

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

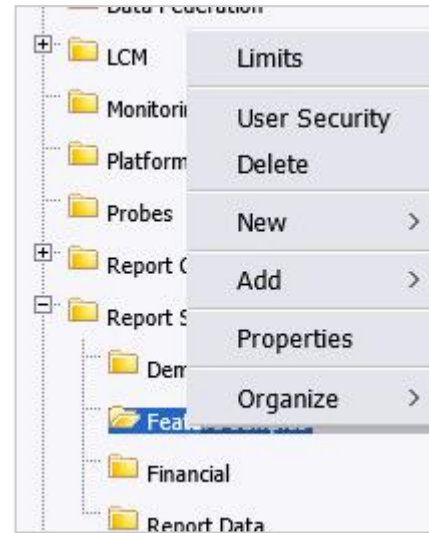
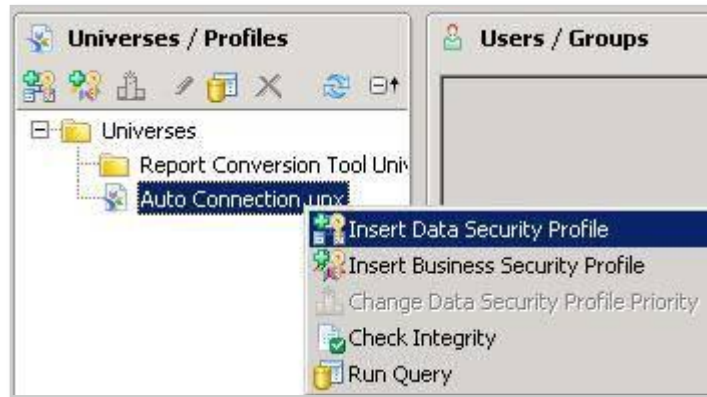
Security changes between 3.1 and 4.x

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: ☐ Client value is used for filtering in

