SAP BusinessObjects security in 60 minutes - A template-based approach

Alan Mayer
Solid Ground Technologies, Inc.

In This Session ...

- Understand the complexities behind BusinessObjects security
- Learn a template-based method that greatly simplifies the creation and maintenance of your security rules
- See how this method can be applied to all corporate environments – from simple to complex
- Automate everyday tasks such as account creation, report design, and administrative responsibilities
- Use the templates provided to kick-start your own optimized security model

What We'll Cover …

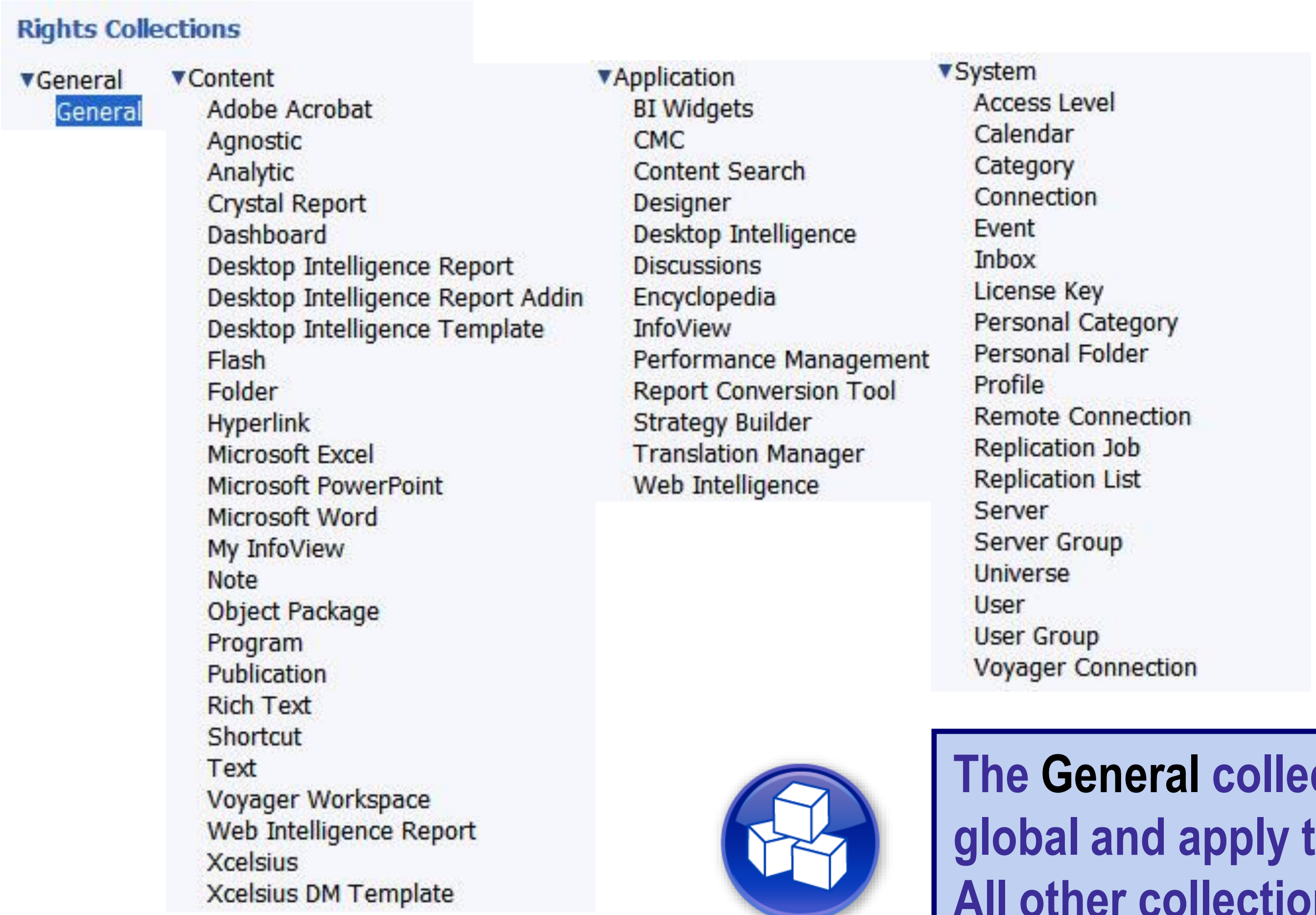
- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

Essentials of BusinessObjects Security

- A good security model does one thing
  - Applies the correct permission on an object for a recipient
- Sounds simple, right?
- The complexity lies in the details as the next few slides will demonstrate

Rights

- Hundreds of available rights can be applied



Rights Collections

▼General
- General

▼Content
- Adobe Acrobat
- Agnostic
- Analytic
- Crystal Report
- Dashboard
- Desktop Intelligence Report
- Desktop Intelligence Report Addin
- Desktop Intelligence Template
- Flash
- Folder
- Hyperlink
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Word
- My InfoView
- Note
- Object Package
- Program
- Publication
- Rich Text
- Shortcut
- Text
- Voyager Workspace
- Web Intelligence Report
- Xcelsius
- Xcelsius DM Template

▼Application
- BI Widgets
- CMC
- Content Search
- Designer
- Desktop Intelligence
- Discussions
- Encyclopedia
- InfoView
- Performance Management
- Report Conversion Tool
- Strategy Builder
- Translation Manager
- Web Intelligence

