

SECURE UNIVERSES USING RESTRICTION SETS

Dallas J. Marks

BREAKOUT INFORMATION

- ▶ Secure Universes Using Restriction Sets
 - ▶ Do you need to tailor universe security to specific users or groups within your organization? Attend this session to learn about restriction sets and how they can apply security to selected groups or user accounts for the universe. Hear how applied restrictions can control objects, rows, query types, and connections. See live demonstrations on how to use each type of restriction and the effect they have on user Web Intelligence documents.

Print Information (please leave for Business Objects use)

Print Code

AGENDA

1. The need for universe security
2. What are restriction sets?
3. Previewing access restrictions
4. Tips & Tricks
5. Live demonstrations
6. Conclusion
7. Q&A

ABOUT DALLAS MARKS

- ▶ Dallas is an SAP Certified Application Associate and authorized trainer for Web Intelligence, Information Design Tool, Universe Design Tool, Dashboards (formerly Xcelsius), and SAP BusinessObjects Business Intelligence administration. A seasoned consultant and speaker, Dallas has worked with SAP BusinessObjects tools since 2003 and presented at the North American conference each year since 2006.
- ▶ Dallas has implemented SAP BusinessObjects solutions for a number of industries, including retail, energy, health care, and manufacturing. He holds a master's degree in Computer Engineering from the University of Cincinnati.
- ▶ Dallas blogs about various business intelligence topics at <http://www.dallasmarks.org/>. You can follow him on Twitter at [@dallasmarks](https://twitter.com/dallasmarks).

THE NEED FOR UNIVERSE SECURITY

TWO METHODS FOR SECURING UNIVERSES



- ▶ Restrict access to entire universe by setting universe rights in the Central Management Console (CMC)
- ▶ Create various forced and optional restrictions within Designer
 - ▶ Forced
 - ▶ Object restrictions
 - ▶ Self-restricting joins
 - ▶ Inferring multiple tables
 - ▶ Optional
 - ▶ Condition objects

BUSINESS PROBLEM

- ▶ Business requirement to secure business critical data based on a user's role in the organization
- ▶ All of these restrictions affect ***all*** users ***unilaterally***
- ▶ A different solution is required to apply security to specific users and groups: **restriction sets**



WHAT IS A RESTRICTION SET?

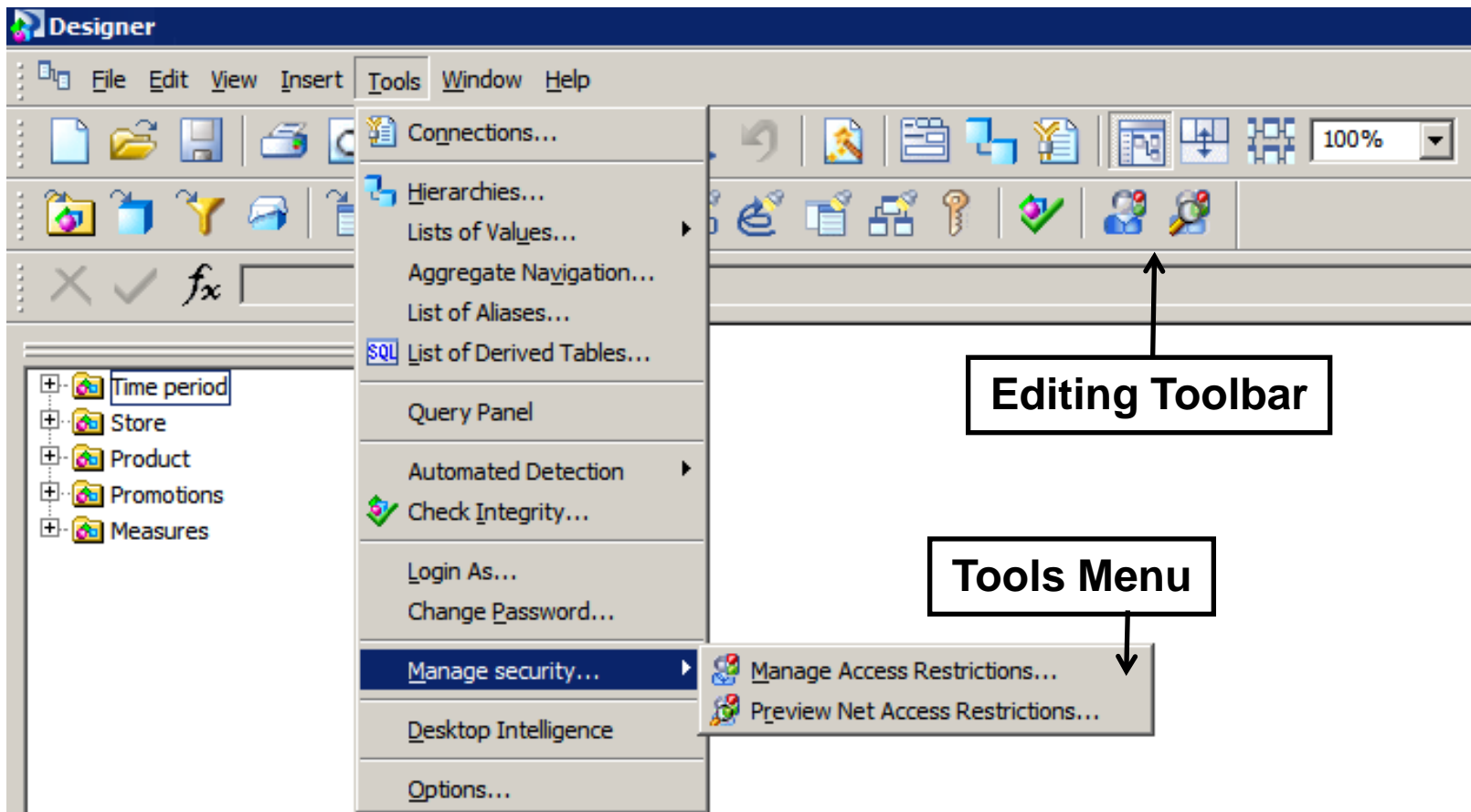
- ▶ A *restriction set* is a named group of restrictions that apply to a universe
- ▶ Restriction sets can be applied to BusinessObjects users and groups to force behavior changes in a universe
- ▶ Restriction sets are managed using the Business Objects Universe Designer application, using a feature named *access restrictions*

WHAT CAN BE RESTRICTED?

Type of restriction	Description
Connection	Override the default universe connection with an alternate connection
Query controls	Limit the size of the result set and query execution time
SQL generation controls	Control how SQL is generated by user query
Object access	Column-level security
Row access	Row-level security – force restrictions into the WHERE clause of inferred SQL
Alternative table access	Replace a table referenced in the universe with another table in the database

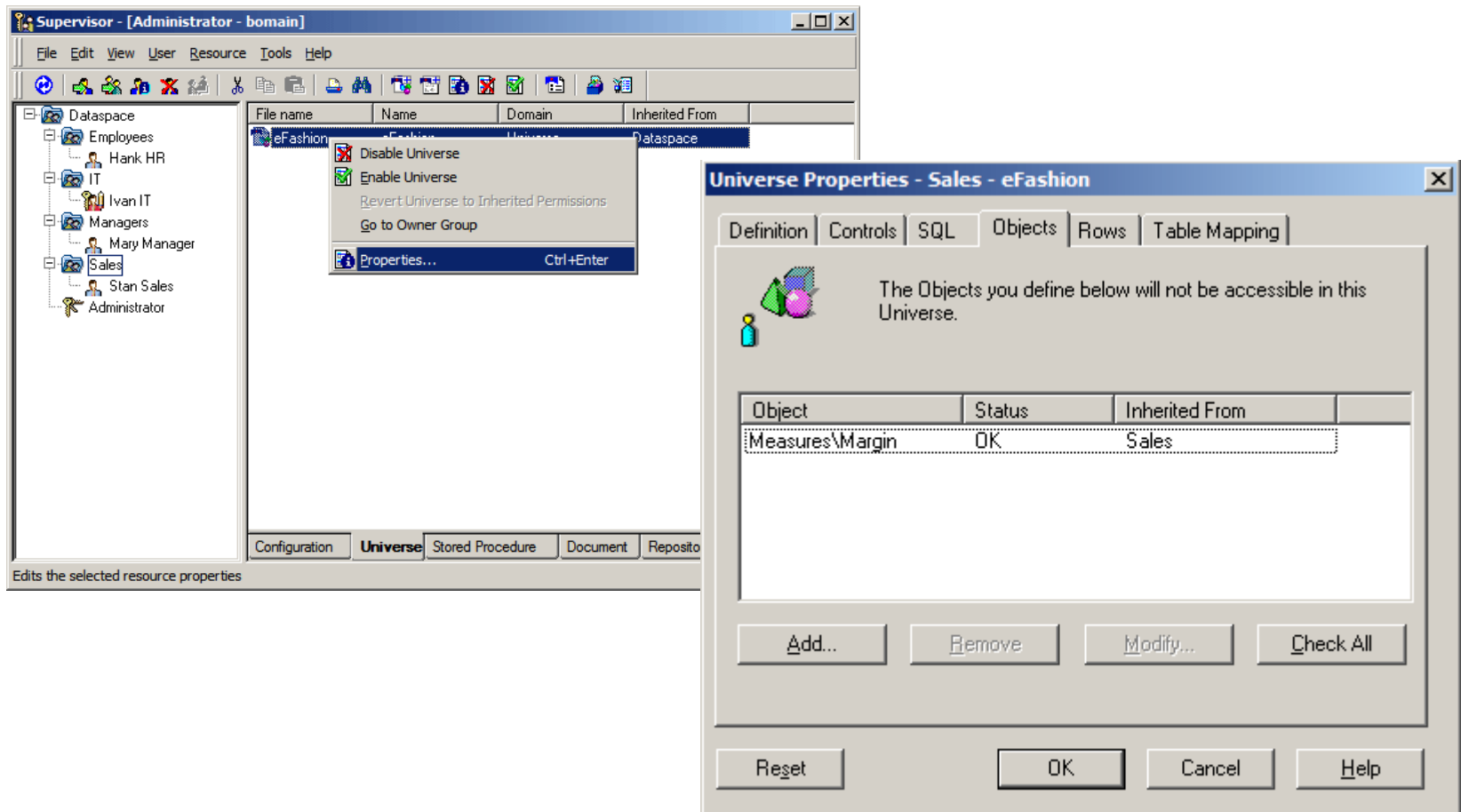
DESIGNER – MANAGING ACCESS RESTRICTIONS

- ▶ Access restrictions can be accessed from either the **tools** menu or the **editing** toolbar