Granted Roles System Privileges Object Privileges Analytic Priv

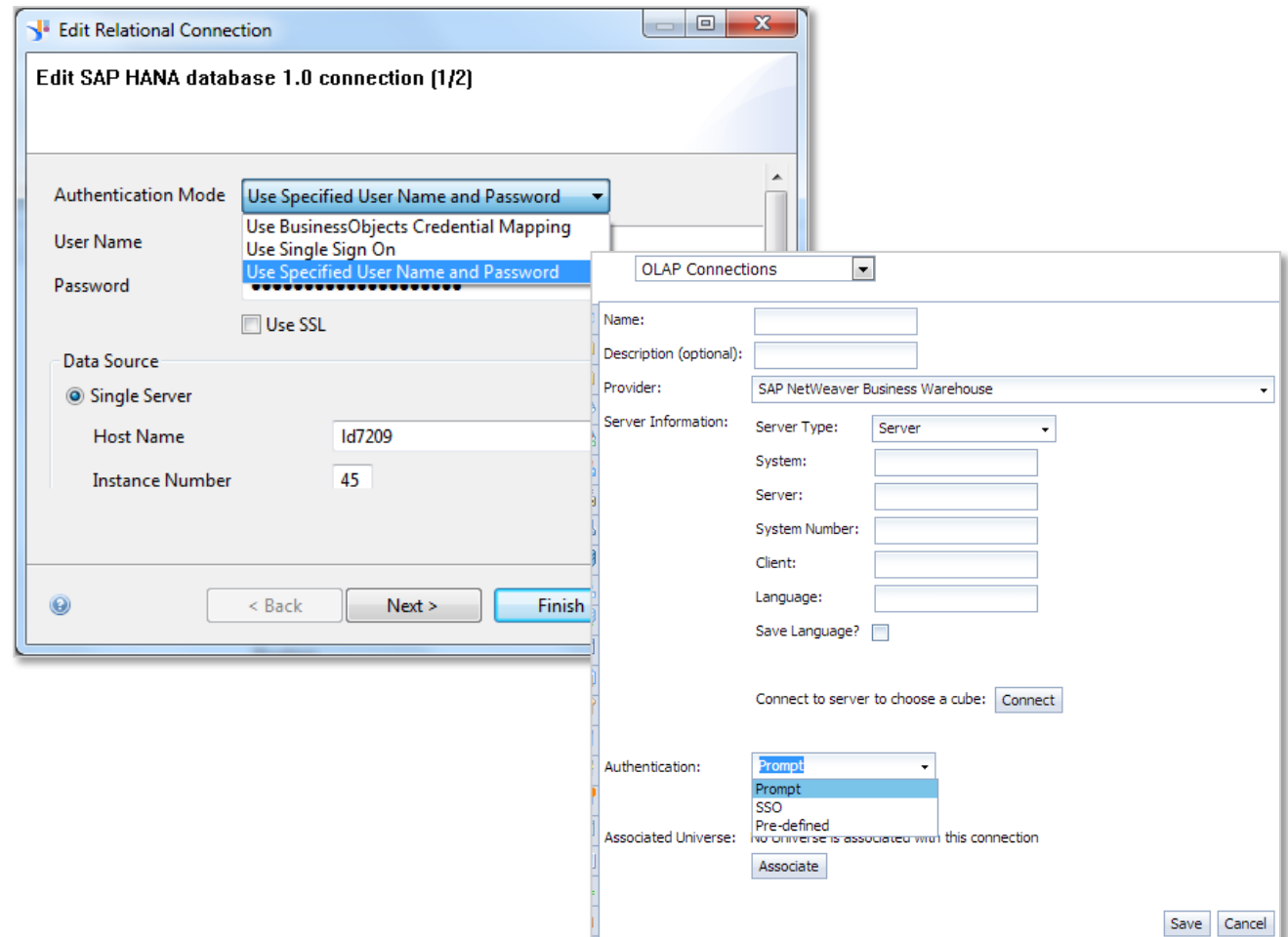
+ x

Role	Grantor
PUBLIC	SYS

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

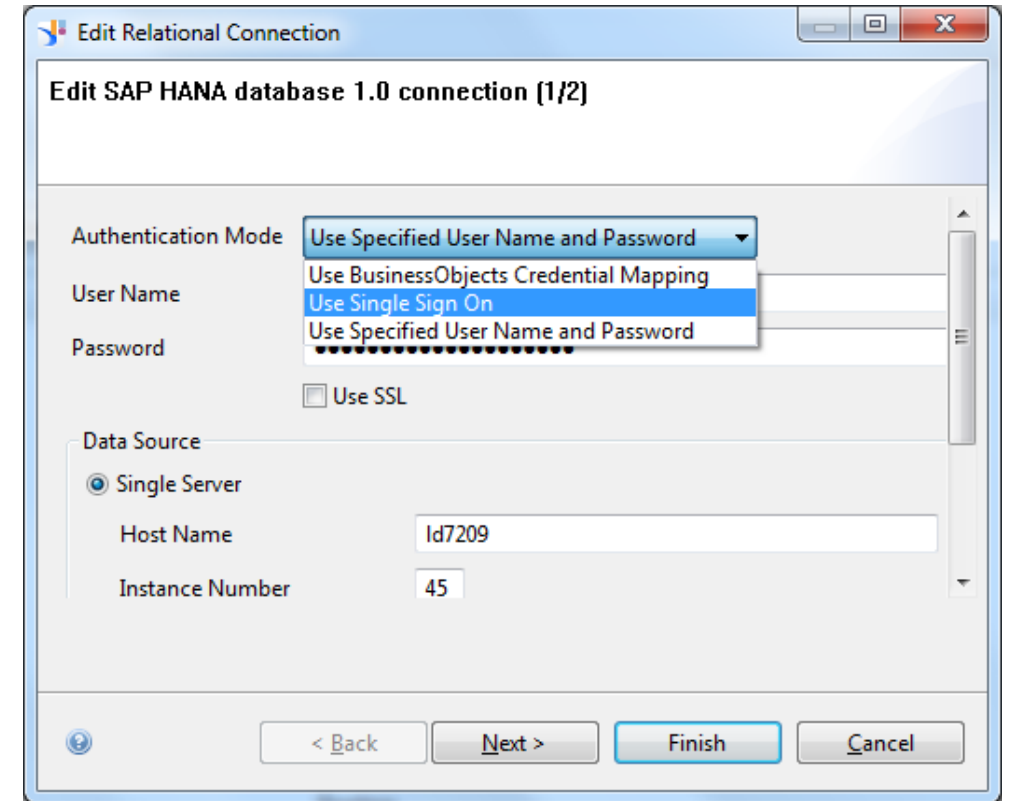
- Kerberos available for
 - MS SQL Server & Analysis Services
 - Oracle
 - Teradata (as of 4.1 via ODBC)
 - HANA
- Trust Certificates*
 - HANA (internally SAML)
 - SAP

Pros:

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

Cons:

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

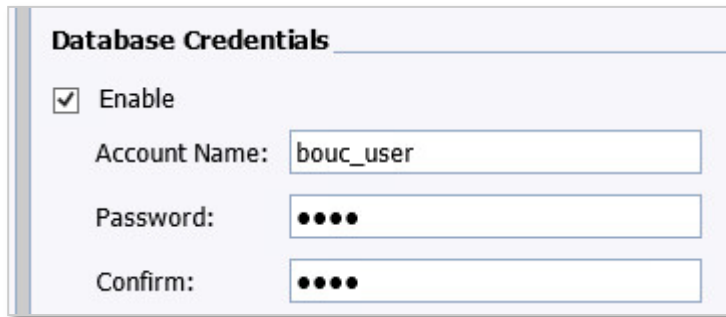


Refer to <http://scn.sap.com/docs/DOC-33875> for full list of SSO options

Considerations when creating Connections to data (save password)