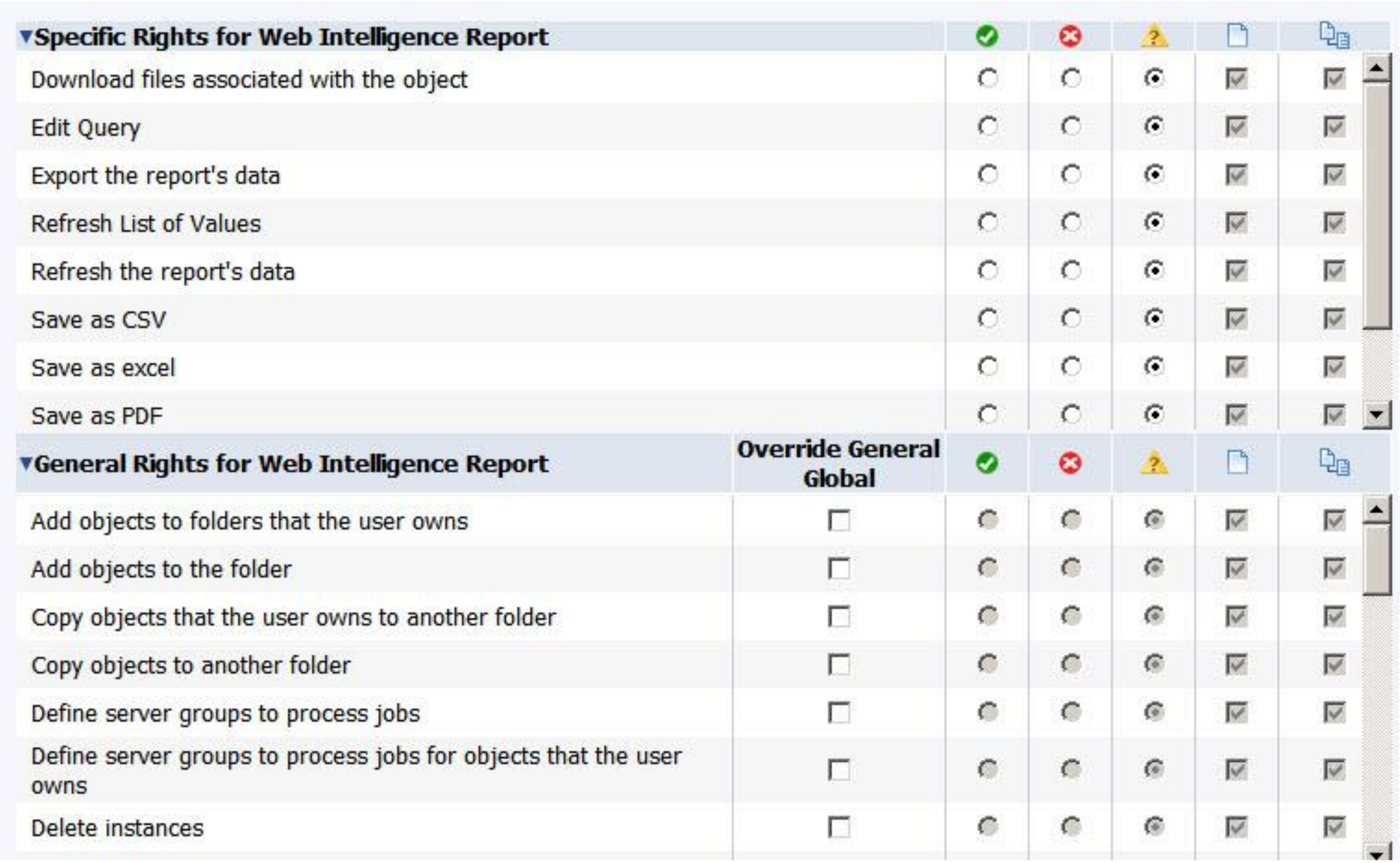
▼System
- Access Level
- Calendar
- Category
- Connection
- Event
- Inbox
- License Key
- Personal Category
- Personal Folder
- Profile
- Remote Connection
- Replication Job
- Replication List
- Server
- Server Group
- Universe
- User
- User Group
- Voyager Connection

Building Blocks

The **General** collection is global and apply to all rights. All other collections include specific rights for that type.

The Anatomy of a Right

- A collection can have general (global) and specific rights



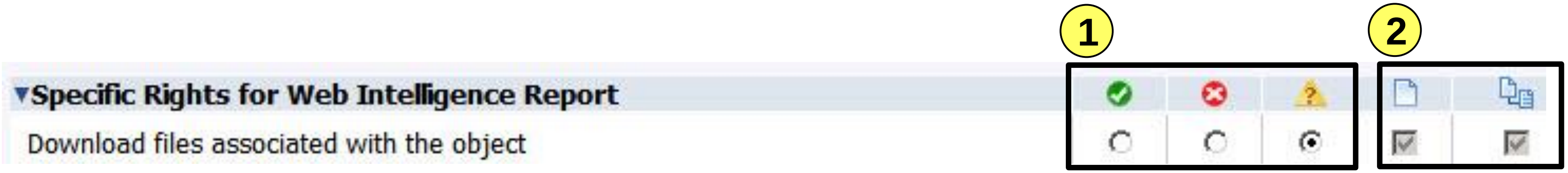
▾Specific Rights for Web Intelligence Report	✓	✗	⚠	🗎	⧉
Download files associated with the object	○	○	●	☑	☑
Edit Query	○	○	●	☑	☑
Export the report's data	○	○	●	☑	☑
Refresh List of Values	○	○	●	☑	☑
Refresh the report's data	○	○	●	☑	☑
Save as CSV	○	○	●	☑	☑
Save as excel	○	○	●	☑	☑
Save as PDF	○	○	●	☑	☑

▾General Rights for Web Intelligence Report	Override General Global	✓	✗	⚠	🗎	⧉
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	□	○	○	●	☑	☑
Define server groups to process jobs	□	○	○	●	☑	☑
Define server groups to process jobs for objects that the user owns	□	○	○	●	☑	☑
Delete instances	□	○	○	●	☑	☑

Building Blocks

The Anatomy of a Right, cont'd

- Lots of information available for a single right



▾Specific Rights for Web Intelligence Report

	✓	✗	?		
Download files associated with the object	○	○	●	☑	☑

1 Type of right

- In general, Denials > Grants > Not Specified
- There are exceptions to this rule (trumping)

2 Scope

- Apply at one level only (NoCascade)
- Apply at this level and all sublevels (Cascade)

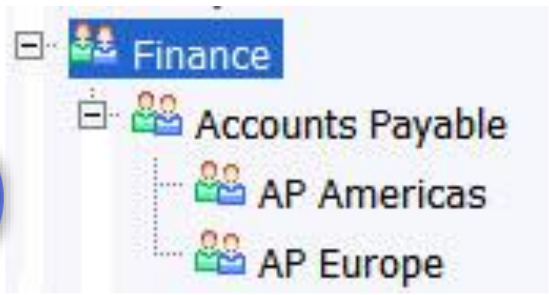
Building Blocks

Objects

- Many types of objects need to be secured
  - Folders
  - Reports
  - Universes
    - Universe connections
    - Universe restrictions
  - Applications
  - Events
  - Server Groups
  - Users
  - User Groups

Applying Privileges

- Privileges can be directly applied to a recipient or inherited
  - Recipients are usually users or groups or users
- The general rule is to directly set privileges on groups as early as possible, then let inheritance take over
  - "Early" here means as close to the top level of security as possible
  - This rule will allow you to create your security model with the fewest number of rules



Finance
- Accounts Payable
  - AP Americas
  - AP Europe

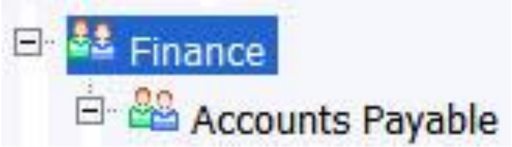
There is a global top level for most objects where security can be set. Rights set at this level are inherited by all groups.

