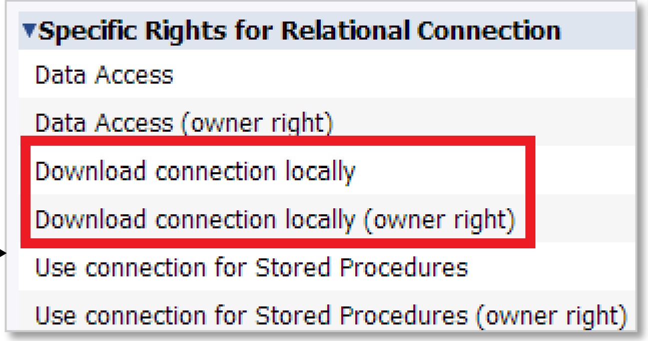
Webi Rights changes/renames
http://wiki.scn.sap.com/wiki/display/BOBJ/WEBI+security+rights+changes+between+XI3.1+and+BI4.x



▾General Global Rights General

- Add objects to folders that the user owns
- Add objects to the folder
- Copy objects that the user owns to another folder
- Copy objects to another folder
- Delete objects
- Delete objects that the user owns
- Edit objects
- Edit objects that the user owns
- Modify the rights users have to objects
- Modify the rights users have to objects that the user owns
- Replicate content
- Replicate content that the user owns
- View objects
- View objects that the user owns

Connection Download right



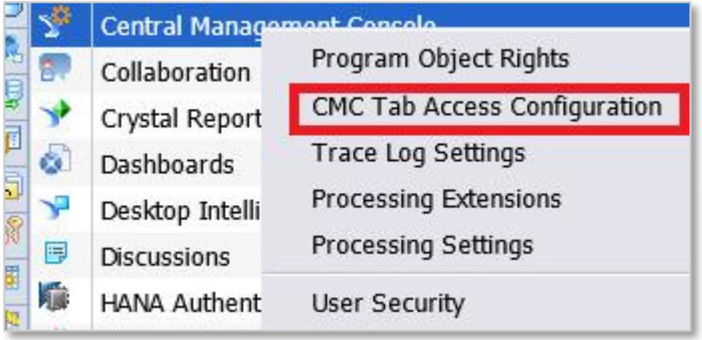
▾Specific Rights for Relational Connection

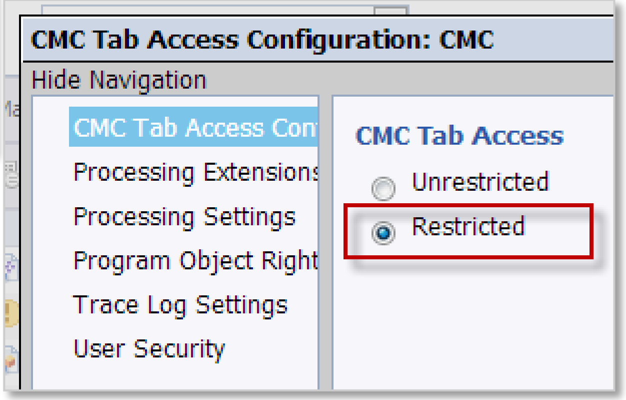
- Data Access
- Data Access (owner right)
- Download connection locally
- Download connection locally (owner right)
- Use connection for Stored Procedures
- Use connection for Stored Procedures (owner right)

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.