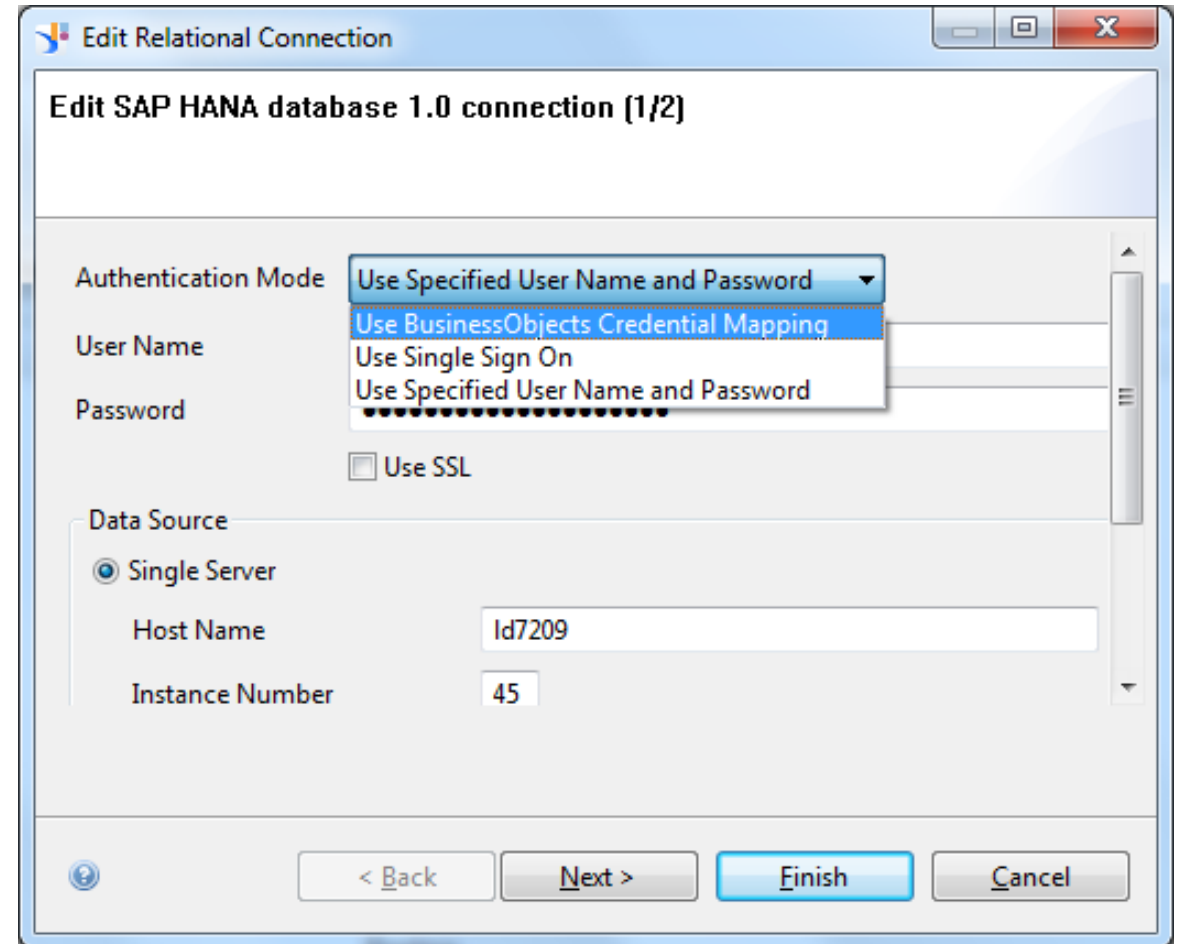
Credential Mapping

- 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.



A screenshot of a 'Database Credentials' dialog box. It has a title bar 'Database Credentials' and a checkbox 'Enable' which is checked. Below the checkbox are three input fields: 'Account Name' with the text 'bouc_user', 'Password' with four dots, and 'Confirm' with four dots.

- Capture during logon if no SSO or set via SDK



A screenshot of the 'Edit Relational Connection' dialog box, titled 'Edit SAP HANA database 1.0 connection (1/2)'. It shows the 'Authentication Mode' dropdown menu open, with options: 'Use Specified User Name and Password', 'Use BusinessObjects Credential Mapping' (highlighted), 'Use Single Sign On', and 'Use Specified User Name and Password'. Below the dropdown are fields for 'User Name' and 'Password' (masked with dots). There is a checkbox for 'Use SSL'. The 'Data Source' section has a radio button for 'Single Server' selected, with fields for 'Host Name' (Id7209) and 'Instance Number' (45). At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