Building Blocks

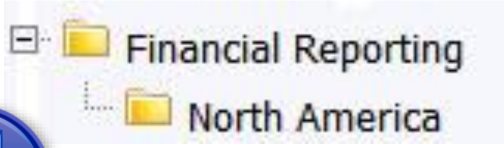
Inheritance

- BusinessObjects employs a “double inheritance” scheme
  - A user or group can inherit privileges from its parent group
  - An object can inherit privileges from its parent folder

Group Inheritance



Folder Inheritance



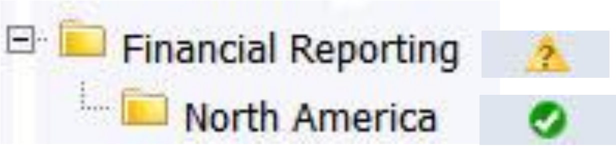
Caution

It is this scheme that causes the most trouble if a security model is designed incorrectly.

Building Blocks

Overriding Inherited Security

- Inherited privileges can be overridden several ways
  - By setting permissions closer to the intended recipient

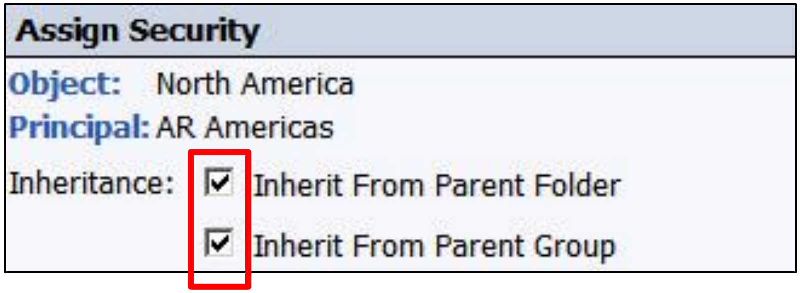


⊟ Financial Reporting ⚠
North America ✓

Not specified - Refresh report data (Effective Denial)

Direct grant - Refresh report data

  - By deliberately breaking inheritance



Assign Security

Object: North America

Principal: AR Americas

Inheritance: ☑ Inherit From Parent Folder

☑ Inherit From Parent Group

Removing inheritance by clearing the check boxes is not a good idea in general. It makes maintaining and troubleshooting your security model harder.

Building Blocks

Too Complicated?

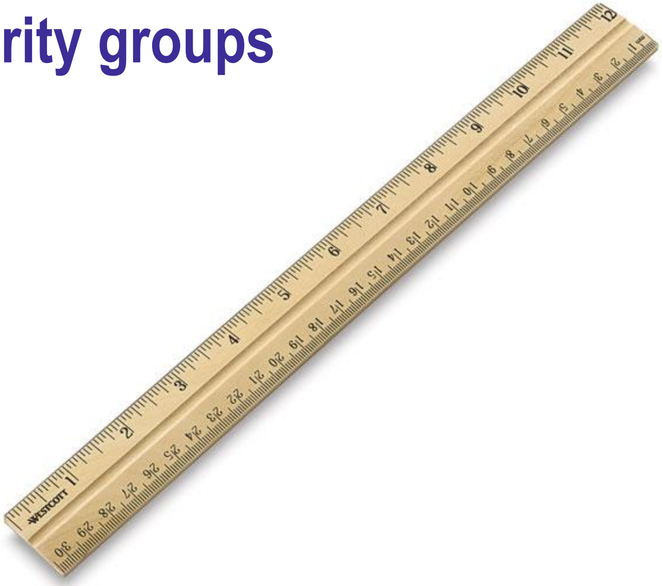
- Exactly!
  - We've only touched the high points
  - Haven't discussed how an administrator can maintain or report on assigned permissions
- There is a MUCH easier way to model security in BusinessObjects
  - Hopefully that's why you're attending this session