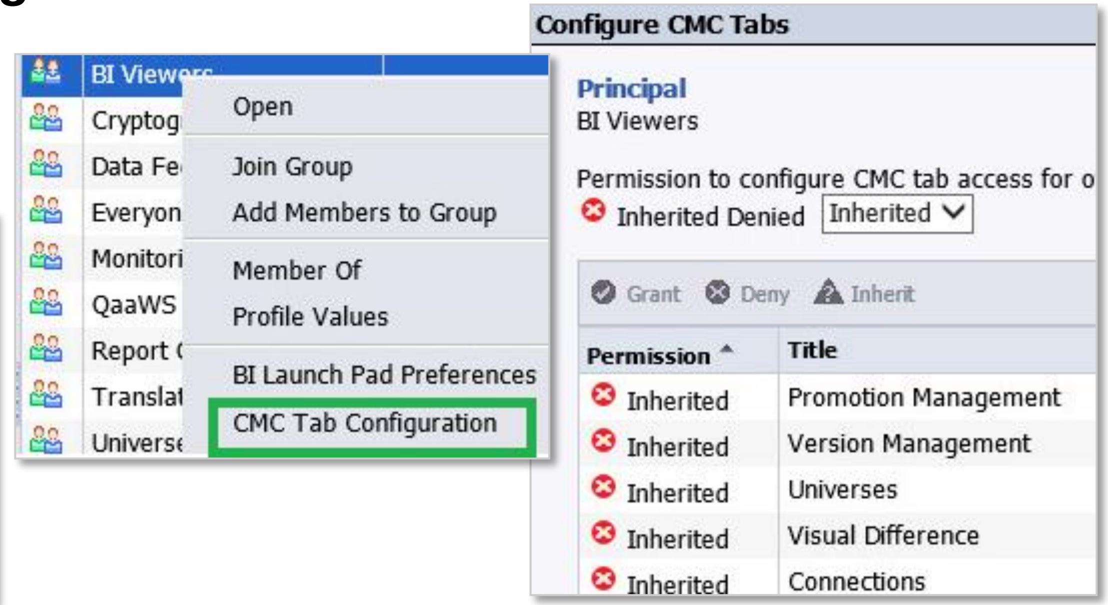




CMC Tab Access Configuration: CMC

CMC Tab Access

○ Unrestricted
● Restricted



Configure CMC Tabs

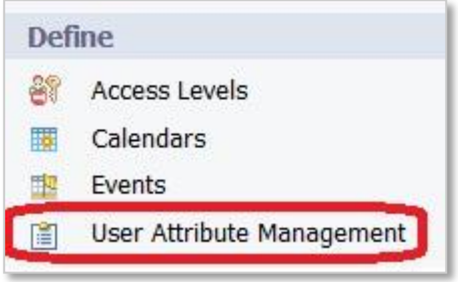
Principal
BI Viewers

Permission to configure CMC tab access for o
⊗ Inherited Denied Inherited

Permission	Title
⊗ Inherited	Promotion Management
⊗ Inherited	Version Management
⊗ Inherited	Universes
⊗ Inherited	Visual Difference
⊗ Inherited	Connections

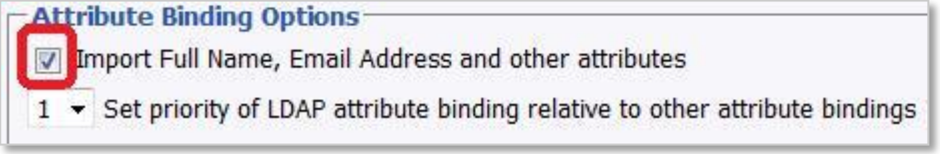
More on universe rights, User attribute mapping 1/2

Custom user attributes can be used to further secure universe



Define

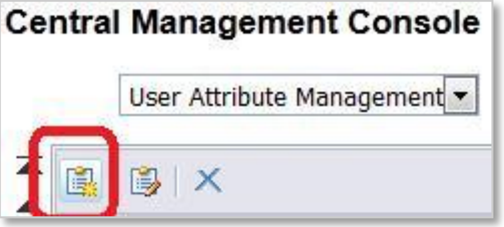
- Access Levels
- Calendars
- Events
- User Attribute Management



Attribute Binding Options

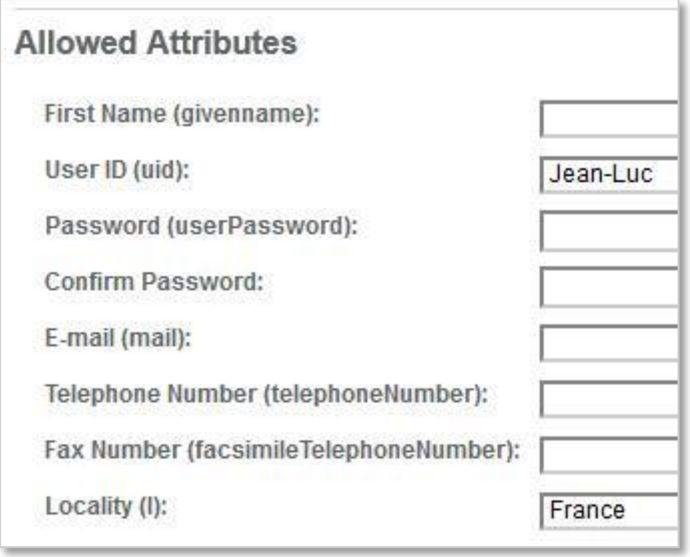
☑ Import Full Name, Email Address and other attributes

1 ▾ Set priority of LDAP attribute binding relative to other attribute bindings



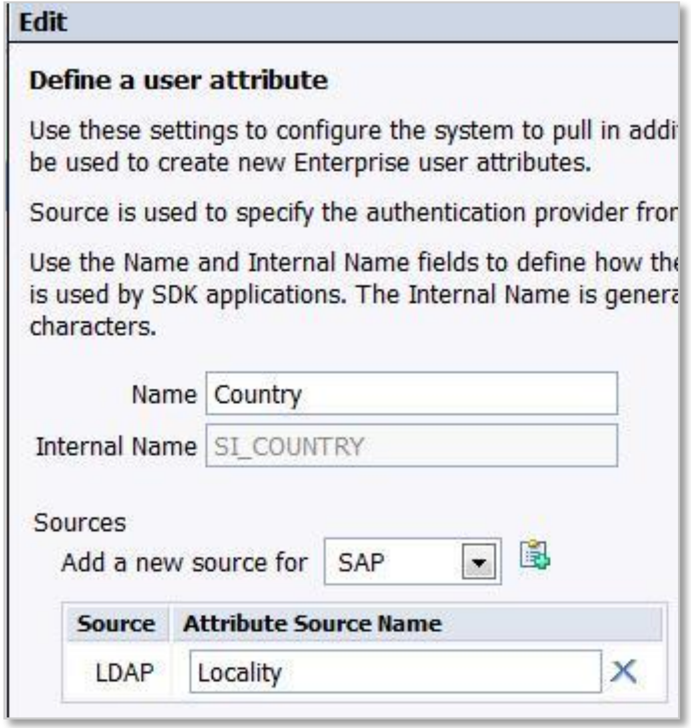
Central Management Console

User Attribute Management ▾



Allowed Attributes

First Name (givenname):	
User ID (uid):	Jean-Luc
Password (userPassword):	
Confirm Password:	
E-mail (mail):	
Telephone Number (telephoneNumber):	
Fax Number (facsimileTelephoneNumber):	
Locality (l):	France



Edit

Define a user attribute

Use these settings to configure the system to pull in addi be used to create new Enterprise user attributes.