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

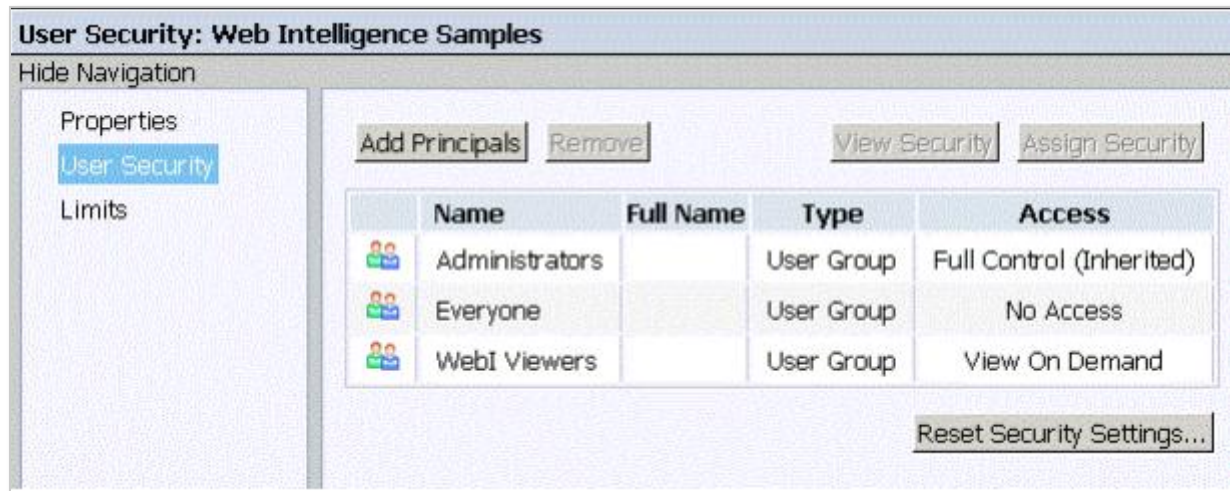
Set what user can do in system

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.



Access Levels

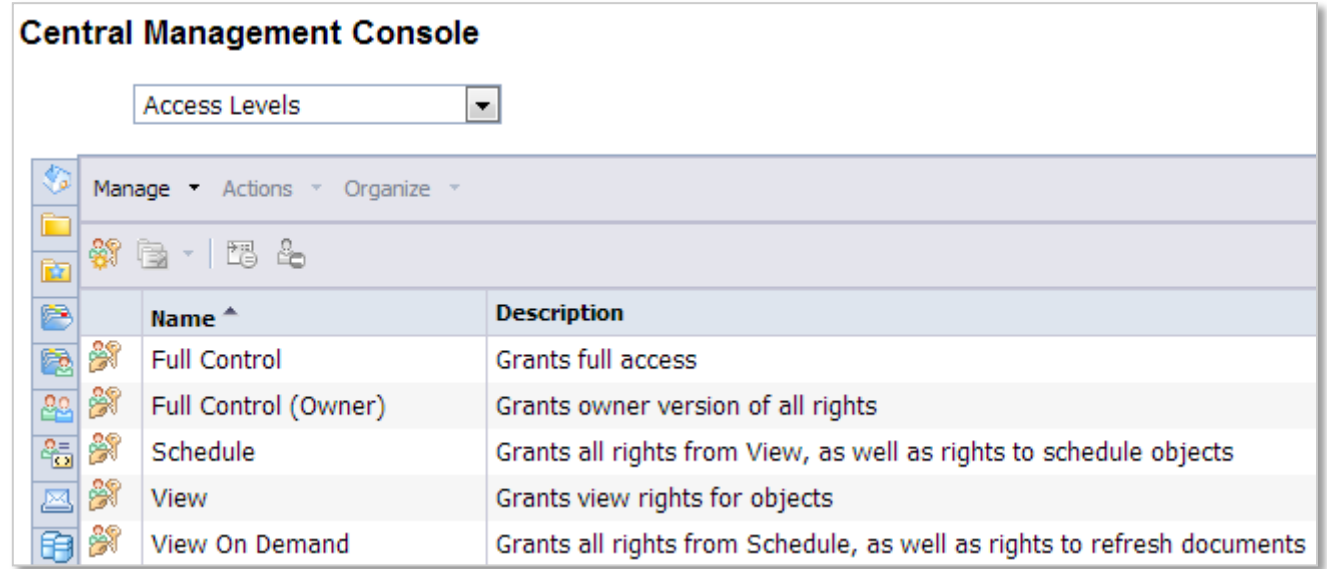
Many rights in the system

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



The screenshot shows the 'Central Management Console' interface. At the top, there is a dropdown menu labeled 'Access Levels'. Below this, there is a navigation bar with 'Manage', 'Actions', and 'Organize' tabs. A sidebar on the left contains various icons for system management. The main area displays a table of access levels.