What We'll Cover …

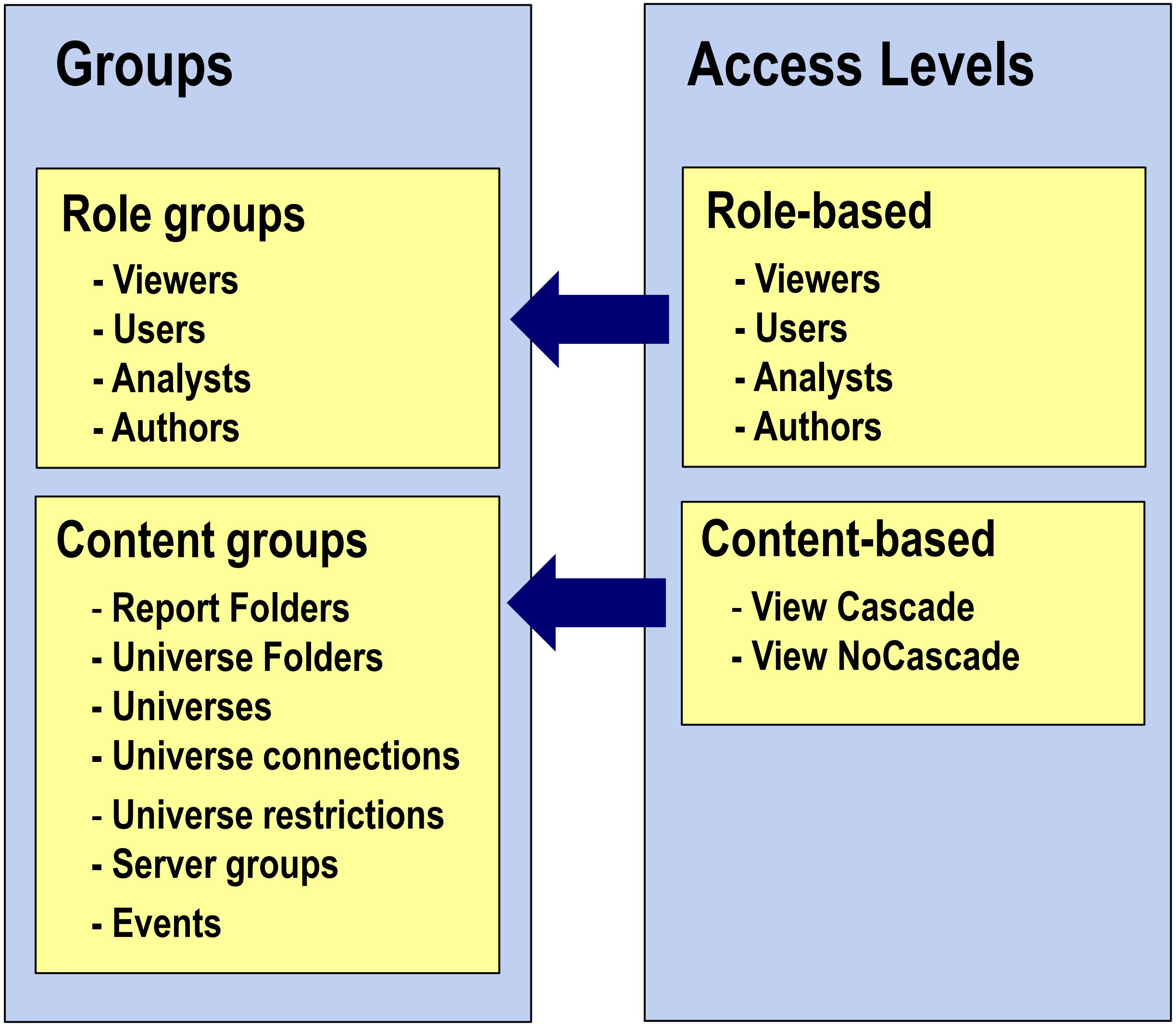
- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

Rules Behind Template-Based Security

- Combine privileges into easier to manage levels
  - Levels can be driven by the types of users involved
    - Viewers, Users, Analysts, Authors, …
- Create groups that those privileges will target
  - Two specific types: Role-based and Content-based
  - Different privileges allocated to each
- The combination of access levels and security groups is your template
- Apply templates across available objects
  - Objects include folders, reports, groups, universes, connections, …



The BusinessObjects Template Model



Groups

Role groups
- Viewers
- Users
- Analysts
- Authors

Content groups
- Report Folders
- Universe Folders
- Universes
- Universe connections
- Universe restrictions
- Server groups
- Events

Access Levels

Role-based
- Viewers
- Users
- Analysts
- Authors

Content-based
- View Cascade
- View NoCascade

The Most Important Rule …

- Role-based access levels control all rights EXCEPT viewing
  - General rights like Add / Delete / Edit
  - Specific rights like Refresh Report Data
- Content-based access levels controls ONLY viewing
  - All general viewing rights
  - Right to view reports and report instances
  - Right to view whether you own the object or not
  - Scope also controlled (one level or cascaded)

Key Feature

Preparing for Templates

- We’ll walk you through the process of creating templates
  - 1. Identify likely custom access levels
  - 2. Create a set of security groups
  - 3. Applying the resulting templates in various scenarios
- The resulting model has been battle-tested
  - Companies from 10 to 12,000+ users

Checklist

What We'll Cover …

- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

Access Level Types

- Two types of access levels to consider
  - Role
    - Based on a user's role
    - Viewer, User, Analyst, Author, …
  - Override
    - Collections of related grants / denials
    - Combined with core access levels to achieve a particular result
    - Example: A core User role with the NoSchedule Override to prevent scheduling
  - A user may be granted one role for an object area and many overrides

Access Level Naming Conventions

- A good naming convention for your custom access levels will speed their adoption and minimize operational mistakes
  - Role Access Levels
    - Custom_Role_<User Type>
    - Assume that all role privileges will cascade

Examples:

Custom_Role_Viewer
Custom_Role_User
Custom_Role_Analyst

Some customers use numbers or abbreviations like ‘aa’ rather than ‘Custom-’ to get the access levels to sort alphabetically near the top

Best Practice

Access Level Naming Conventions, cont’d

- A good naming convention for your custom access levels will speed their adoption and minimize operational mistakes
  - Override Access Levels
    - Custom_Override_<Short Privilege Description>
    - Begin description with ‘No’ to indicate denials
    - End description with ‘NoCascade’ when override applies to one level only

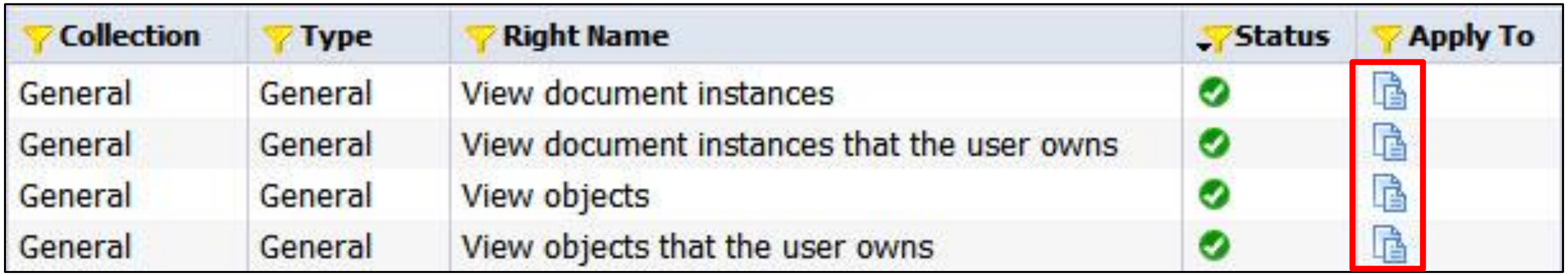
Examples:

Custom_Override_AddEdit
Custom_Override_NoSchedule

Best Practice

A Special Override for Content

- Controlling whether a user can view particular content is allowed through dedicated overrides
  - Custom_Override_View_Cascade