PREVIOUS VERSIONS – SUPERVIOR

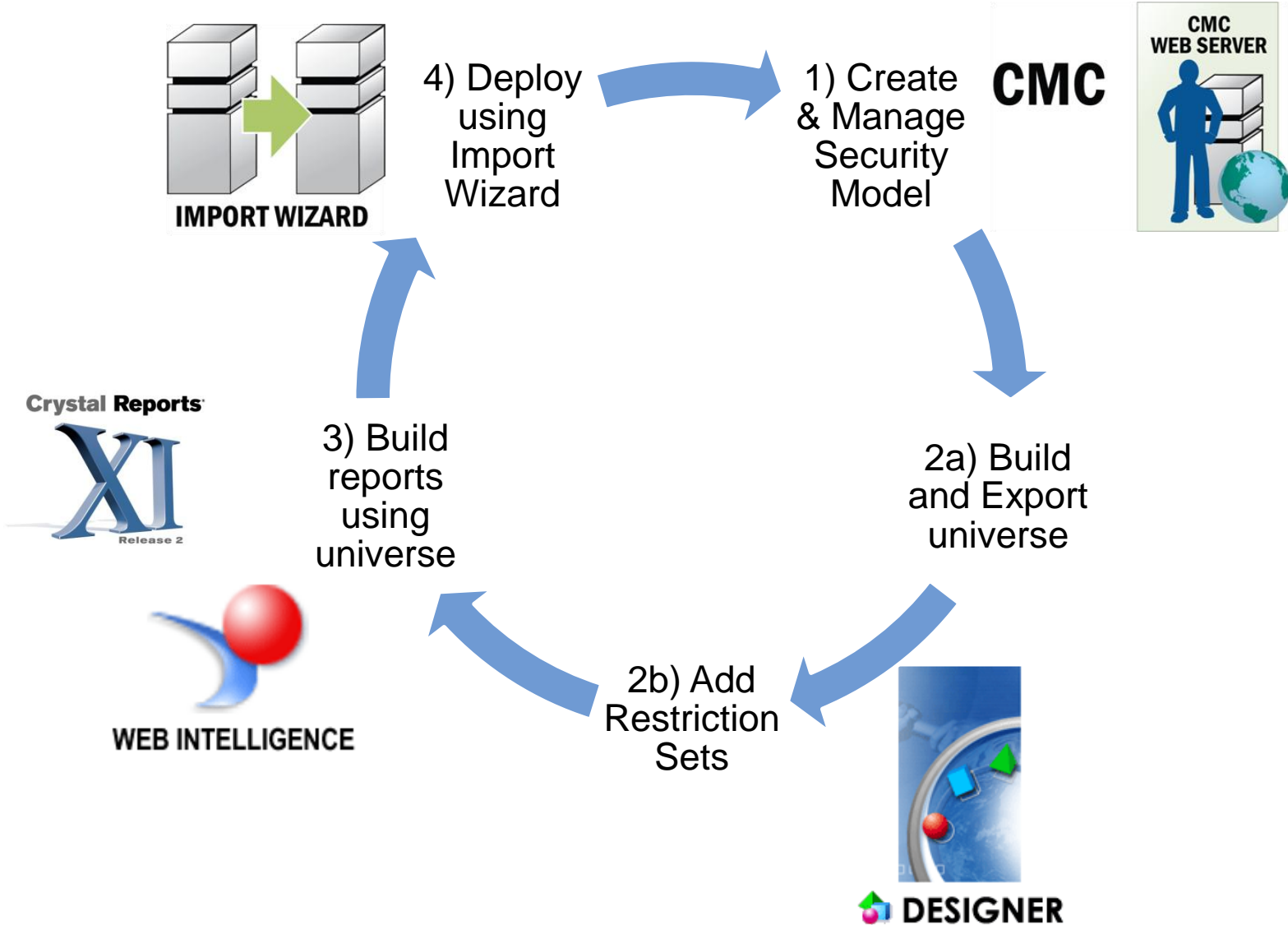
- ▶ Previous versions of BusinessObjects provided similar capabilities, accessed from the supervisor application



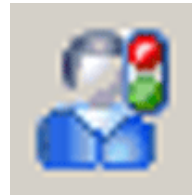
Creating and managing user- and group-based universe security

WHAT ARE RESTRICTION SETS?

SECURING UNIVERSES – DESIGN PROCESS



MANAGE ACCESS RESTRICTIONS IN DESIGNER



- ▶ Three basic steps to follow

1. Create new restrictions

2. Add appropriate groups and users

The screenshot shows the 'Manage Access Restrictions' dialog box. It has a title bar and a main area with a blue header. Below the header is a text box explaining the purpose of the dialog. There are two main sections: 'Available Restrictions' on the left and 'Available groups and users' on the right. A '>>Apply' button is located between them. At the bottom, there are buttons for 'New', 'Edit', 'Add user or group', 'Priority', 'Preview', 'OK', and 'Cancel'. Three callout boxes with arrows point to the 'Available Restrictions' list, the 'Available groups and users' list, and the '>>Apply' button.

Manage Access Restrictions

You can create security restrictions and apply them to groups or users. The list on the left shows all the existing security restrictions for this universe. The list on the right shows all the users and groups that have security restrictions applied.

Available Restrictions:

Available groups and users:

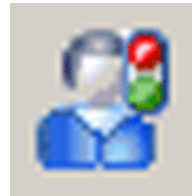
Name	Restriction	Priority
------	-------------	----------

>>Apply

New Edit X Add user or group Priority Preview X OK Cancel

3. Map restrictions to groups and users

MANAGE ACCESS RESTRICTIONS IN DESIGNER



► Additional configuration

Priority of multiple restrictions

Manage Access Restrictions

You can create security restrictions and apply them to groups or users. The list on the left shows all the existing security restrictions for this universe. The list on the right shows all the users and groups that have security restrictions applied.

Available Restrictions:

Available groups and users:

Name	Restriction	Priority
------	-------------	----------

>>Apply

New Edit X

Add user or group Priority Preview X ?

OK Cancel

Options

Priority of multiple restrictions

GETTING HELP



- ▶ On-line help is available from the manage access restrictions dialog

The screenshot shows the 'Manage Access Restrictions' dialog box. On the left, there is a list of 'Available Restriction Sets' including 'eFashion Manager', 'eFashion SQL Restrictions', 'eFashion Table Mapping', and 'Original eFashion Manager'. The 'eFashion Managers Storage' restriction set is selected. The main area of the dialog shows a table of existing security restrictions:

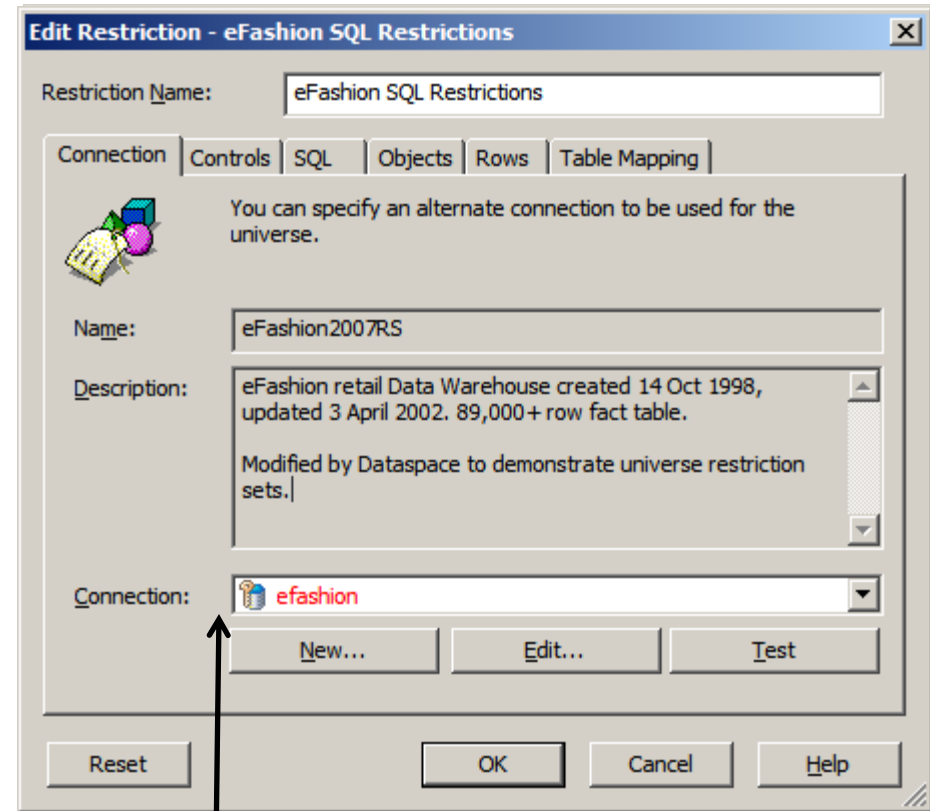
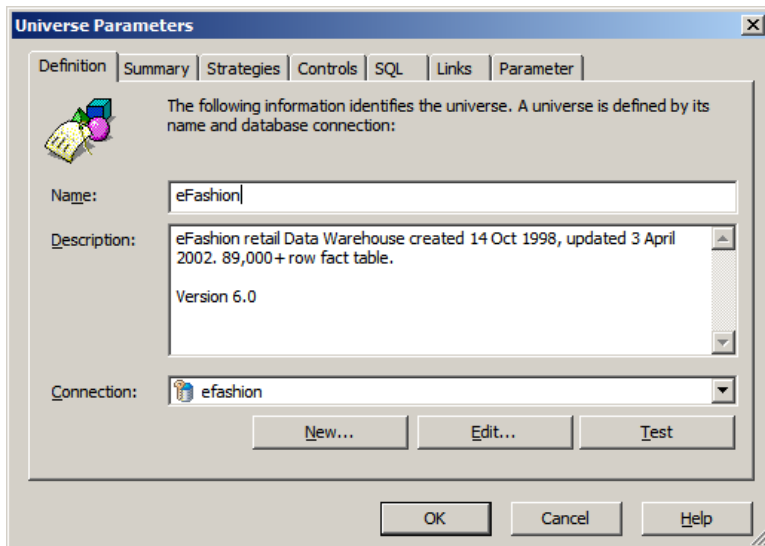
Restriction	P
Office	2
Original eFashion Connection	2
eFashion Managers Storage	1
Central	3
eFashion SQL Restrictions	3
South	4
eFashion Table Mapping	4

An online help window titled 'New Window Caption' is overlaid on the dialog. It has a search bar and a list of search results. The search results include '@AggregateAware', '@Functions', 'use of', '@Prompt', '@Script', '@Select', '@Variable', 'access', 'all users', 'activate', 'list mode', 'add', 'connection', 'advanced properties', and 'object'. The 'Managing access restrictions' section is highlighted, and the text reads: 'Access restrictions are managed from the Manage Access Restrictions dialog box.' Below this, there are two bullet points: 'The restriction sets currently available to the universe are listed in the Available Restriction Sets pane.' and 'The users and user groups that are defined for each restriction set appear in the Available Groups and Users pane.' At the bottom of the help window, it says: 'The options available to manage access restrictions are described as follows. Click on each options for...'