Source is used to specify the authentication provider fror

Use the Name and Internal Name fields to define how the is used by SDK applications. The Internal Name is genera characters.

Name: Country

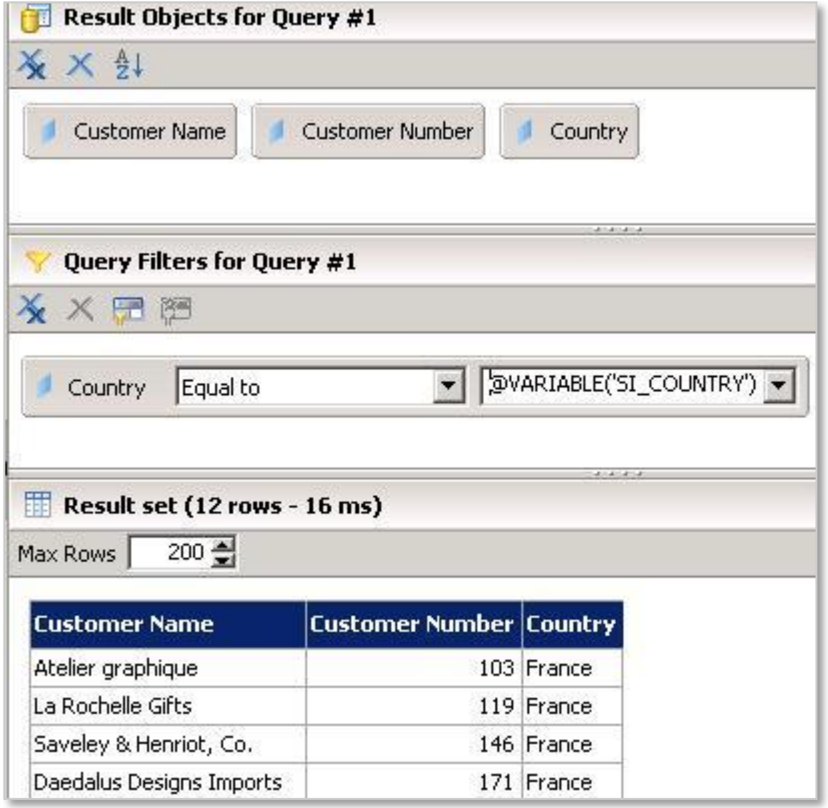
Internal Name: SI_COUNTRY

Sources

Add a new source for SAP ▾

Source	Attribute Source Name
LDAP	Locality

More on universe rights, User attribute mapping 2/2



Result Objects for Query #1

Customer Name | Customer Number | Country

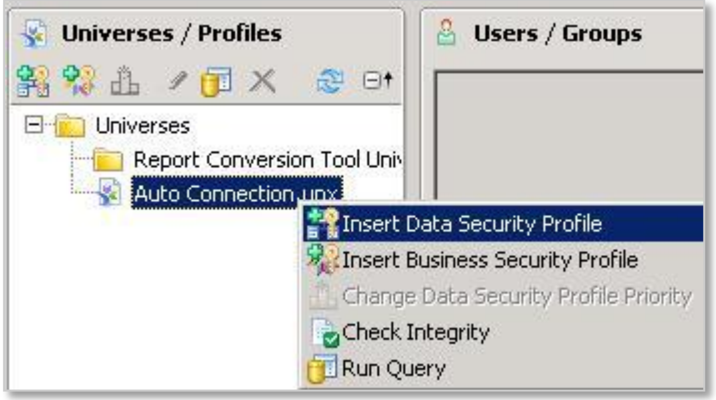
Query Filters for Query #1

Country | Equal to | @VARIABLE('SI_COUNTRY')

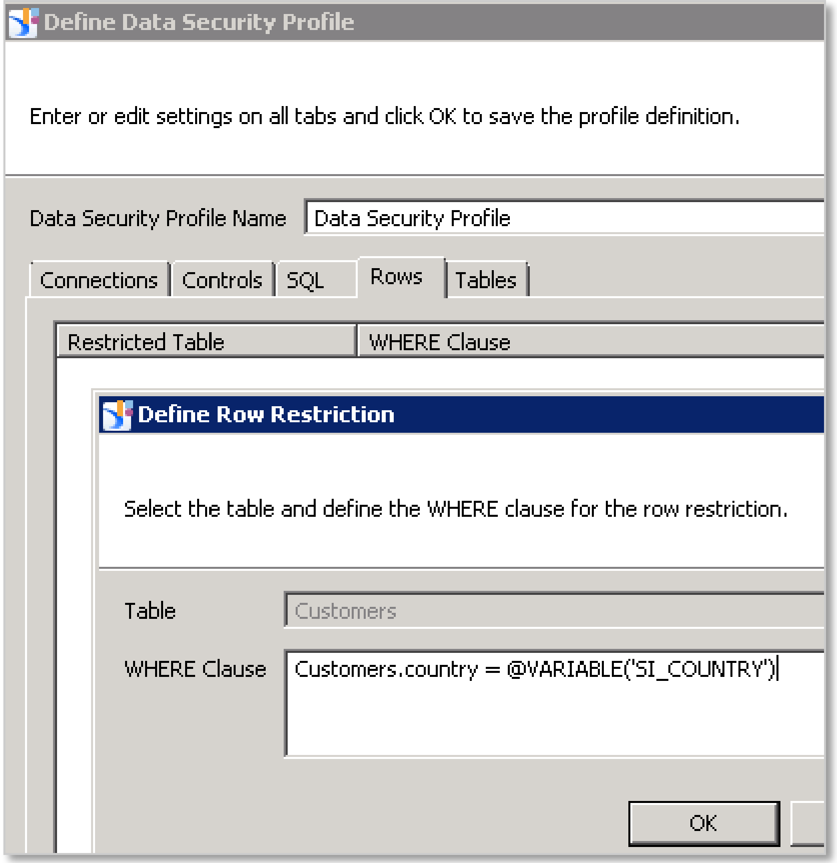
Result set (12 rows - 16 ms)