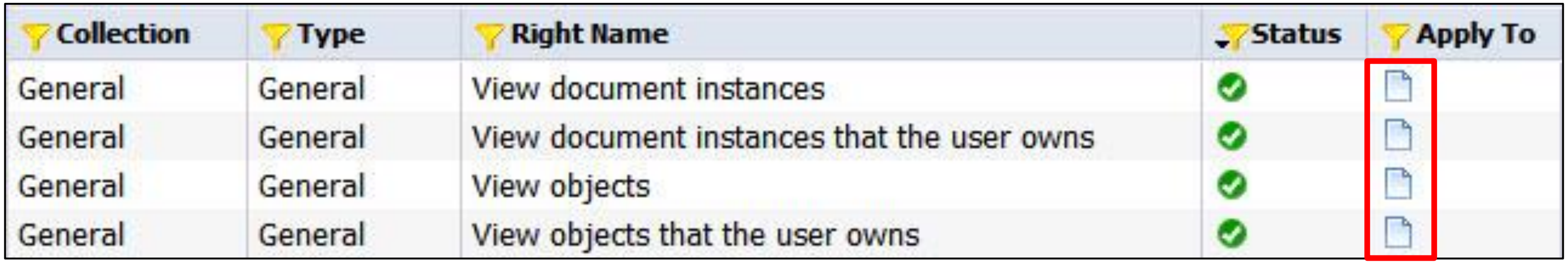


Collection	Type	Right Name	Status	Apply To
General	General	View document instances	✓	🗐
General	General	View document instances that the user owns	✓	🗐
General	General	View objects	✓	🗐
General	General	View objects that the user owns	✓	🗐

Note how two pages appear rather than one. This indicates that the Cascade feature has been set.

A Special Override for Content, cont’d

- Controlling whether a user can view particular content is allowed through dedicated overrides
  - Custom_Override_View_NoCascade

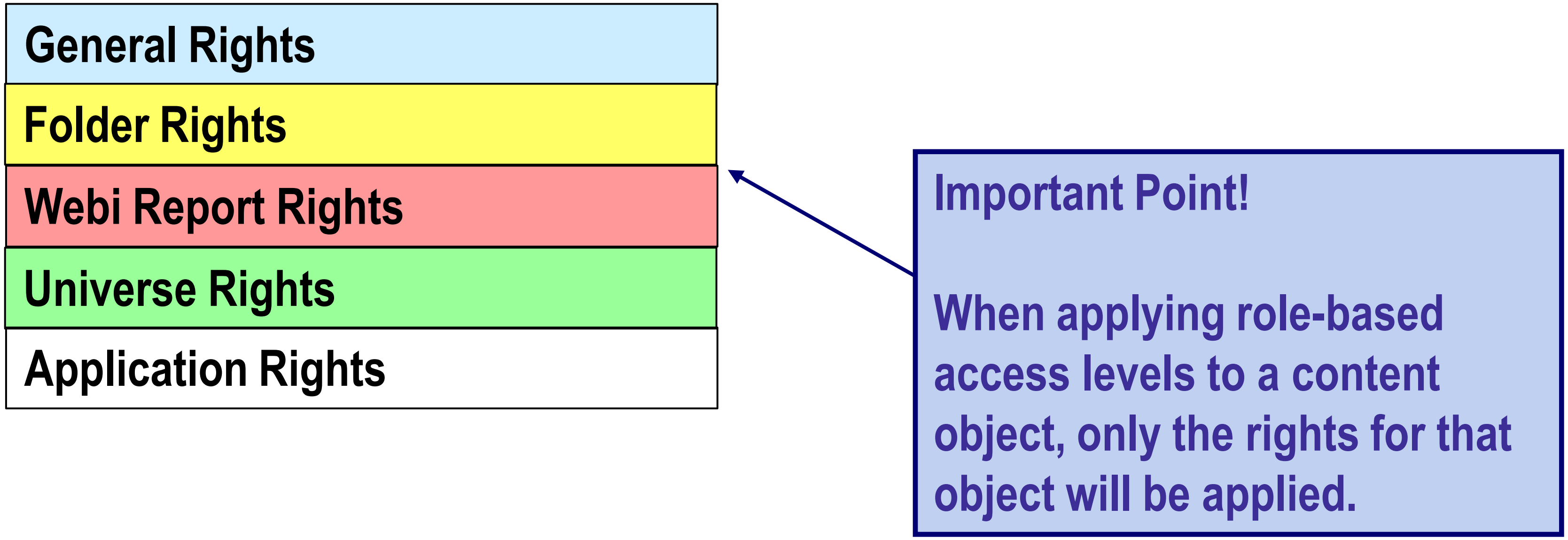


Collection	Type	Right Name	Status	Apply To
General	General	View document instances	✓	📄
General	General	View document instances that the user owns	✓	📄
General	General	View objects	✓	📄
General	General	View objects that the user owns	✓	📄

One page indicates that the right is allowed for the one level. The NoCascade feature has been set.

Collective Rights for a Role

- The final set of rights granted to an access level might cover many different content types



General Rights

Folder Rights

Webi Report Rights

Universe Rights

Application Rights

Important Point!

When applying role-based access levels to a content object, only the rights for that object will be applied.

Heads-Up

The Viewer Role

- A viewer should be able to see previously scheduled reports
- Report can be printed and exported to PDF and Excel
- No refreshing is allowed

The Viewer Role - Rights

Collection	Type	Right
Application	Infoview	Log on to Infoview
Application	Infoview	Do an advanced search
Application	Infoview	Change user's preferences
Application	Web Intelligence	Log on to Web Intelligence
Application	Web Intelligence	Enable interactive HTML viewing
Content	Web Intelligence Report	Export the report's data
Content	Web Intelligence Report	Save as excel
Content	Web Intelligence Report	Save as PDF

Some rights have not been shown on the slide for clarity. See the provided BIAR archive for a list of all rights for this access level.

The User Role

- A user can do everything a viewer can
- In addition:
  - Refresh reports
  - Schedule reports
  - Create shortcuts for Public reports under Favorites

The User Role - Rights

Collection	Type	Right
System	Universe	Data access
System	Connection	Data access
Content	Shortcut	Add objects to folders that the user owns
General	General	Schedule document to run
General	General	Reschedule instances that the user owns
Application	Infoview	View the favorites folder
Application	Infoview	View the Inbox
Content	Web Intelligence Report	Refresh the report's data
Content	Web Intellgence Report	Use Lists of Values

Some rights have not been shown on the slide for clarity and brevity. Viewer rights have been omitted among others.