At the bottom right of the 'Manage Access Restrictions' dialog, there is a 'Help' icon (a question mark in a blue circle) next to the 'Preview' button. An arrow points from this icon to the help window.

RESTRICTION SET DIALOGS – CONNECTION

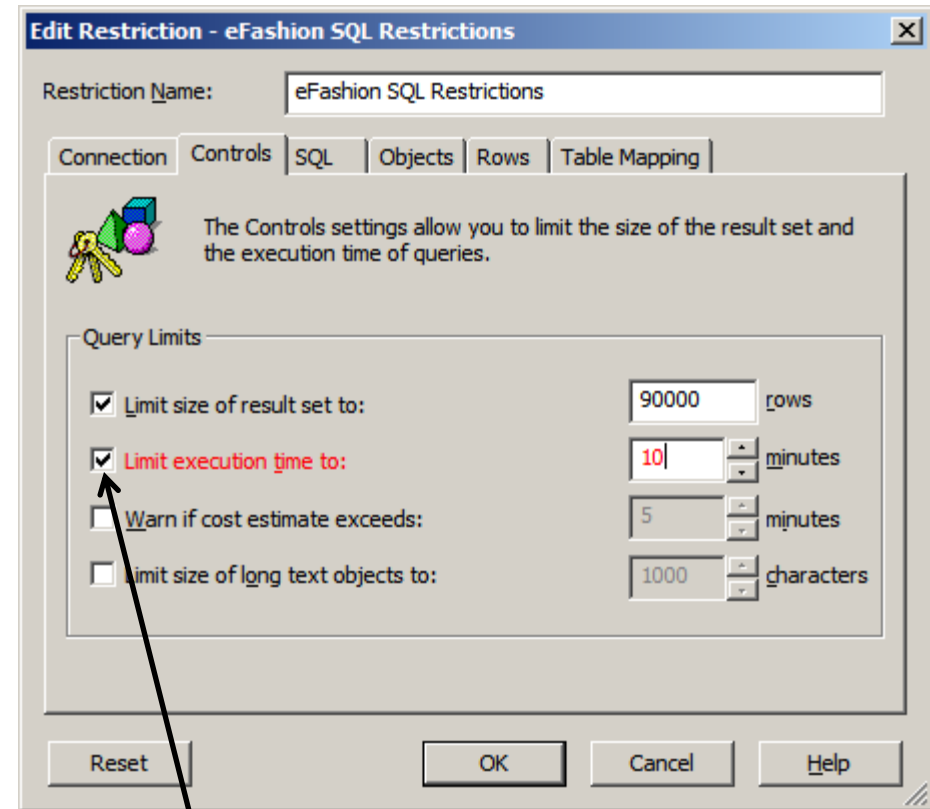
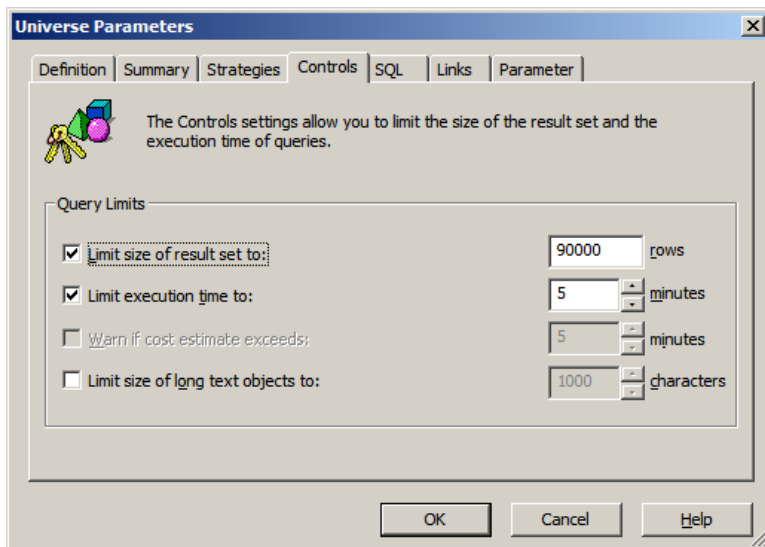
- ▶ Control which database connection is used
- ▶ Identical to definition tab of universe parameters
- ▶ Useful for pointing subset of users to alternate data source (ex. QA instead of production)



Restrictions that differ from universe defaults appear in **red**

RESTRICTION SET DIALOGS – CONTROLS

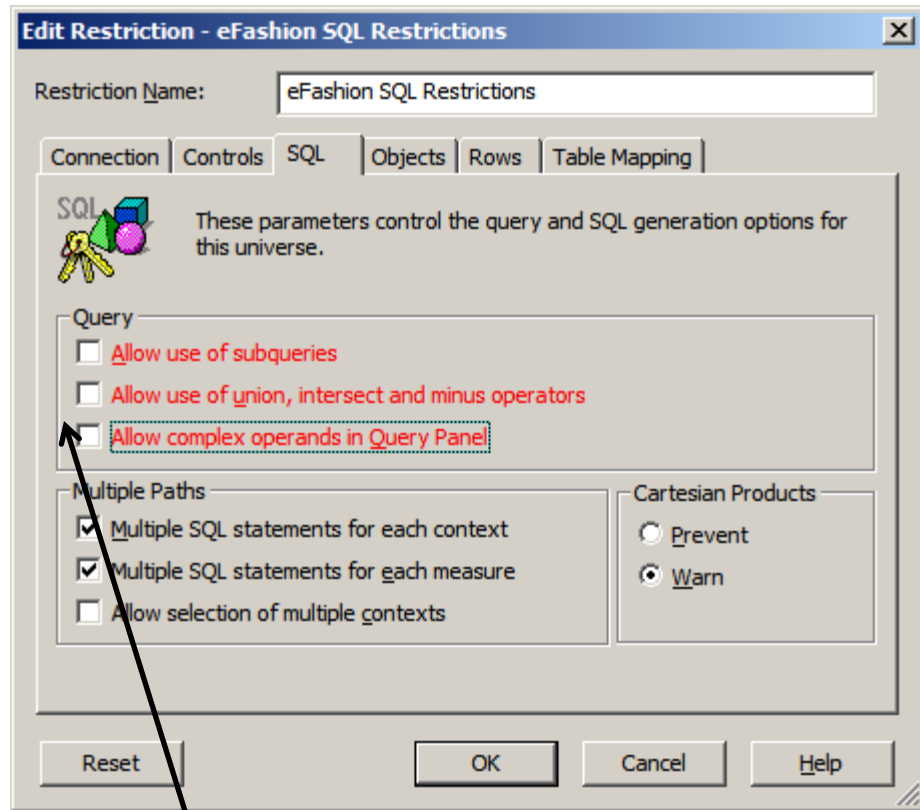
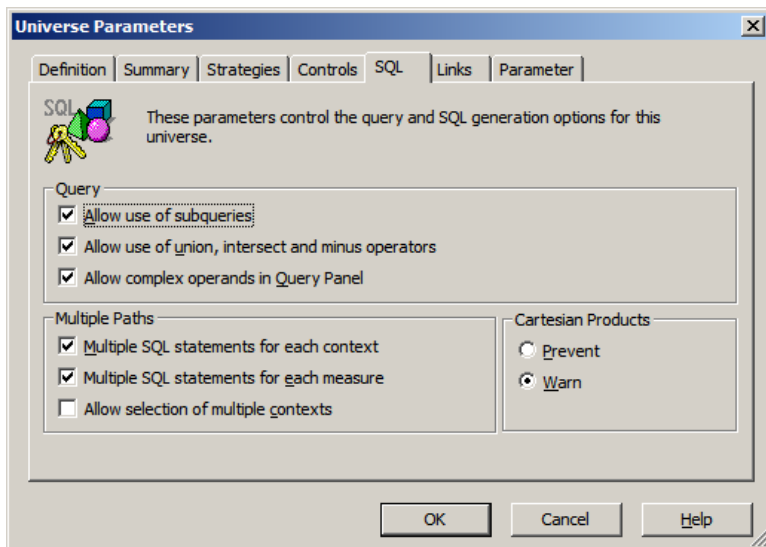
- ▶ Define limits on query execution
- ▶ Identical to controls tab of universe parameters
- ▶ Useful for giving power users higher limits than standard users



Restrictions that differ from universe defaults appear in **red**

RESTRICTION SET DIALOGS – SQL

- ▶ Define limits on what types of queries users may create
- ▶ Identical to SQL tab of universe parameters
- ▶ Useful for limiting the complexity of queries



Restrictions that differ from universe defaults appear in **red**

RESTRICTION SET – SQL

- ▶ The “Allow use of subqueries” checkbox controls access to the feature in the Web Intelligence query panel

The screenshot shows the 'Edit Restriction - eFashion SQL Restrictions' dialog box with the 'SQL' tab selected. The 'Restriction Name' is 'eFashion SQL Restrictions'. The 'Query' section contains the following options:

- Allow use of subqueries
- Allow use of union, intersect and minus operators
- Allow complex operands in Query Panel

The 'Multiple Paths' section contains:

- Multiple SQL statements for each context
- Multiple SQL statements for each measure
- Allow selection of multiple contexts

The 'Cartesian Products' section contains:

- Prevent
- Warn

A callout box at the bottom right contains the text: "Restrictions that differ from universe defaults appear in red".