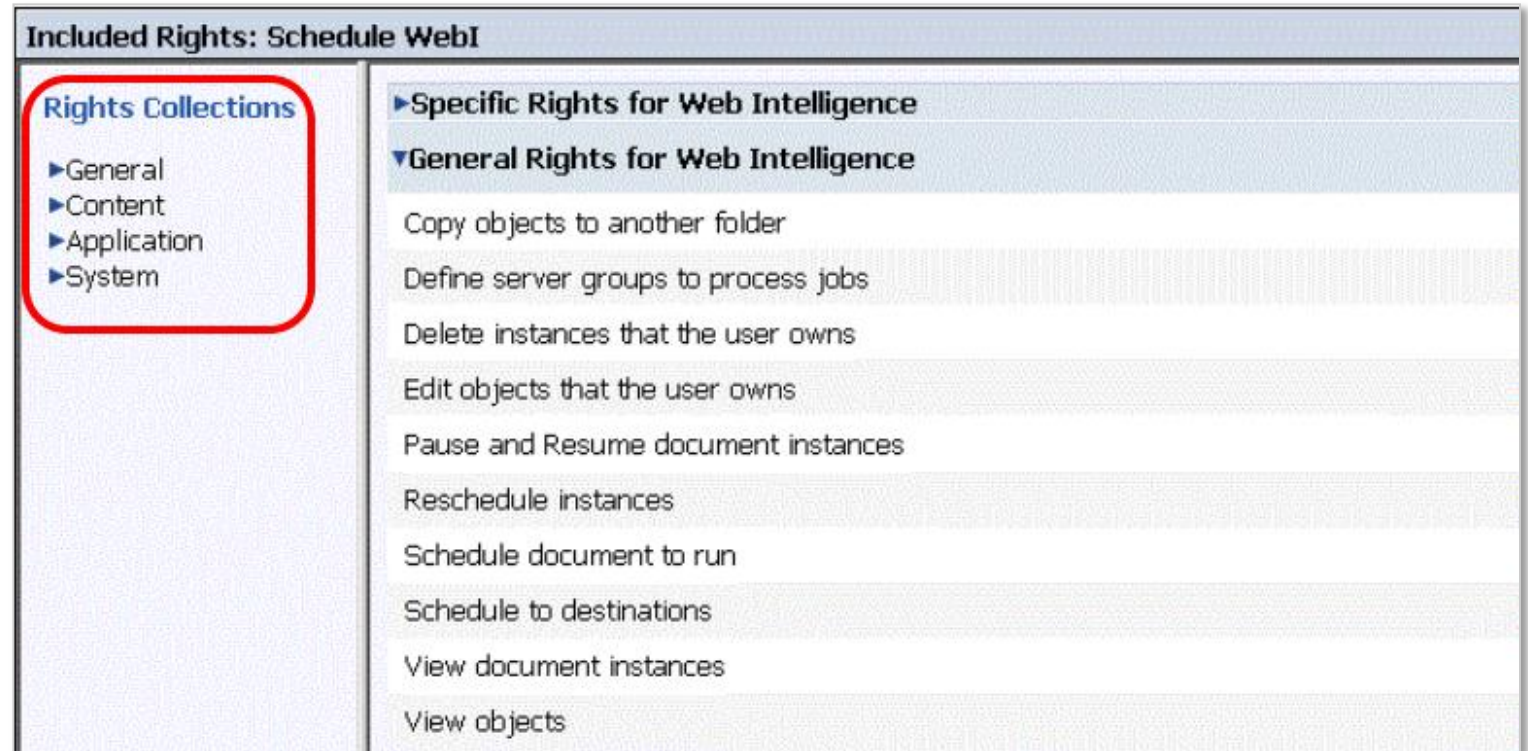
	Name ^	Description
	Full Control	Grants full access
	Full Control (Owner)	Grants owner version of all rights
	Schedule	Grants all rights from View, as well as rights to schedule objects
	View	Grants view rights for objects
	View On Demand	Grants all rights from Schedule, as well as rights to refresh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



Example of Application rights

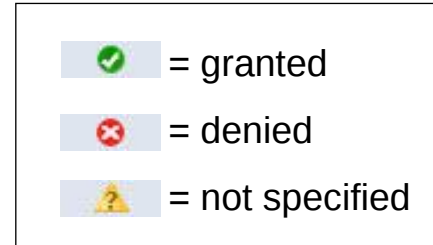
Dictates what you can do with the application

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

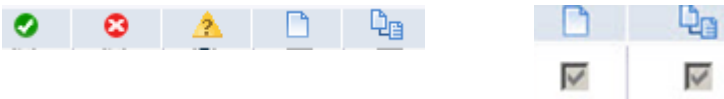
Add/Remove Rights							
Object: Web Intelligence Principal: Everyone ▼General General ▼Application Web Intelligence	▼Specific Rights for Web Intelligence		Implicit Value	✓	✗	⚠	📄
	Desktop interface - install from BI launch pad	Not Specified	☐	☐	☒	☒	☒
	Desktop interface - print documents	Granted	☐	☐	☒	☒	☒
	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
- **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).

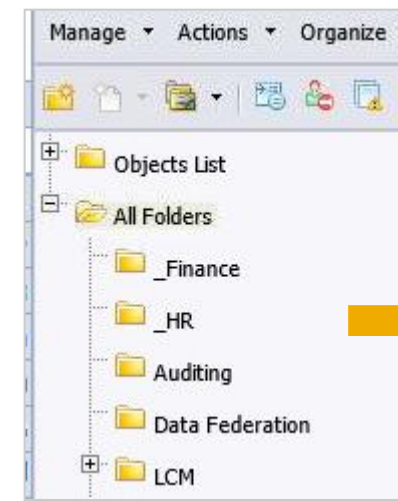
“I have 20 department folders. For each department group, I have to deny permission on 19 folders and grant permission on the single folder. Times 20...”