Max Rows: 200

Customer Name	Customer Number	Country
Atelier graphique	103	France
La Rochelle Gifts	119	France
Saveley & Henriot, Co.	146	France
Daedalus Designs Imports	171	France



Universes / Profiles
Users / Groups
Universes
Report Conversion Tool Univ
Auto Connection.unx
Insert Data Security Profile
Insert Business Security Profile
Change Data Security Profile Priority
Check Integrity
Run Query



Define Data Security Profile

Enter or edit settings on all tabs and click OK to save the profile definition.

Data Security Profile Name: Data Security Profile

Define Row Restriction

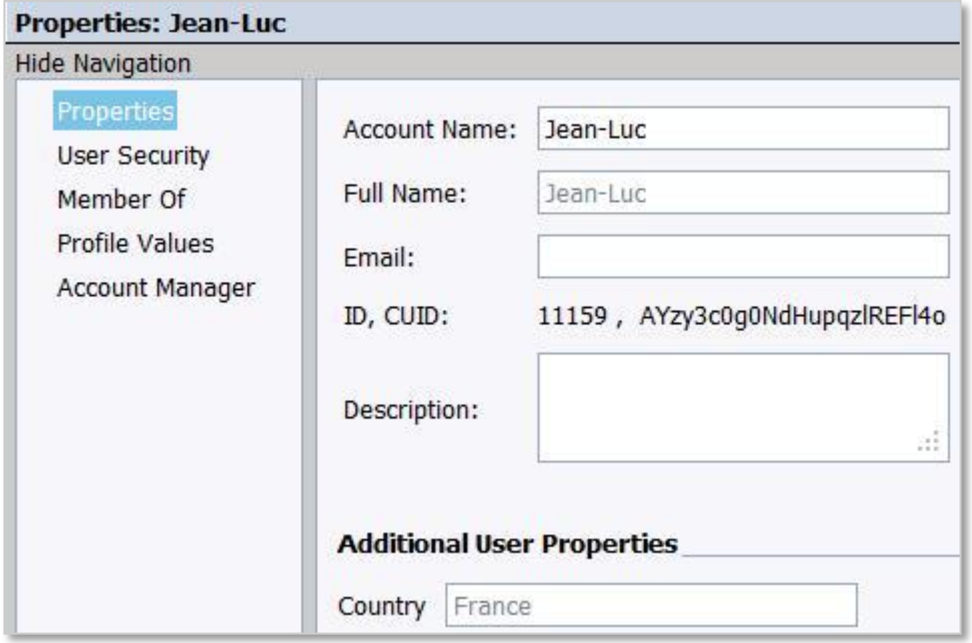
Select the table and define the WHERE clause for the row restriction.

Table: Customers

WHERE Clause: Customers.country = @VARIABLE('SI_COUNTRY')