The Analyst Role

- An analyst can do everything a user can
- In addition:
  - Create private queries and reports
  - Modify existing reports that they own

The Analyst Role - Rights

Collection	Type	Right
Application	Web Intelligence	Create document
Application	Web Intelligence	Enable Java Report Panel
Application	Web Intelligence	Enable formula and variable creation
Application	Web Intelligence	Interactive: General – Enable toolbar and menus
Application	Web Intelligence	Interactive: General – Enable right click menu
Application	Web Intelligence	Merge dimensions for synchronization
System	Universe	Create and Edit Queries Based on Universe
Content	Web Intelligence Report	View SQL

Some rights have not been shown on the slide for clarity and brevity. Viewer and user rights have been omitted among others.

The Author Role

- An author can do everything an analyst can
- In addition:
  - Create public queries and reports
  - Modify existing public reports regardless of owner

The Author Role - Rights

Collection	Type	Right
General	General	Add objects to the folder
General	General	Copy objects to another folder
General	General	Edit objects

Some rights have not been shown on the slide for clarity and brevity. Viewer, user, and analyst rights have been omitted among others.

Speciality Roles - Publisher

- Has all the rights of an author
- In addition:
  - Can create publications

Speciality Roles - Admins

- Allows a smaller set of users to act as delegated administrators
- Privileges vary widely depending on intent
  - Full Control
    - Ability to do anything for particular content area
  - Limited Control
    - Create and maintain additional users
    - Assign new users to their areas

The Favorites Content Area

- All users by default are Administrators over their own Favorites folder
- Translation: They have extra privileges in this area that were never intended
  - Example:
    - Suppose a User can copy a public report to Favorites
    - Under the Favorites folder, the user can modify the report
    - This privilege is NOT part of a User’s access level

Problem

Popular Overrides

- Group privileges by major action

Custom_Override_Schedule

Collection	Type	Right
General	General	Schedule documents to run
General	General	Schedule to destinations
General	General	Pause and resume instances
General	General	Reschedule instances

Tip

Popular Overrides, continued

- Provide negative (denial) version of same override

Custom_Override_NoSchedule

Collection	Type	Right
General	General	Schedule documents to run (Denied)
General	General	Schedule to destinations (Denied)
General	General	Pause and resume instances (Denied)
General	General	Reschedule instances (Denied)

Tip

Popular Overrides, continued

- Group related actions together

Custom_Override_AddEdit

Collection	Type	Right
General	General	Add objects to the folder
General	General	Copy objects to the folder
General	General	Edit objects

Tip

What We'll Cover …

- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

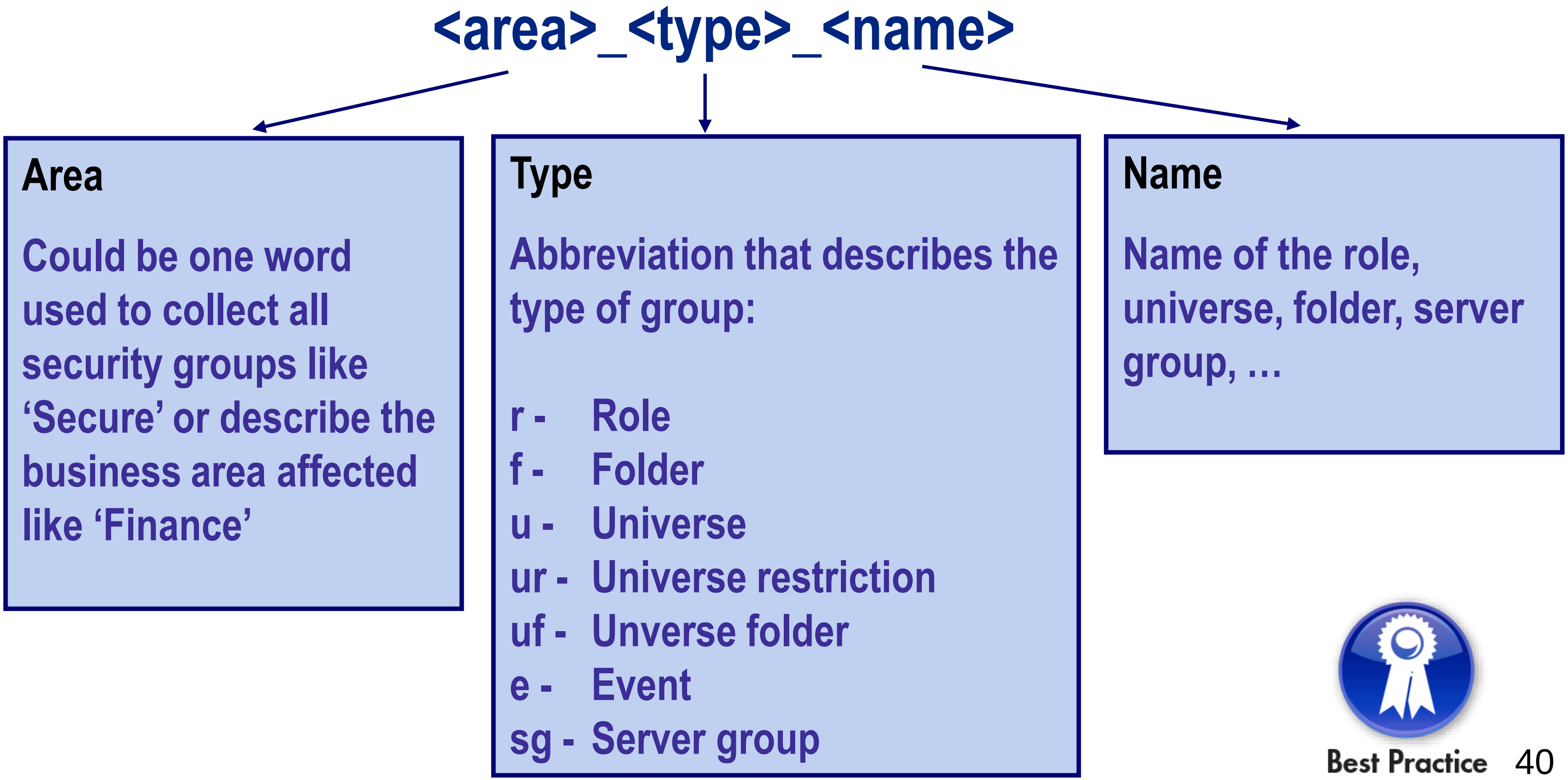
Security Groups

- These groups will serve as the recipients of custom access levels previously defined
- Two types of groups allowed:
  - Role
    - Can receive role-based access levels and overrides
  - Content
    - Can ONLY receive View-based overrides