Example, how do we actually set this up:

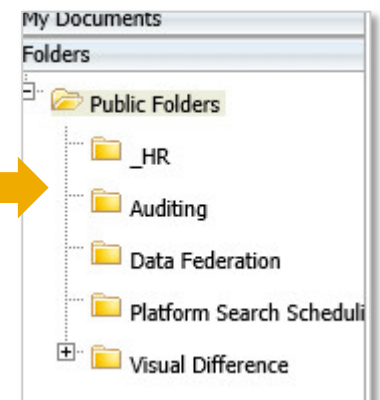


Grant view object but not subobjects

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

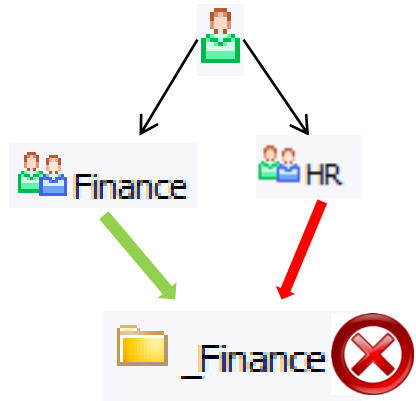
Common roles:

- **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:

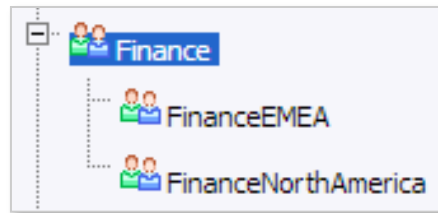
G + NS = Grant

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
Access Levels Advanced	

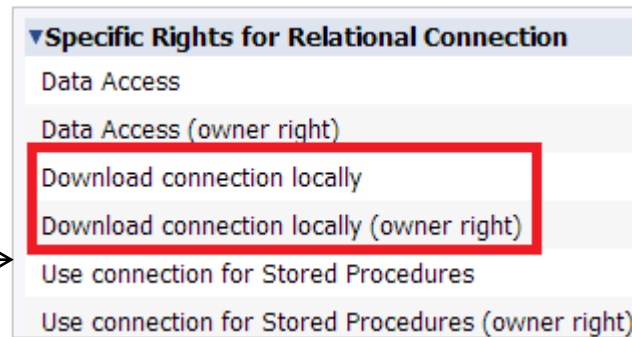
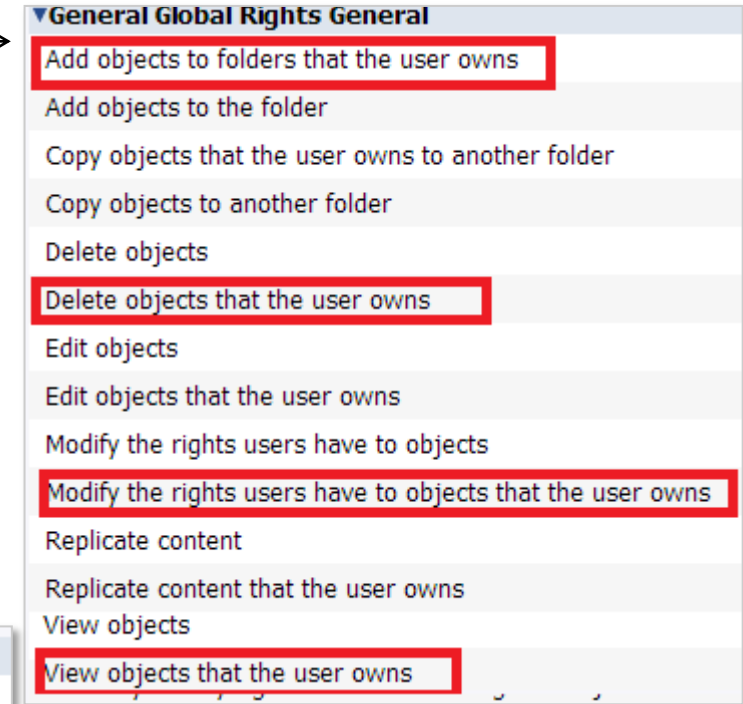
What has changed between 3.x and 4.x

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.

The image displays three screenshots from the SAP Central Management Console and BI Viewers interface, illustrating the configuration of CMC tab access.

Central Management Console: The left sidebar shows the 'Central Management Console' menu. The 'CMC Tab Access Configuration' option is highlighted with a red box.

CMC Tab Access Configuration: CMC: The main window shows the 'CMC Tab Access Configuration' dialog. The 'Restricted' radio button is selected and highlighted with a red box.

BI Viewers: The right sidebar shows the 'BI Viewers' menu. The 'CMC Tab Configuration' option is highlighted with a green box.