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

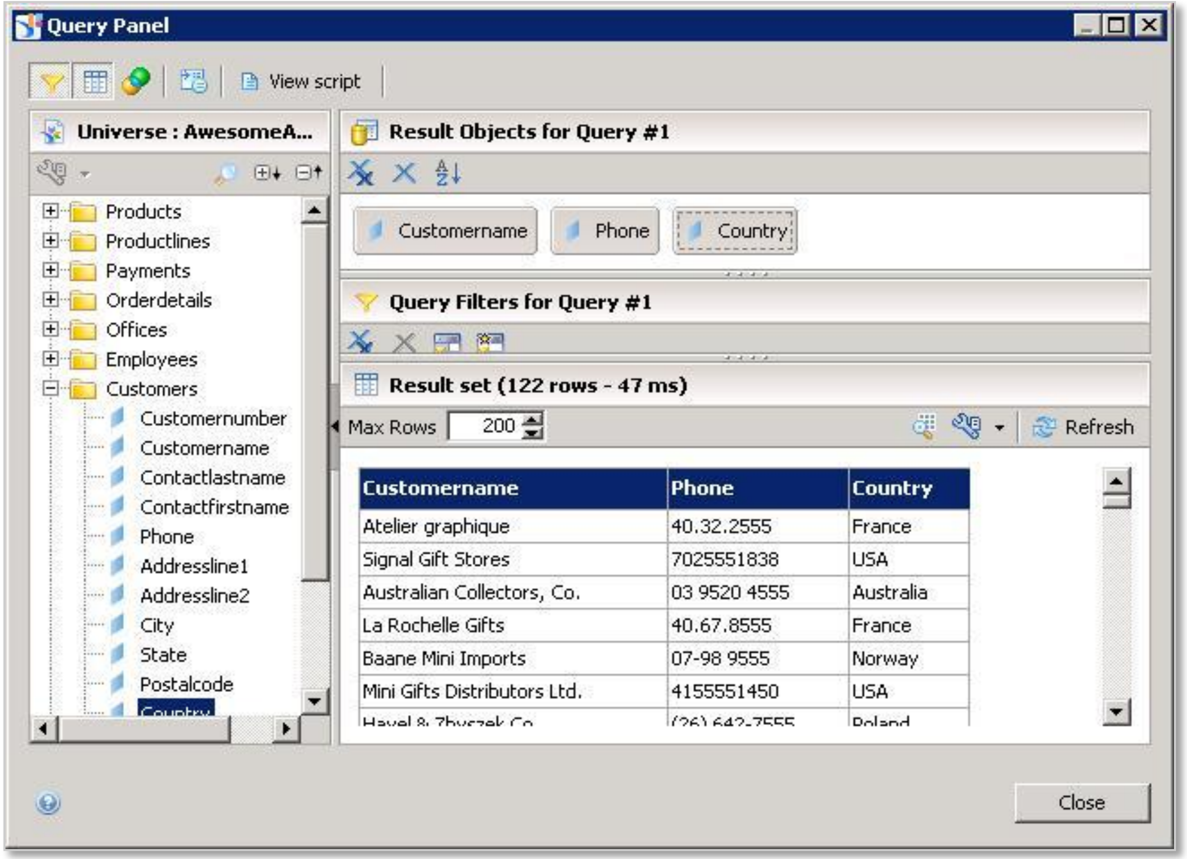


Properties: Jean-Luc

Account Name:	Jean-Luc
Full Name:	Jean-Luc
Email:	
ID, CUID:	11159 , AYzy3c0g0NdHupqzlREFl4o
Description:	

Additional User Properties

Country	France



Result set (122 rows - 47 ms)

Max Rows 200

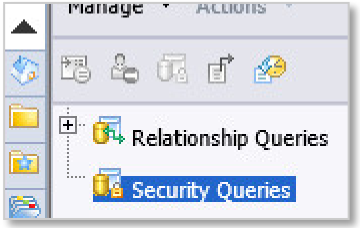
Customername	Phone	Country
Atelier graphique	40.32.2555	France
Signal Gift Stores	7025551838	USA
Australian Collectors, Co.	03 9520 4555	Australia
La Rochelle Gifts	40.67.8555	France
Baane Mini Imports	07-98 9555	Norway
Mini Gifts Distributors Ltd.	4155551450	USA
Havel & Zbyszek Co	(26) 642-7555	Poland

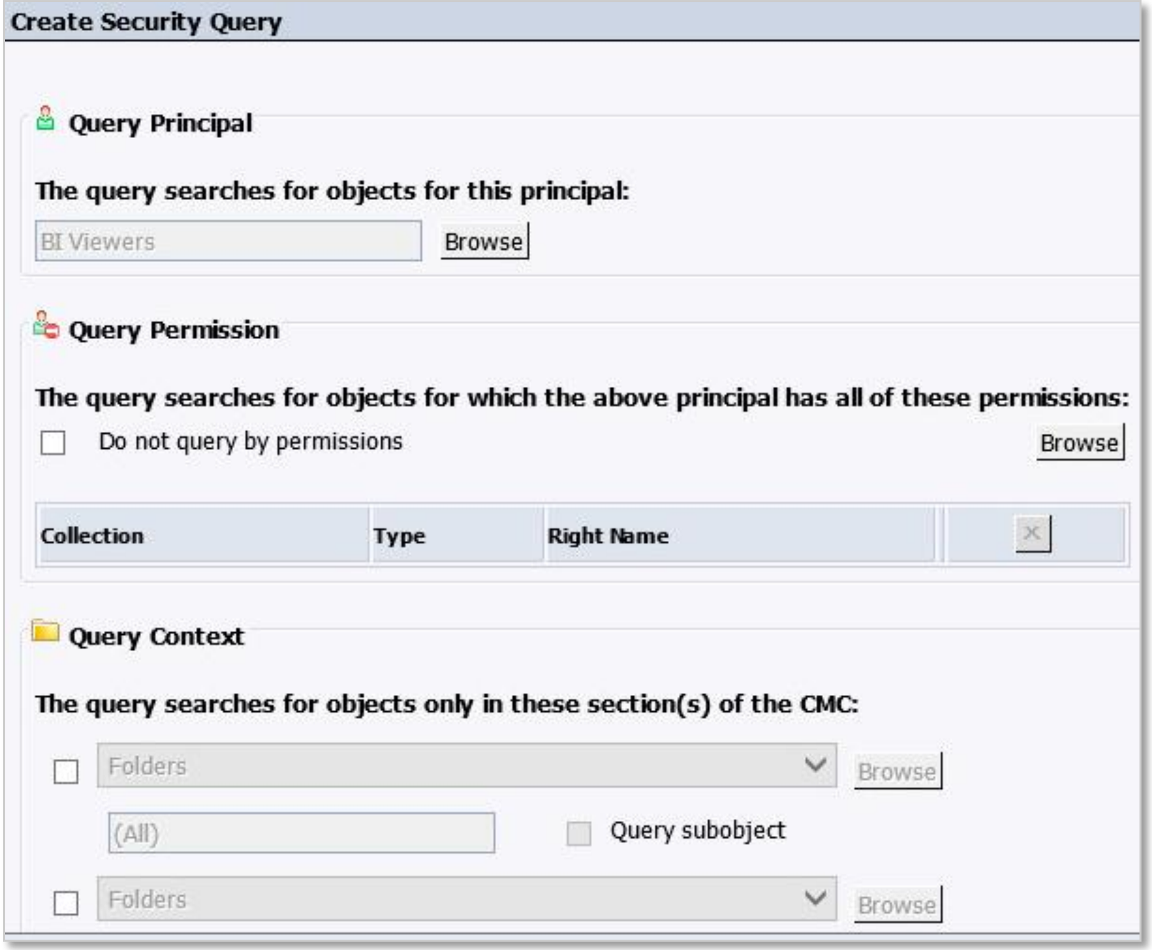
Full how to at:
http://scn.sap.com/community/bi-platform/blog/2012/07/05/user-attribute-mapping-in-bi4