Heads-Up

Security Group Naming Convention

- A good naming convention will do wonders for administrators looking to use and maintain these groups



<area>_<type>_<name>

Area

Could be one word used to collect all security groups like ‘Secure’ or describe the business area affected like ‘Finance’

Type

Abbreviation that describes the type of group:

r -	Role
f -	Folder
u -	Universe
ur -	Universe restriction
uf -	Unverse folder
e -	Event
sg -	Server group

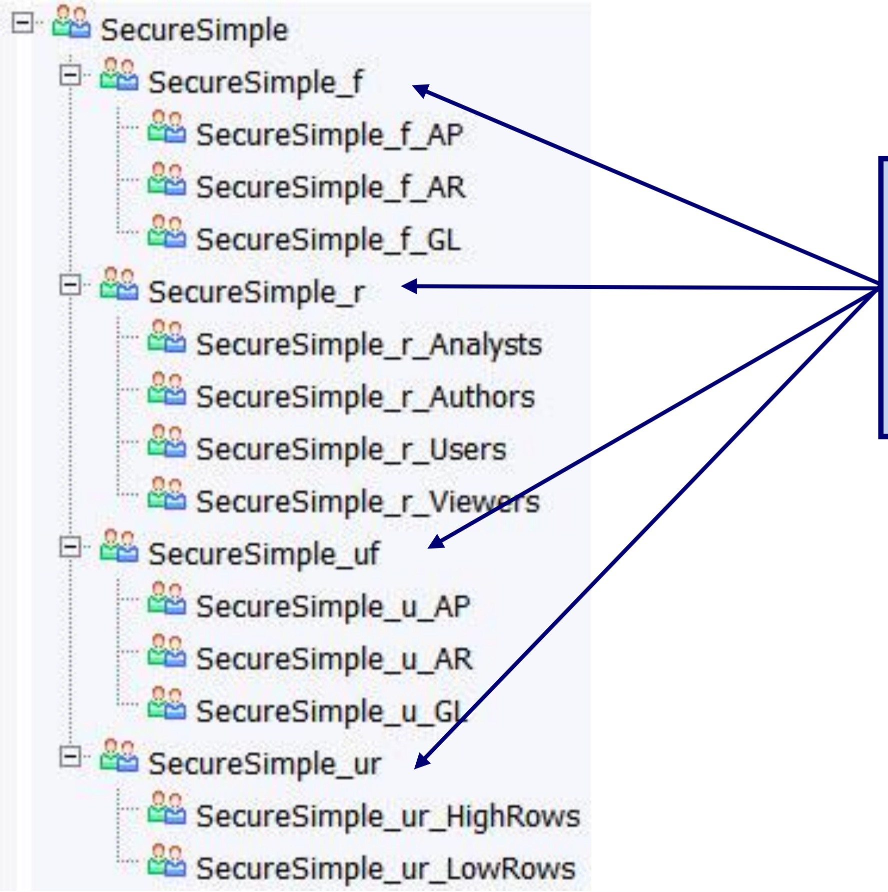
Name

Name of the role, universe, folder, server group, …

Best Practice

Security Group Hierarchies

- Arranging groups in a hierarchy will make it easier to find and maintain them



- SecureSimple
  - SecureSimple_f
    - SecureSimple_f_AP
    - SecureSimple_f_AR
    - SecureSimple_f_GL
  - SecureSimple_r
    - SecureSimple_r_Analysts
    - SecureSimple_r_Authors
    - SecureSimple_r_Users
    - SecureSimple_r_Viewers
  - SecureSimple_uf
    - SecureSimple_u_AP
    - SecureSimple_u_AR
    - SecureSimple_u_GL
  - SecureSimple_ur
    - SecureSimple_ur_HighRows
    - SecureSimple_ur_LowRows

Parent groups are very important! Use them when assigning rights for ALL child groups.

Best Practice

What We'll Cover …

- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

Simple Scenario: Assumptions

- Your company wants to adopt a template-driven security scheme after returning home from the conference
- Users can be slotted against one role (Viewer, User, Analyst, …)
- No user will be in more than one role …. ever.
- A user will be assigned to one role group and one more content groups

Viewer

User

Analyst

Author

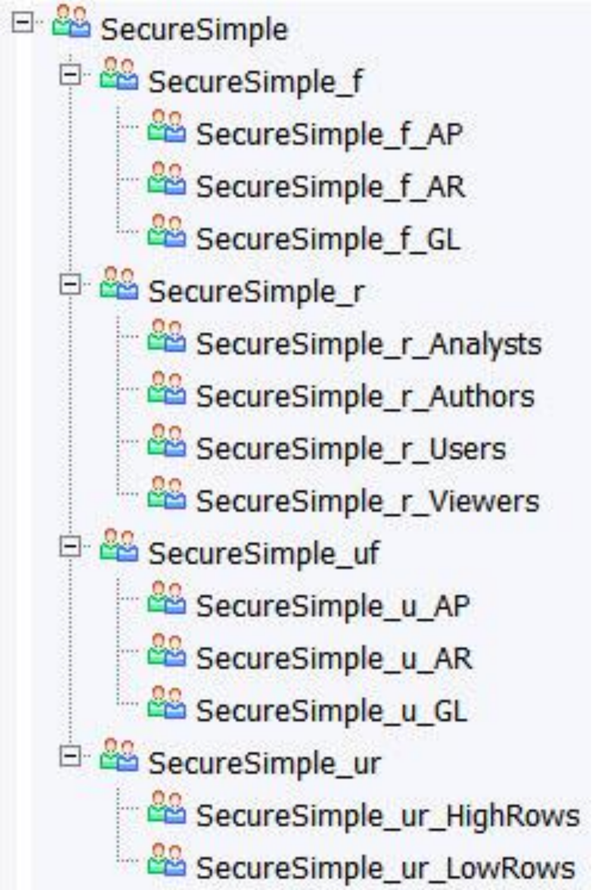
Simple Scenario: Access Levels

- You've created the following custom access levels as part of your template (at minimum):

Access Levels
Custom_Role_Viewer
Custom_Role_User
Custom_Role_Analyst
Custom_Role_Author
Custom_Override_View_Cascade
Custom_Override_View_NoCascade