RESTRICTION SETS - SQL

- ▶ The “Allow use of union, intersect and minus operators” checkbox controls access to the feature in the Web Intelligence query panel

The screenshot displays the 'Edit Restriction - eFashion SQL Restrictions' dialog box. The 'SQL' tab is selected, and the 'Query' section contains the following options:

- Allow use of subqueries
- Allow use of union, intersect and minus operators
- Allow complex operands in Query Panel

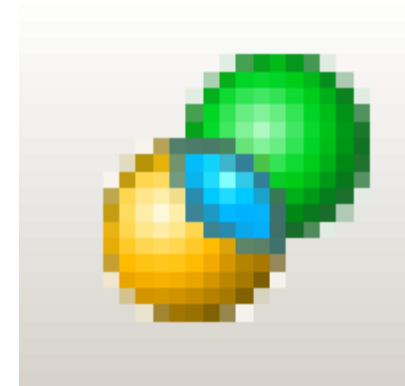
The 'Data' pane on the right shows a tree view of objects:

- Store name
- Store details
- Sales floor size?
- Owned stores
- Stores with long oper
- Product
 - Lines
 - Category

The 'Result Objects' pane shows the following objects:

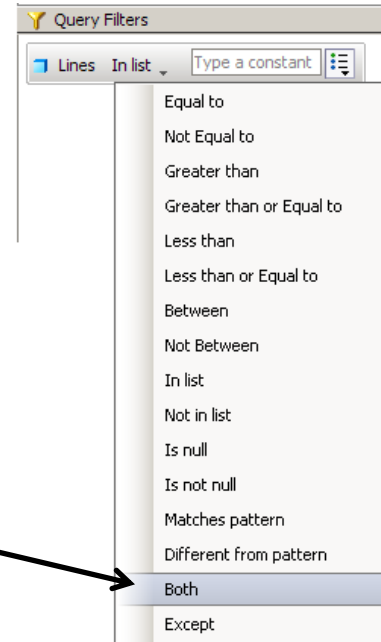
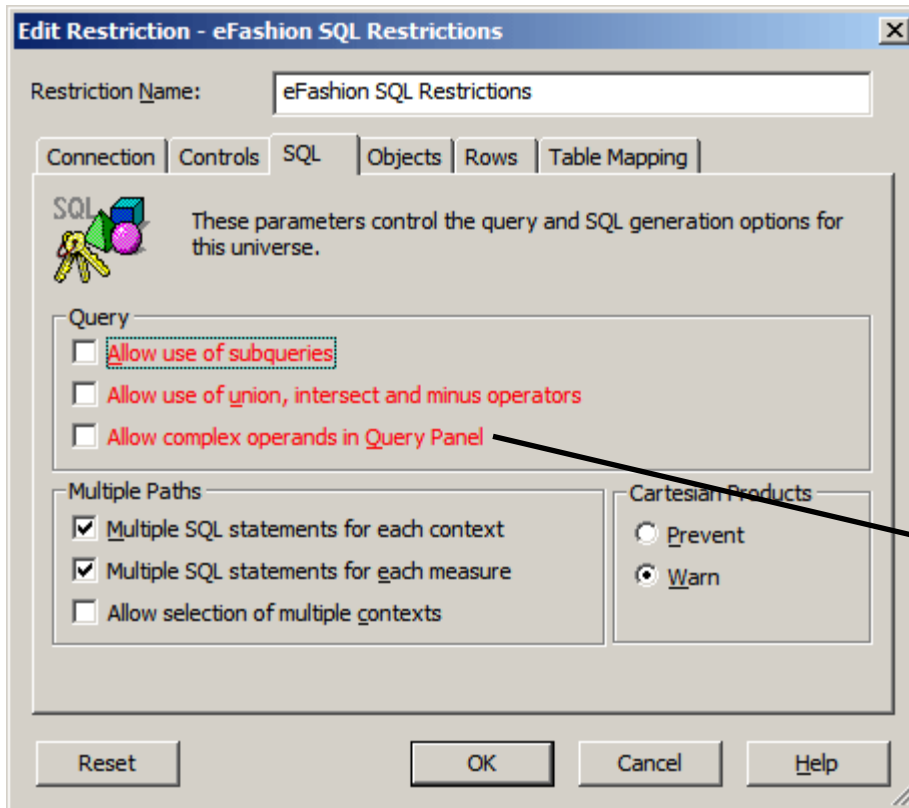
- Lines
- Category
- Color
- Quantity sold

The 'Cartesian Products' section has the 'Warn' radio button selected.

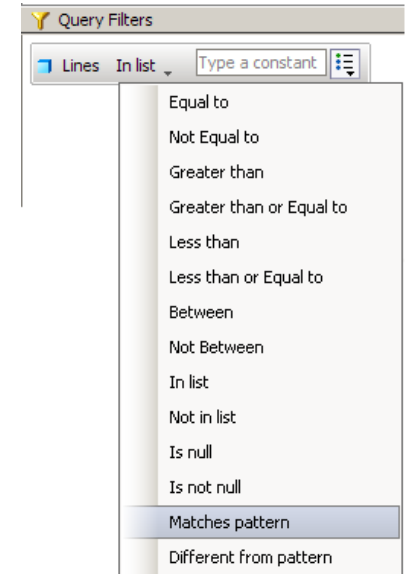


RESTRICTION SETS - SQL

- ▶ The “Allow complex operands in Query Panel” checkbox controls access to the both and except query filter operators in the Web Intelligence query panel



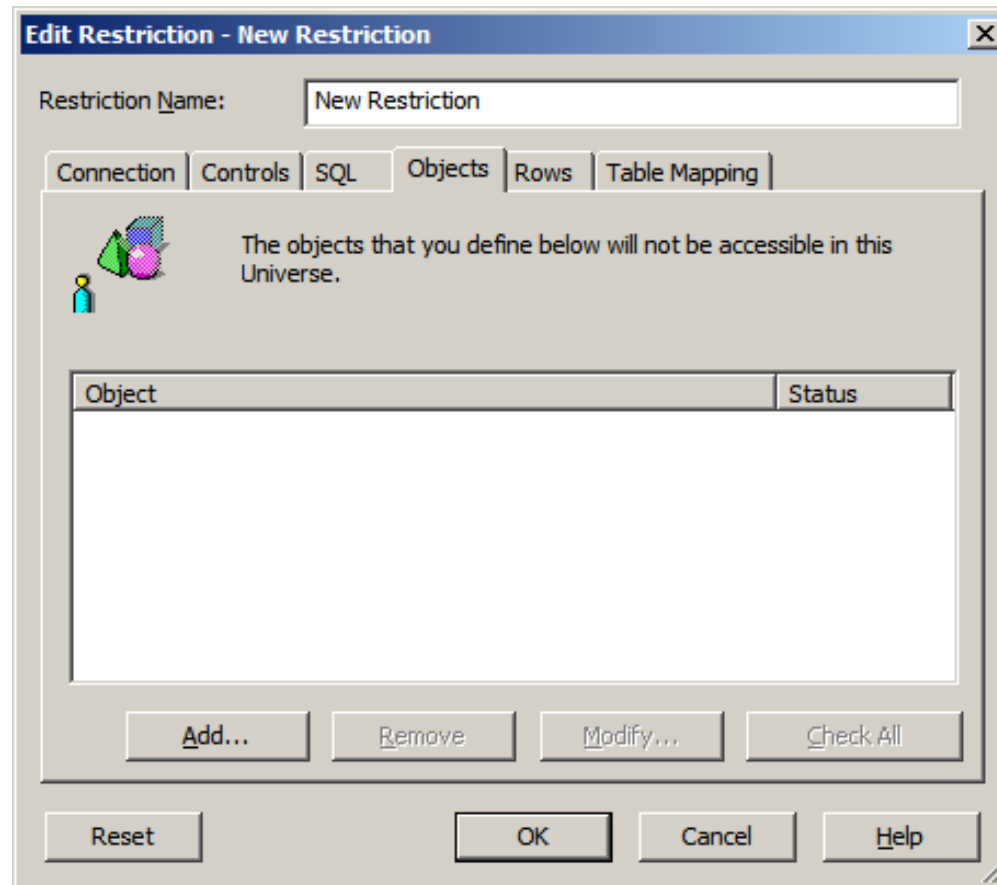
Allowed
(checked)



Disallowed
(unchecked)

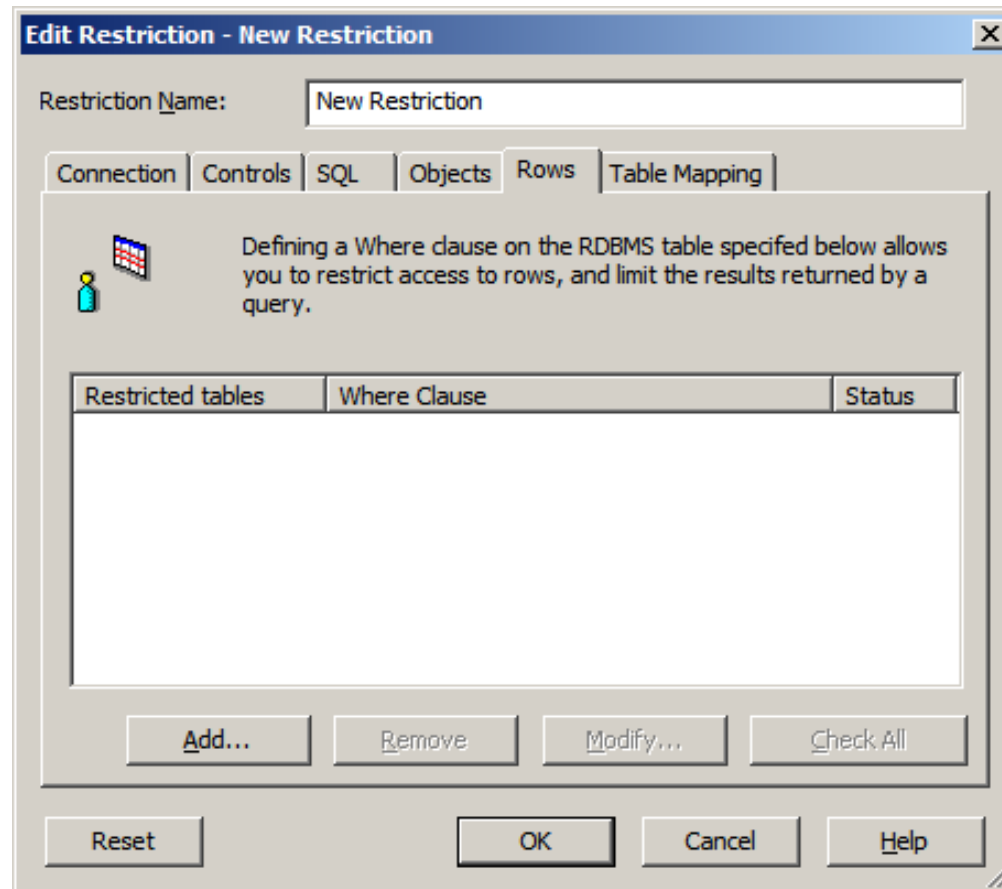
RESTRICTION SET DIALOGS – OBJECTS

- ▶ Restrict access to universe objects, for example, employee salary or other sensitive objects