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





Create Security Query

Query Principal

The query searches for objects for this principal:

BI Viewers — Browse

Query Permission

The query searches for objects for which the above principal has all of these permissions:

□ Do not query by permissions — Browse

Collection	Type	Right Name	×

Query Context

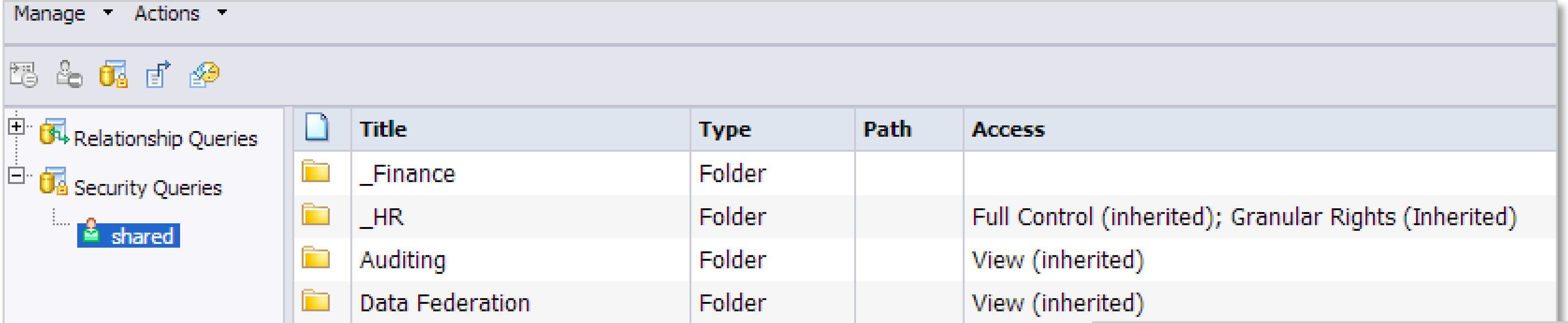
The query searches for objects only in these section(s) of the CMC:

□ Folders — Browse

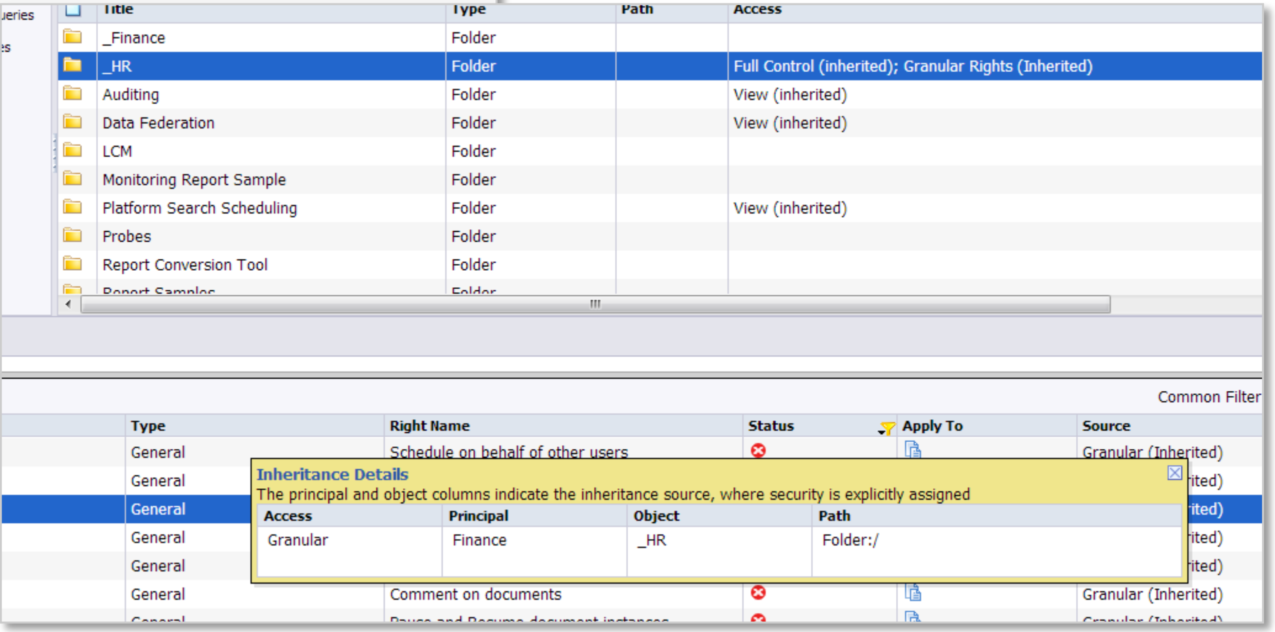
(All) — □ Query subobject

□ Folders — Browse

Security Query Tool Results



Title	Type	Path	Access
_Finance	Folder		
_HR	Folder		Full Control (inherited); Granular Rights (Inherited)
Auditing	Folder		View (inherited)
Data Federation	Folder		View (inherited)



Title	Type	Path	Access
_Finance	Folder		
_HR	Folder		Full Control (inherited); Granular Rights (Inherited)
Auditing	Folder		View (inherited)
Data Federation	Folder		View (inherited)
LCM	Folder		
Monitoring Report Sample	Folder		
Platform Search Scheduling	Folder		View (inherited)
Probes	Folder		
Report Conversion Tool	Folder		

Type	Right Name	Status	Apply To	Source
General	Schedule on behalf of other users	✖		Granular (Inherited)
General				ited)
General				ited)
General				ited)
General				ited)
General	Comment on documents	✖		Granular (Inherited)

Inheritance Details

The principal and object columns indicate the inheritance source, where security is explicitly assigned

Access	Principal	Object	Path
Granular	Finance	_HR	Folder:/

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

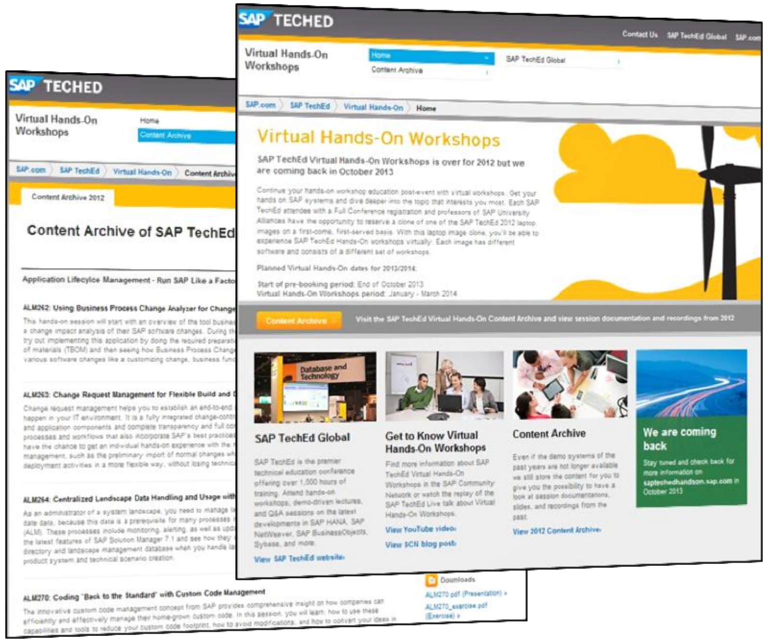
SAP TechEd Virtual Hands-on Workshops and SAP TechEd Online

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/



Virtual Hands-On Workshops

SAP TechEd Virtual Hands-On Workshops is over for 2012 but we are coming back in October 2013

Continue your hands-on workshop education post-event with virtual workshops. Get your hands on SAP systems and dive deeper into the topic that interests you most. Each SAP TechEd attendee with a Full Conference registration and professors of SAP University Alliances have the opportunity to reserve a clone of one of the SAP TechEd 2012 laptop images on a first-come, first-served basis. With this laptop image clone, you'll be able to experience SAP TechEd Hands-On workshops virtually. Each image has different software and consists of a different set of workshops.

Planned Virtual Hands-On dates for 2013/2014:

Start of pre-booking period: End of October 2013
Virtual Hands-On Workshops period: January - March 2014

Content Archive › Visit the SAP TechEd Virtual Hands-On Content Archive and view session documentation and recordings from 2012

SAP TechEd Global

SAP TechEd is the premier technical education conference offering over 1,000 hours of training. Attend hands-on workshops, demo-driven lectures, and Q&A sessions on the latest developments in SAP HANA, SAP NetWeaver, SAP BusinessObjects, Sybase, and more.

View SAP TechEd website›

Get to Know Virtual Hands-On Workshops

Find more information about SAP TechEd Virtual Hands-On Workshops in the SAP Community Network or watch the replay of the SAP TechEd Live talk about Virtual Hands-On Workshops.

View YouTube video›

View SCN blog post›

Content Archive

Even if the demo systems of the past years are not longer available we still store the content for you to give you the possibility to have a look at session documentations, slides, and recordings from the past.