Configure CMC Tabs: The main window shows the 'Configure CMC Tabs' dialog. The 'Principal' is 'BI Viewers'. The 'Permission' is 'Inherited Denied' (indicated by a red X). The 'Title' is 'CMC Tab Configuration'.

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

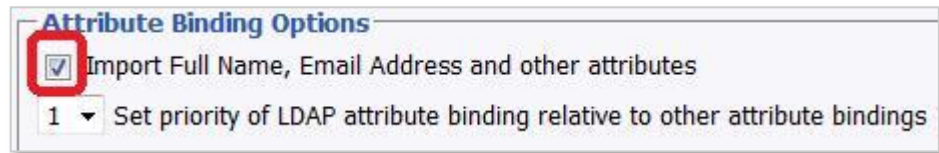
More on universe rights, User attribute mapping 1/2

Custom user attributes can be used to further secure universe



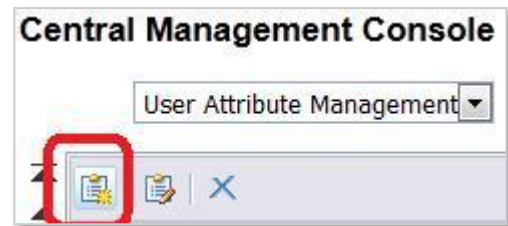
Define

- Access Levels
- Calendars
- Events
- User Attribute Management**



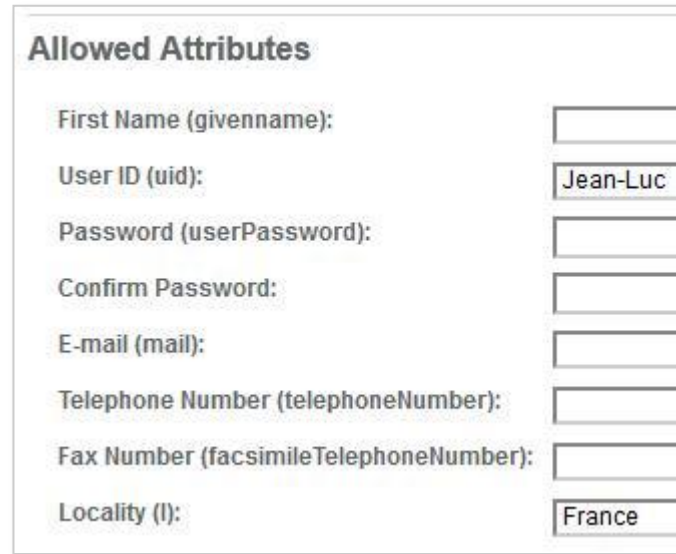
Attribute Binding Options

- ☒ 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):

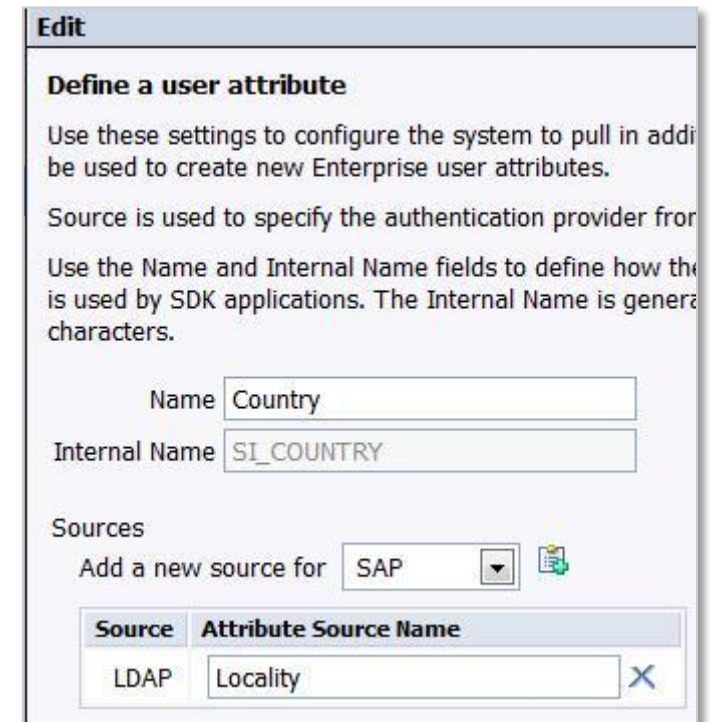
Confirm Password:

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 additional attributes to be used to create new Enterprise user attributes.

Source is used to specify the authentication provider from which the attribute is pulled.

Use the Name and Internal Name fields to define how the attribute is used by SDK applications. The Internal Name is generated by the system.

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

The first screenshot shows the 'Result Objects for Query #1' window. It displays three result objects: 'Customer Name', 'Customer Number', and 'Country'. Below these, the 'Query Filters for Query #1' section shows a filter for 'Country' set to 'Equal to' with a dropdown menu showing '@VARIABLE("SI_COUNTRY")'. The 'Result set (12 rows - 16 ms)' section shows a table with 12 rows and 3 columns: 'Customer Name', 'Customer Number', and 'Country'.