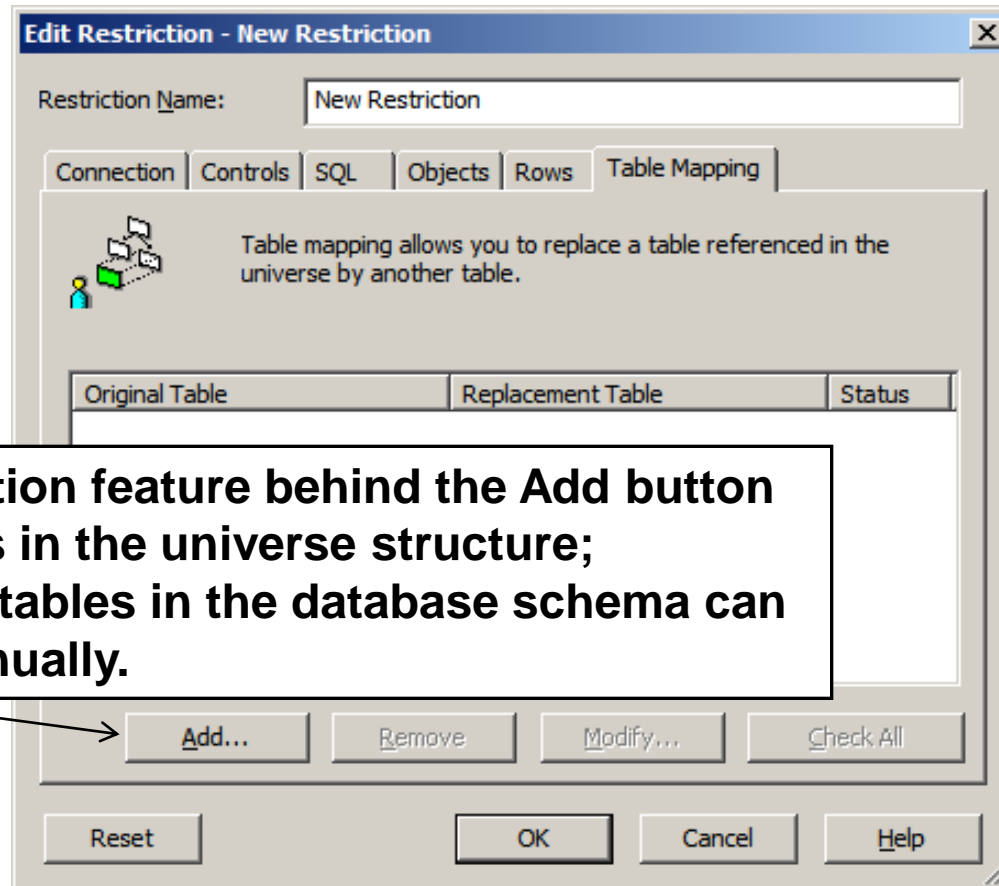
RESTRICTION SET DIALOGS – ROWS

- ▶ Restrict access to universe objects



RESTRICTION SET DIALOGS – TABLE MAPPING

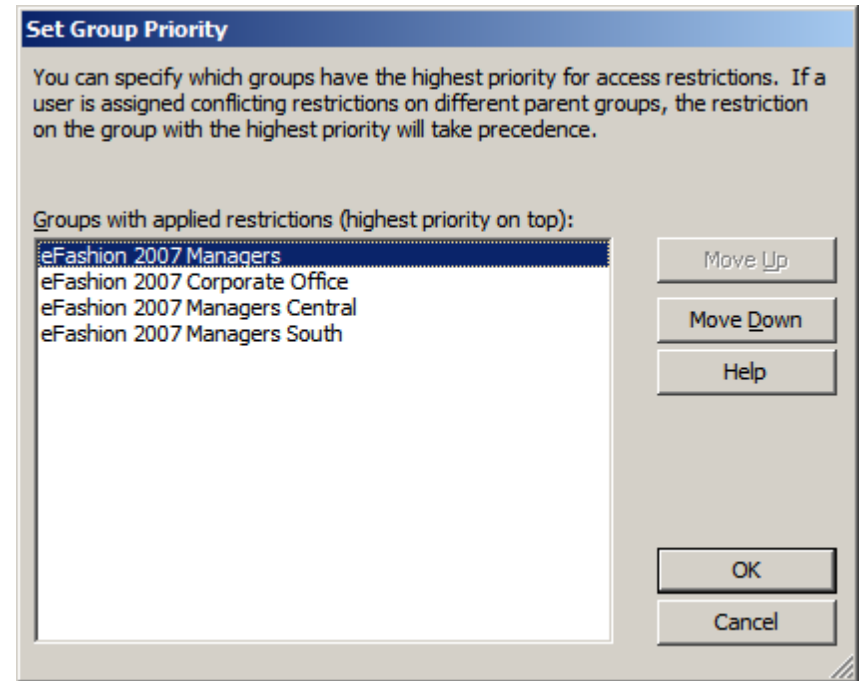
- ▶ Replace a table referenced in the universe by another table in the database



The table selection feature behind the Add button only lists tables in the universe structure; however, other tables in the database schema can be typed in manually.

RESTRICTION PRIORITY

- ▶ Users that belong to multiple groups may have multiple restrictions
- ▶ You can arrange user groups in order. The restriction for the lowest group in the listed order is used
- ▶ Applies only to exclusive restrictions such as connection, table mapping, or SQL controls. ALL object restrictions are applied





RESTRICTION OPTIONS

- ▶ By default, all restrictions are ANDed together
- ▶ When organized into user and group hierarchies, useful to be able to switch between AND and OR
- ▶ This feature was not available in XI Release 1

Restriction Options [X]

You can specify options to manage access restrictions for this universe.

Row Restriction Combination

Combine row restrictions using AND

Combine row restrictions using AND within group hierarchies and OR between groups

OK

Cancel

Help

Verifying the security model

PREVIEWING ACCESS RESTRICTIONS

PREVIEWING RESTRICTION SETS – 1 of 3



- Restrictions can be previewed using the preview button on the editing toolbar

Preview net access restrictions for users or groups

You can view the net result of combining all security restrictions for a user or group, and all parent groups. Select a user or group in the list below, and click Preview to view the net restriction. The list of available users and groups may be filtered using the search criteria.

Available groups and users: 1-7/7 (filtered)

Account Name	Full Name	Description
eFashion 2007		Parent group for eFashion managers
eFashion 2007 Corporate Office		Management in the corporate office
eFashion 2007 Managers		Parent group for all region subgroups
eFashion 2007 Managers Central		Managers in Central region
eFashion 2007 Managers East		Managers in the East region
eFashion 2007 Managers South		Managers in the South region
eFashion 2007 Managers West		Managers in the West region

Search

Search by:

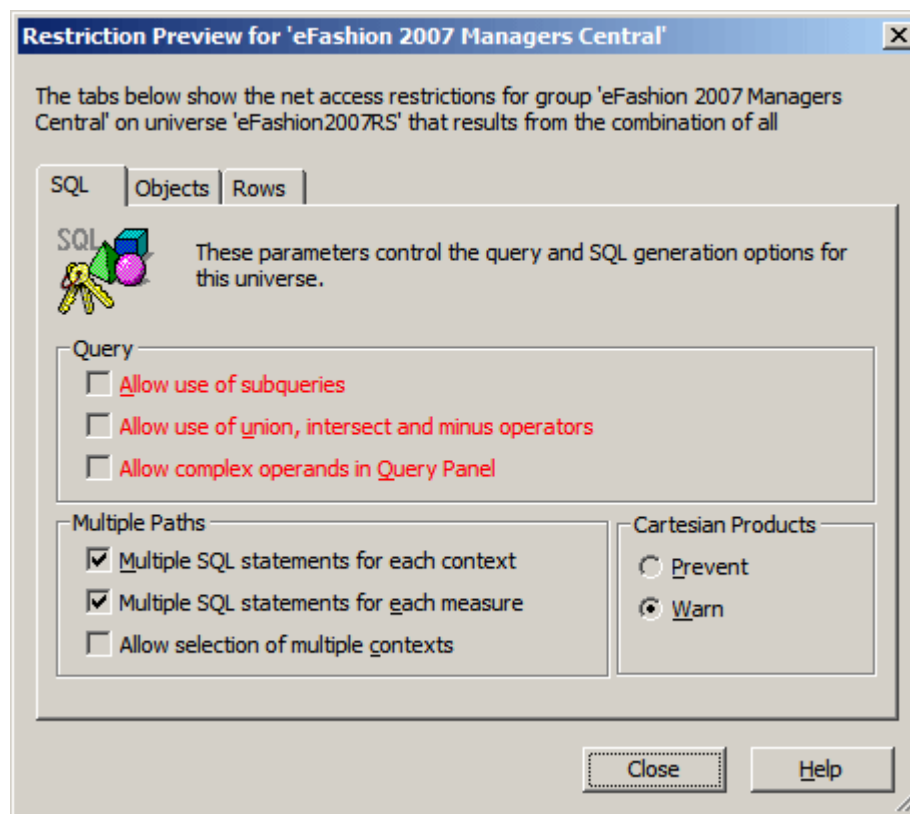
For text:

Look in: Groups Users

PREVIEWING RESTRICTION SETS – 2 of 3



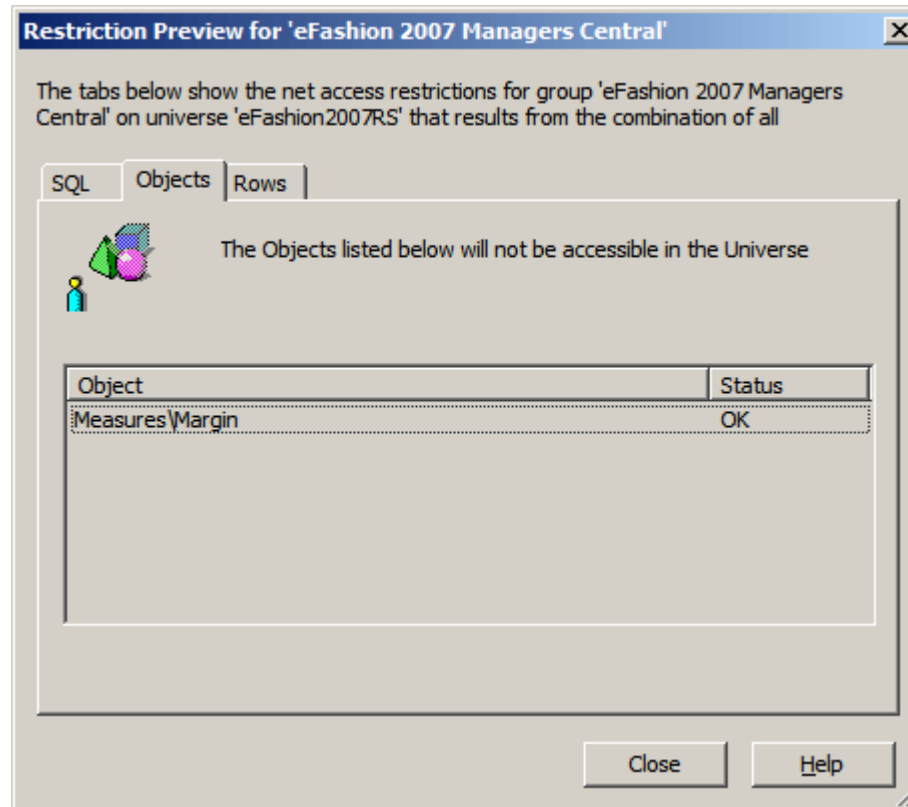
- ▶ Click **preview** to show tabbed dialog showing all restrictions applied to a user or group