View 2012 Content Archive›

We are coming back

Stay tuned and check back for more information on saptechedhandson.sap.com in October 2013

Content Archive of SAP TechEd

Application Lifecylce Management - Run SAP Like a Facto

ALM262: Using Business Process Change Analyzer for Change

ALM263: Change Request Management for Flexible Build and D

ALM264: Centralized Landscape Data Handling and Usage wit

ALM270: Coding "Back to the Standard" with Custom Code Management

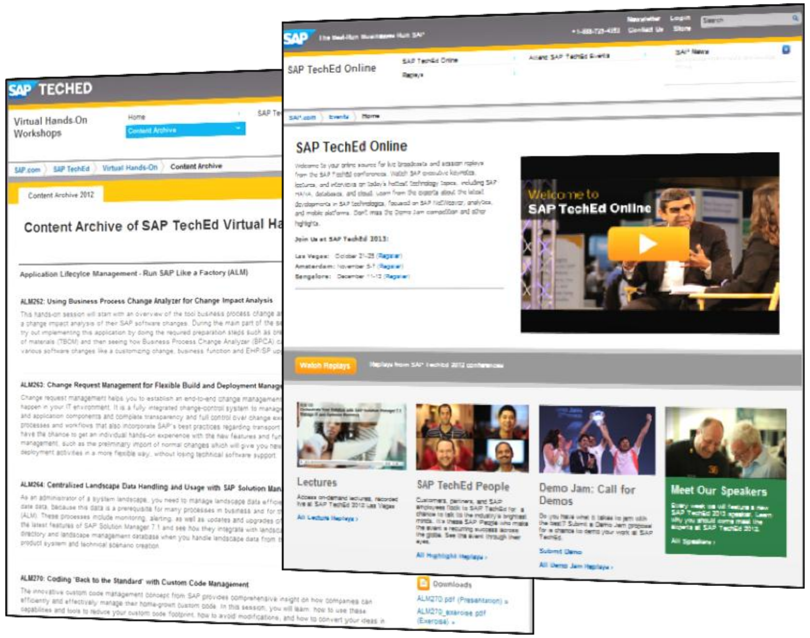
The innovative custom code management concept from SAP provides comprehensive insight on how companies can efficiently and effectively manage their home-grown custom code. In this session, you will learn: how to use these capabilities and tools to reduce your custom code footprint, how to avoid modifications, and how to convert your ideas in

Downloads
ALM270.pdf (Presentation) ›
ALM270_exercise.pdf (Exercise) ›

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



SAP TechEd Online

Welcome to your online source for live broadcasts and session replays from the SAP TechEd conference. Watch SAP executive keynotes, lectures, and interviews on today's hottest technology topics, including SAP HANA, databases, and cloud. Learn from the experts about the latest developments in SAP technologies, focused on SAP NetWeaver, analytics, and mobile platforms. Don't miss the Demo Jam competition and other highlights.

Join Us at SAP TechEd 2013:

Las Vegas: October 21-25 (Register)
Amsterdam: November 5-7 (Register)
Bangalore: December 11-13 (Register)

Watch Replays › Replays from SAP TechEd 2012 conferences

Lectures

Access on-demand lectures, recorded live at SAP TechEd 2012 Las Vegas

All Lecture Replays ›

SAP TechEd People

Customers, partners, and SAP employees flock to SAP TechEd for a chance to talk to the industry's brightest minds. It's these SAP People who make the event a recurring success across the globe. See the event through their eyes.

All Highlight Replays ›

Demo Jam: Call for Demos

Do you have what it takes to jam with the best? Submit a Demo Jam proposal for a chance to demo your work at SAP TechEd.

Submit Demo

All Demo Jam Replays ›

Meet Our Speakers

Every week we will feature a new SAP TechEd 2013 speaker. Learn why you should come meet the experts at SAP TechEd 2013.

All Speakers ›

Content Archive of SAP TechEd Virtual Ha

Application Lifecylce Management - Run SAP Like a Factory (ALM)

ALM262: Using Business Process Change Analyzer for Change Impact Analysis

This hands-on session will start with an overview of the tool business process change a a change impact analysis of their SAP software changes. During the main part of the s try out implementing this application by doing the required preparation steps such as b of materials (TBOM) and then seeing how Business Process Change Analyzer (BPCA) c various software changes like a customizing change, business function and EHP/SP up

ALM263: Change Request Management for Flexible Build and Deployment Manag

Change request management helps you to establish an end-to-end change managemen happen in your IT environment. It is a fully integrated change-control system to manag and application components and complete transparency and full control over change ex processes and workflows that also incorporate SAP's best practices regarding transport have the chance to get an individual hands-on experience with the new features and fu management, such as the preliminary import of normal changes which will give you ne deployment activities in a more flexible way, without losing technical software support.

ALM264: Centralized Landscape Data Handling and Usage with SAP Solution Man

As an administrator of a system landscape, you need to manage landscape data effici date data, because this data is a prerequisite for many processes in business and for t (ALM). These processes include monitoring, alerting, as well as updates and upgrades o the latest features of SAP Solution Manager 7.1 and see how they integrate with landsc directory and landscape management database when you handle landscape data from t product system and technical scenario creation.

ALM270: Coding "Back to the Standard" with Custom Code Management

The innovative custom code management concept from SAP provides comprehensive insight on how companies can efficiently and effectively manage their home-grown custom code. In this session, you will learn: how to use these capabilities and tools to reduce your custom code footprint, how to avoid modifications, and how to convert your ideas in

Downloads
ALM270.pdf (Presentation) ›
ALM270_exercise.pdf (Exercise) ›

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.