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

The second screenshot shows the 'Universes / Profiles' and 'Users / Groups' windows. The 'Universes / Profiles' window shows a tree structure with 'Universes' and 'Report Conversion Tool Uni'. The 'Users / Groups' window shows a list of users. A context menu is open over the 'Auto Connection.unx' file, showing options: 'Insert Data Security Profile', 'Insert Business Security Profile', 'Change Data Security Profile Priority', 'Check Integrity', and 'Run Query'.

The third screenshot shows the 'Define Data Security Profile' window. It has tabs for 'Connections', 'Controls', 'SQL', 'Rows', and 'Tables'. The 'Rows' tab is selected, showing a 'Restricted Table' section with a 'WHERE Clause' field. The 'WHERE Clause' field contains the text: 'Customers.country = @VARIABLE("SI_COUNTRY")'. There is an 'OK' button at the bottom right.

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

Hide Navigation

- Properties
- User Security
- Member Of
- Profile Values
- Account Manager

Account Name: Jean-Luc

Full Name: Jean-Luc

Email:

ID, CUID: 11159 , AYzy3c0g0NdHupqzIREFI4o

Description:

Additional User Properties

Country: France

Query Panel

View script

Universe : AwesomeA...

- Products
- Productlines
- Payments
- Orderdetails
- Offices
- Employees
- Customers
 - Customernumber
 - Customername
 - Contactlastname
 - Contactfirstname
 - Phone
 - Addressline1
 - Addressline2
 - City
 - State
 - Postalcode
 - Country

Result Objects for Query #1

Customername Phone Country

Query Filters for Query #1

Result set (122 rows - 47 ms)

Max Rows: 200 Refresh

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 & Zhuravsk Co	(76) 642-7555	Ireland

Close

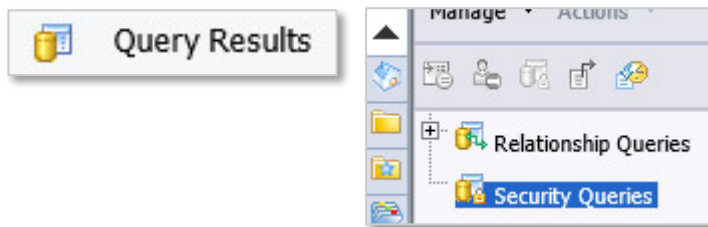
Full how to at:

<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

Query Permission

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

☐ Do not query by permissions

Collection	Type	Right Name	
			X

Query Context

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

☐ Folders

(All) ☐ Query subobject

☐ Folders

Security Query Tool Results

Manage ▾ Actions ▾

Relationship Queries

Security Queries

shared

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		

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

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		
Report Samples	Folder		

Type	Right Name	Status	Apply To	Source
General	Schedule on behalf of other users	✖	📄	Granular (Inherited)
General				(Inherited)
General				(Inherited)
General				(Inherited)
General				(Inherited)
General	Comment on documents	✖	📄	Granular (Inherited)
General	Pause and Resume document instances	✖	📄	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:/

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

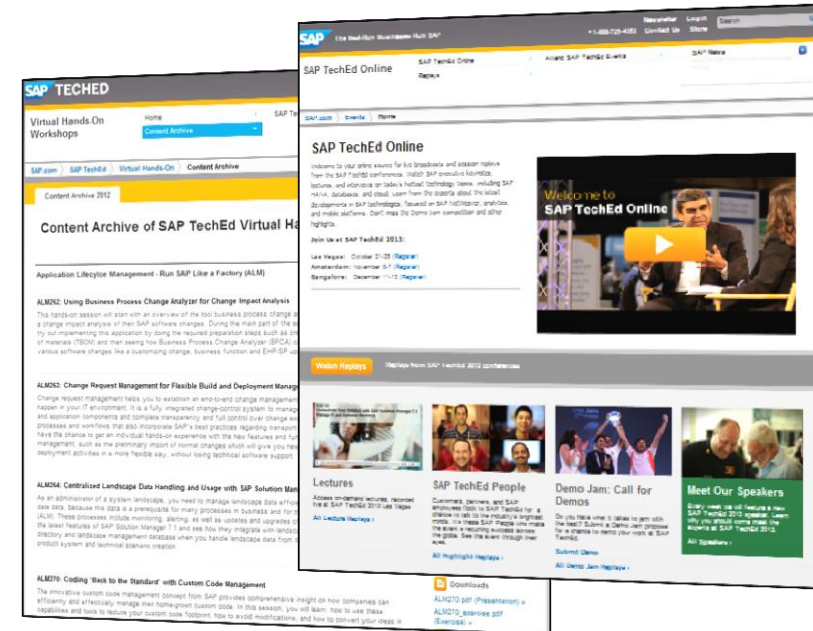
<http://saptechedhandson.sap.com/>



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.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.