PREVIEWING RESTRICTION SETS – 2 of 3



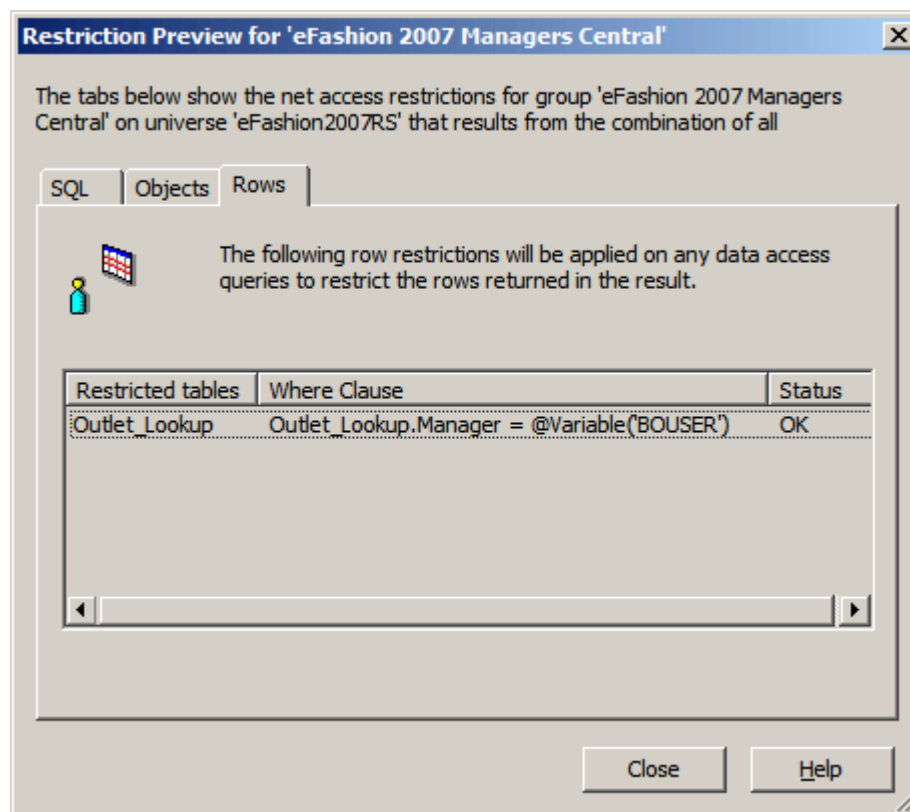
- ▶ Click **preview** to show tabbed dialog showing all restrictions applied to a user or group



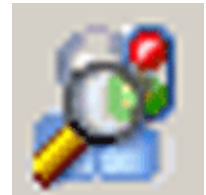
PREVIEWING RESTRICTION SETS – 2 of 3



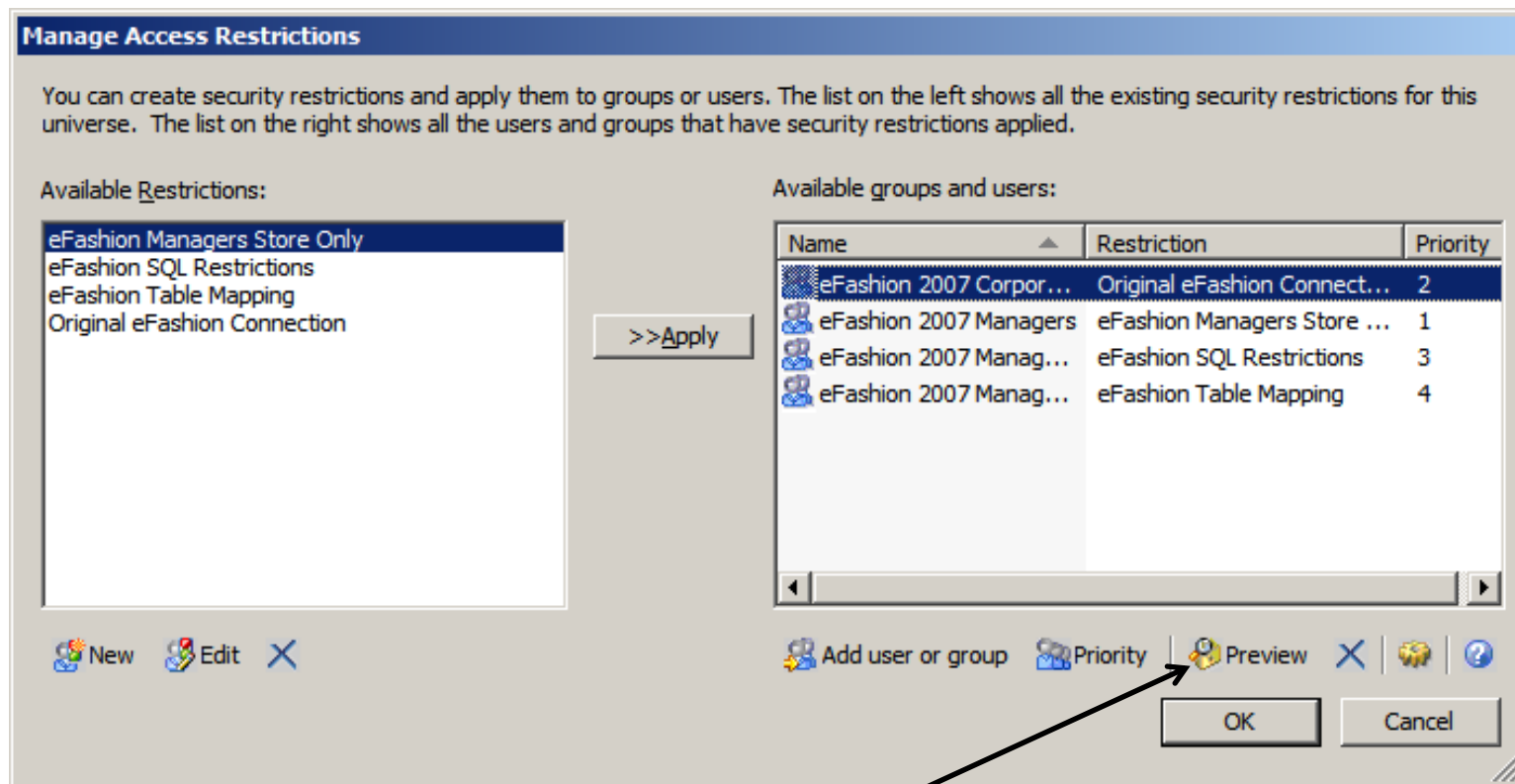
- ▶ Click **preview** to show tabbed dialog showing all restrictions applied to a user or group



PREVIEWING RESTRICTION SETS – 3 of 3



- ▶ Restrictions can also be previewed from the manage access restrictions dialog



Preview cumulative restrictions

Best practices for working with restriction sets

TIPS AND TRICKS

EXPORTING UNIVERSE



- ▶ You must export the universe before you can apply restriction sets
- ▶ Although most changes become effective when a universe is exported, remember that restrictions take effect as soon as they are applied



@AGGREGATE_AWARE

- ▶ The @AGGREGATE_AWARE function can be used to create objects that leverage aggregate tables, where appropriate
- ▶ Make sure that each aggregate table supports your requirements for row-level security
 - ▶ Each aggregate level should have a database column used to store the attribute used as the row-level filter
- ▶ The sample eFashion universe contains aggregates, however, they did not support row-level security for managers, so a modified version of eFashion (without aggregate tables) was used for this presentation

@VARIABLE – 1 of 2

- ▶ The @VARIABLE function is a Business Objects function that can be used for
 - ▶ The text of an interactive object previously created with the @Prompt function; i.e. the first argument entered in the @Prompt function
 - ▶ BusinessObjects system variable such as BOUSER or BOPASS
 - ▶ These variables represent respectively the user name and password forming the user identification

@VARIABLE – 2 of 2

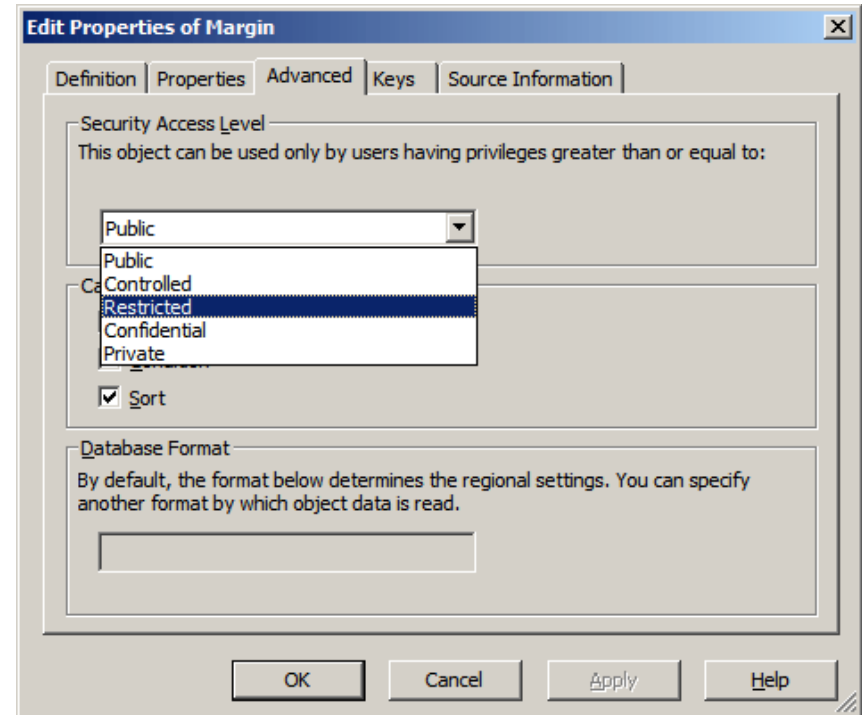
- ▶ System variables also exist for the connection to the RDBMS (DBUSER & DBPASS).
- ▶ @Variable('BOUSER') is useful for creating access restrictions based on user ID
- ▶ The use of @Variable will be explored in one of the demonstrations

Object Level Security

ADDITIONAL CONTENT

OBJECT LEVEL SECURITY – 1 of 3

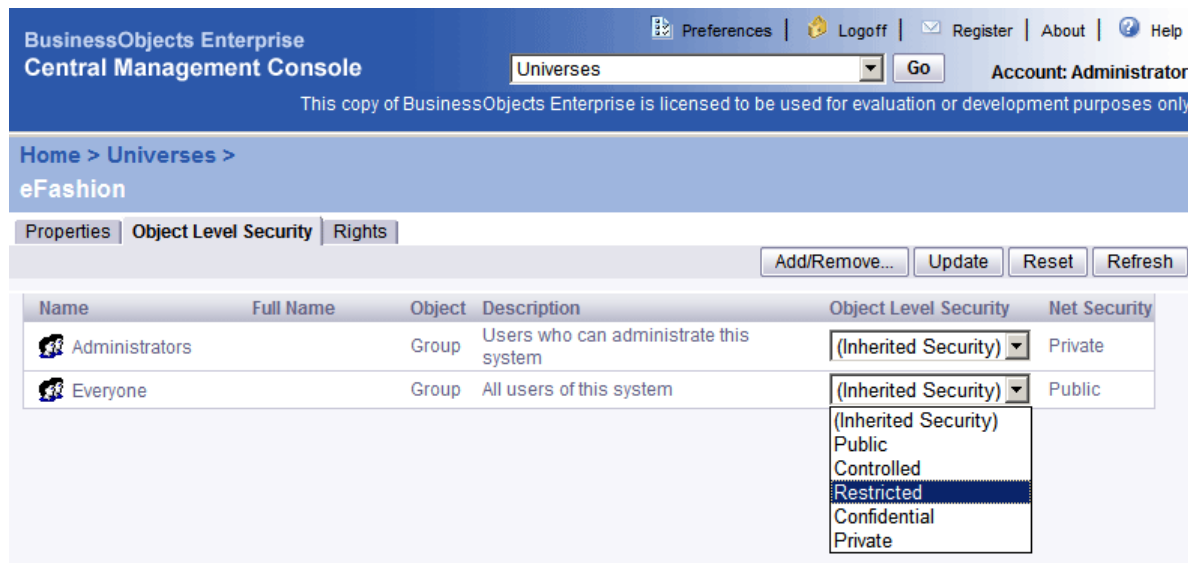
- ▶ A feature called object level security can be used to restrict objects based on five different security levels
 - ▶ Public (default)
 - ▶ Controlled
 - ▶ Restricted
 - ▶ Confidential
 - ▶ Private
- ▶ Object security levels are assigned in Designer from the advanced tab of the object's properties




OBJECT LEVEL SECURITY –

2 of 3

- ▶ An object security level is assigned in the CMC
- ▶ A user must have an object security level equal to or greater to that of an object to be able to use it
- ▶ For example, if a user has an object security level of restricted, that user can use public, controlled or restricted objects, but not confidential or private objects



The screenshot shows the BusinessObjects Enterprise Central Management Console interface. The top navigation bar includes links for Preferences, Logoff, Register, About, and Help. The main content area displays the 'eFashion' universe configuration. The 'Object Level Security' tab is active, showing a table of users and their assigned security levels. A dropdown menu is open for the 'Everyone' user, showing the following options: (Inherited Security), Public, Controlled, Restricted (highlighted), Confidential, and Private.

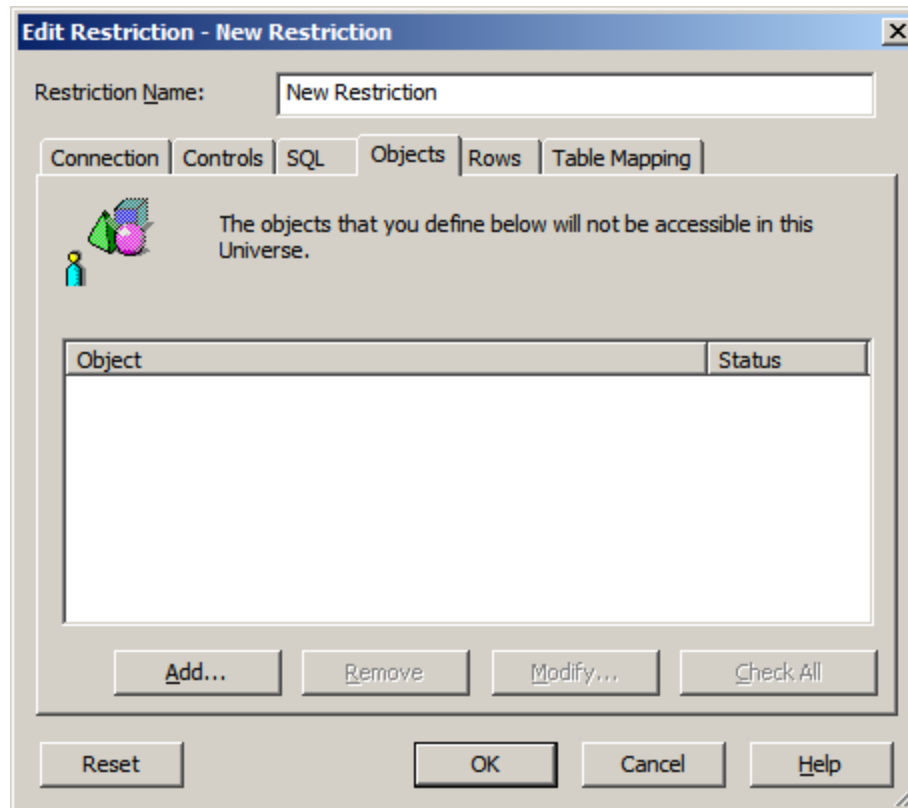
Name	Full Name	Object	Description	Object Level Security	Net Security
 Administrators		Group	Users who can administrate this system	(Inherited Security)	Private
 Everyone		Group	All users of this system	(Inherited Security)	Public

- (Inherited Security)
- Public
- Controlled
- Restricted
- Confidential
- Private

OBJECT LEVEL SECURITY –

3 of 3

- ▶ Although the effect is similar, maintaining object security is generally easier using restriction sets rather than object level security

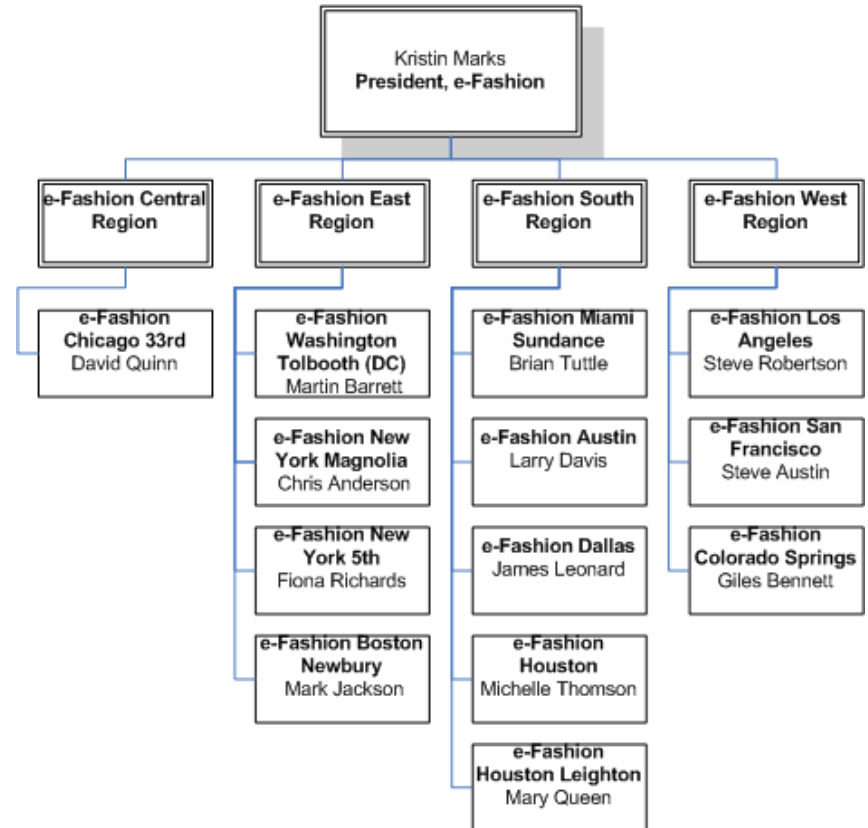


- 1) Creating and previewing a restriction set
- 2) Restriction options
- 3) Restriction priority
- 4) Using the schedule for option

LIVE DEMONSTRATIONS

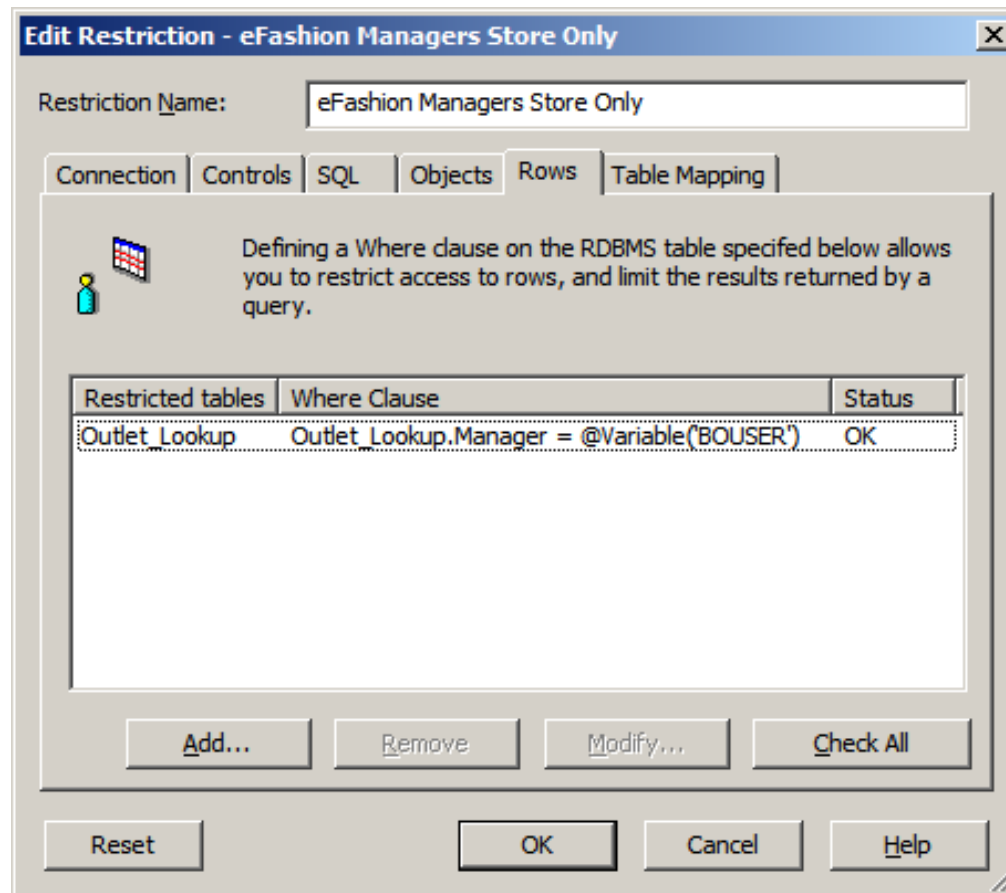
DEMO 1: CREATING AND PREVIEWING A RESTRICTION SET

- ▶ Goal: Limit managers' data access to their own stores
- ▶ Goal: Restrict manager's access to **margin** object



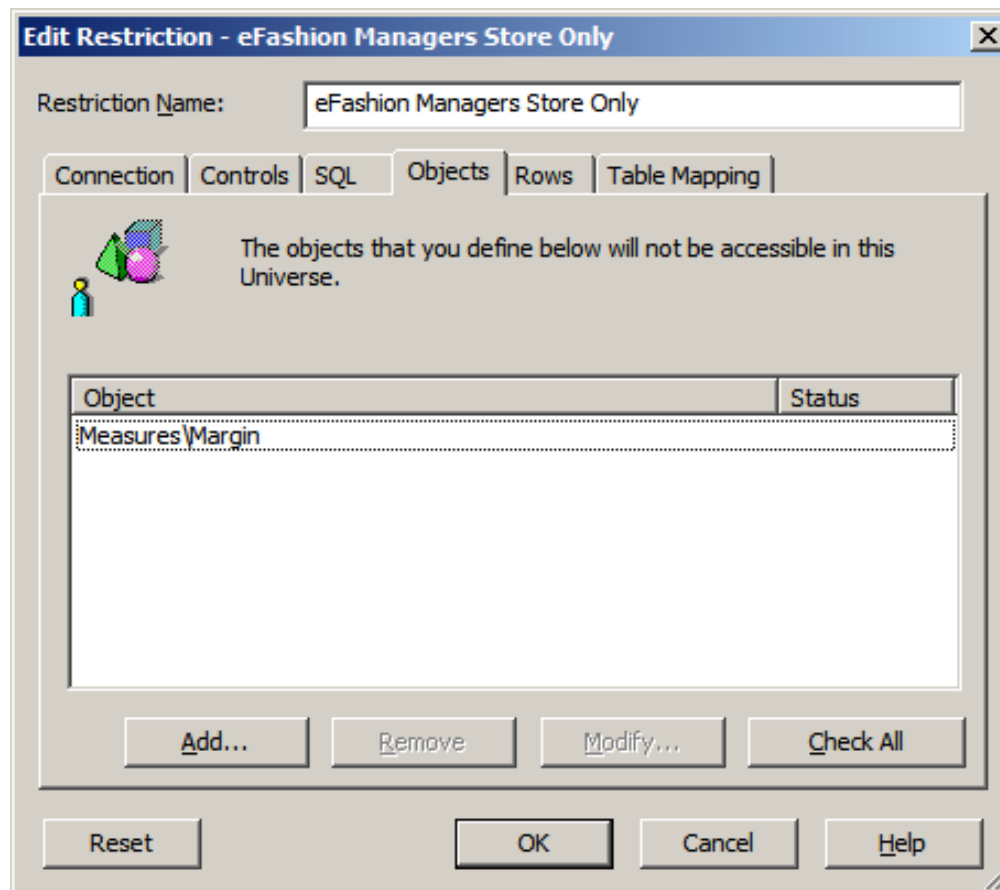
DEMO 1: CREATING AND PREVIEWING A RESTRICTION SET

- ▶ Solution: Limit row access to own stores by creating row restriction using `@Variable('BOUSER')`



DEMO 1: CREATING AND PREVIEWING A RESTRICTION SET

- ▶ Solution: Create object restriction to hide margin object



DEMO 1: CREATING AND PREVIEWING A RESTRICTION SET

- ▶ Test object restrictions for manager Chris Anderson

The screenshot displays a software interface for managing user access. On the left, a vertical list of users is shown, with 'e-Fashion New York Magnolia Chris Anderson' highlighted in red. The main window, titled 'Preview net access restrictions for users or groups', contains a table of available users. 'Anderson Chris Anderson' is selected. Below the table are search and look-in options. A secondary window, 'Restriction Preview for 'Anderson'', shows a table of restricted tables with a where clause: 'Outlet_Lookup Outlet_Lookup.Manager = @Variable('BOUSER') OK'.

Account Name	Full Name	Description
Administrator		Administrator account
Administrators		Users who can administrate this system
Anderson	Chris Anderson	e-Fashion New York Magnolia
Barrett	Martin Barrett	e-Fashion Washington Tolbooth (DC)
Bennett	Gles Bennett	e-Fashion Colorado Springs manager
BusinessObjects NT Users		BusinessObjects NT Users can use their NT user accounts to log ...
Dataspace		Group to identify all users added for
Dataspace Management		A group used for publication demo.
Dataspace No Admin		A group that specifically denies acc
Dataspace Staff		A group used for publication demo.

Restricted tables	Where Clause	Status
Outlet_Lookup	Outlet_Lookup.Manager = @Variable('BOUSER')	OK

DEMO 2: RESTRICTION OPTIONS



- ▶ Show the effect of cumulative restrictions by using subgroups
- ▶ A1 is a parent group, with A2 and A3 as nested subgroups
- ▶ B1 is a peer group to A1
Irene is a member of both groups



Insight 2007 A1
Irene, Iggy
Year = 2003



Insight 2007 B1
Irene
Year = 2001



Insight 2007 A2
Ivan
State = Texas



Insight 2007 A3
Isabella
City = Dallas

DEMO 2: RESTRICTION OPTIONS



- ▶ Demonstrate the effect of both options (AND/OR), using user Irene in the Insight 2007 A1 and Insight 2007 B1 security groups


Insight 2007 A1
Irene, Iggy
Year = 2003


Insight 2007 B1
Irene
Year = 2001


Insight 2007 A2
Ivan
State = Texas


Insight 2007 A3
Isabella
City = Dallas

Restriction Options [X]

You can specify options to manage access restrictions for this universe.

Row Restriction Combination

Combine row restrictions using AND

Combine row restrictions using AND within group hierarchies and OR between groups

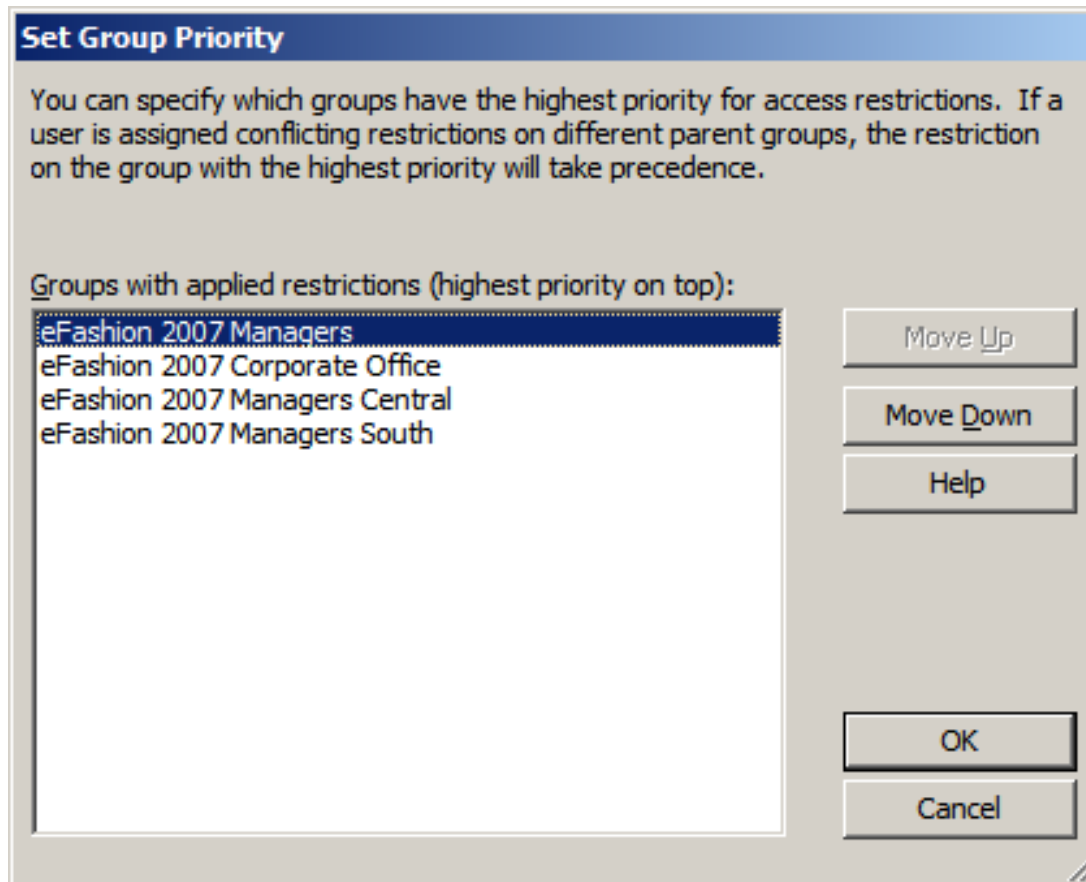
OK

Cancel

Help

DEMO 3: RESTRICTION PRIORITY

- ▶ Determine the effect of priority when a user receives restrictions from more than one restriction set



DEMO 4: USING THE SCHEDULE FOR OPTION

- ▶ The **schedule for** feature allows you to generate reports that contain data for specific users only
- ▶ You can schedule an object and specify for which users or groups you want the system to run the object
- ▶ The system will run the object for each user applying the universe restrictions appropriate to the user

The screenshot displays the BusinessObjects Enterprise Central Management Console interface. The breadcrumb trail is 'Home > Folders > Web Intelligence Samples > Web Intelligence Sample'. The 'Schedule' tab is selected in the top navigation bar. Below the navigation, there are sub-tabs for 'Notification', 'Destination', 'Format', 'Caching Options', and 'Schedule For'. The 'Schedule For' sub-tab is active. The main content area contains the following text: 'Specify which users or user groups to schedule the object for. An instance of the object will be created for each user.' There are two radio button options: 'Schedule only for myself.' (unselected) and 'Schedule for specified users and user groups.' (selected). Below these options is a 'Scheduling list' section with an 'Add/Remove...' button. The list contains one entry: 'eFashion 2007 Managers (Group)'. At the bottom right of the form are 'Update' and 'Reset' buttons.

FOR MORE INFORMATION

- ▶ BusinessObjects documentation
 - ▶ BusinessObjects XI Release 2 Designer's Guide (pp. 441-450)
 - ▶ BusinessObjects Enterprise Administrator's Guide
- ▶ Business Objects XI: The Complete Reference
by Cindi Howson
 - ▶ Chapter 13, Securing the System, (pp. 312-326)
 - ▶ McGraw-Hill/Osborne 2006
 - ▶ ISBN 0-07-226265-6



CONCLUSION

- ▶ Restriction sets allow universe behavior to be tailored and secured for individuals or groups
- ▶ In addition to row and column-level security, restriction sets can override connection, query control, and SQL generation options
- ▶ Restriction set priority can be controlled for users that belong to multiple security groups

- ▶ Questions
 - ▶ Dallas Marks
 - ▶ I will repeat questions to ensure everyone can hear

- ▶ Contact information
 - ▶ Email Dallas AT dallasmarks.org
 - ▶ [Dallas Marks on Business Intelligence](#)
 - ▶ [Dallas Marks on Twitter](#)