Simple Scenario: Groups

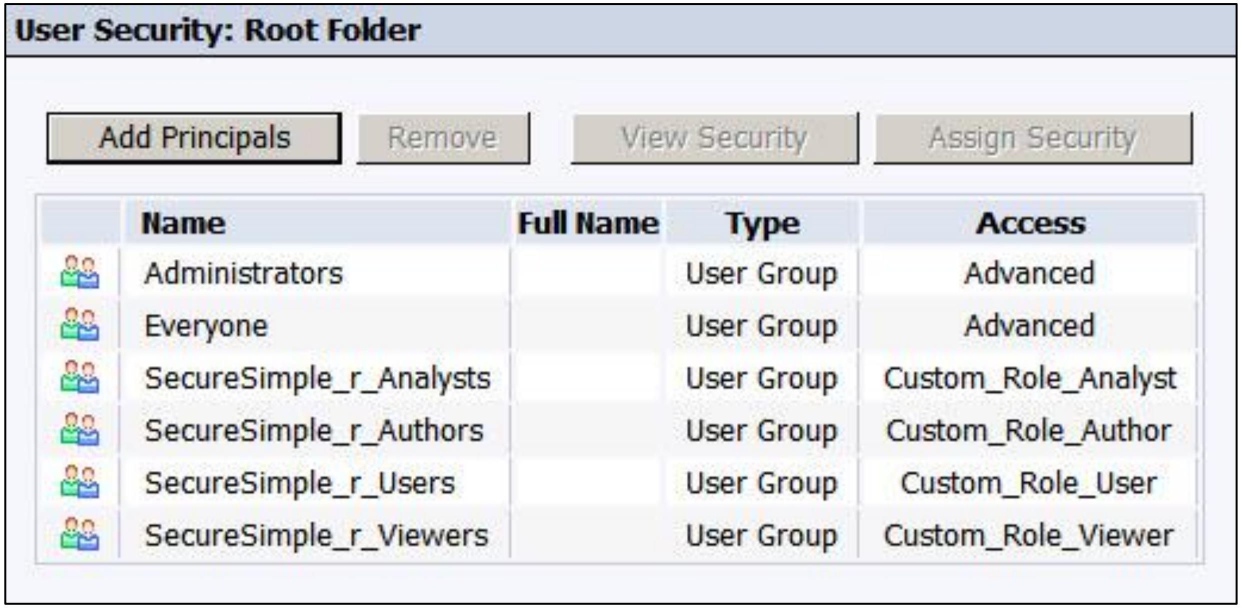
- You’ve created the following group hierarchy as part of your template



- SecureSimple
  - SecureSimple_f
    - SecureSimple_f_AP
    - SecureSimple_f_AR
    - SecureSimple_f_GL
  - SecureSimple_r
    - SecureSimple_r_Analysts
    - SecureSimple_r_Authors
    - SecureSimple_r_Users
    - SecureSimple_r_Viewers
  - SecureSimple_uf
    - SecureSimple_u_AP
    - SecureSimple_u_AR
    - SecureSimple_u_GL
  - SecureSimple_ur
    - SecureSimple_ur_HighRows
    - SecureSimple_ur_LowRows

Simple Scenario: Report Content

- Set role-based security at the global folder level
  - Folders > Manage > Top-Level Security

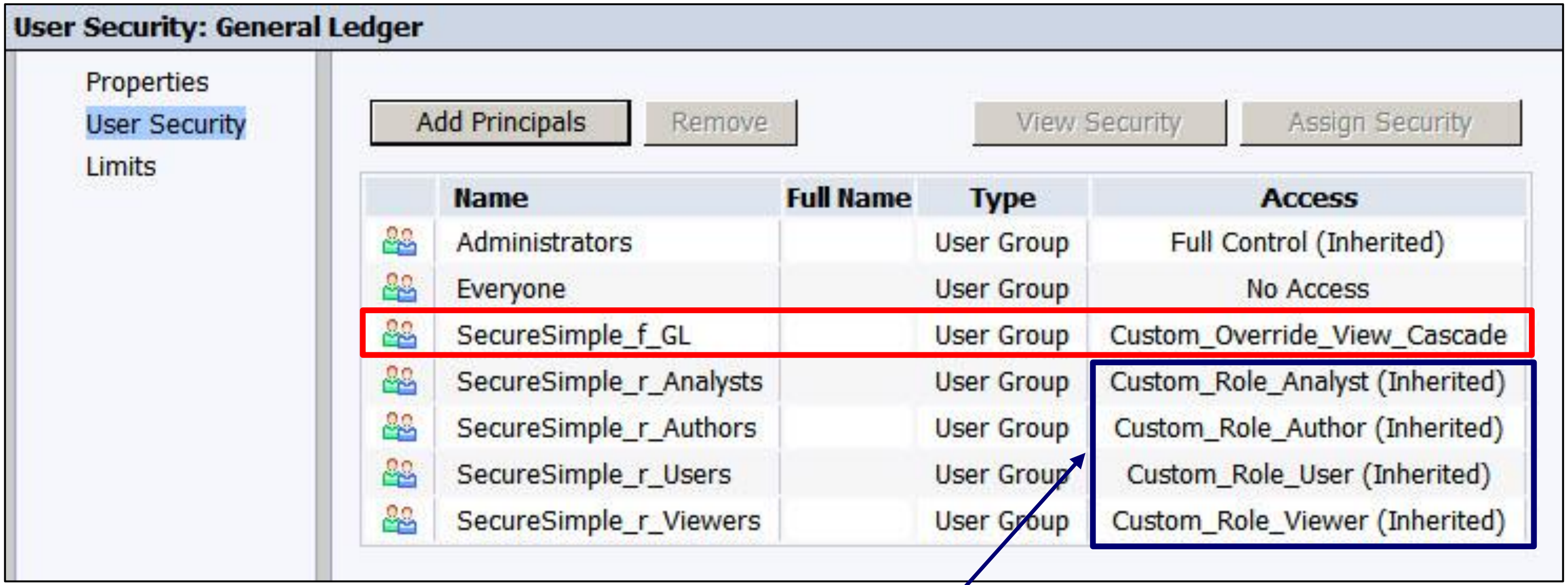


User Security: Root Folder

Name	Full Name	Type	Access
Administrators		User Group	Advanced
Everyone		User Group	Advanced
SecureSimple_r_Analysts		User Group	Custom_Role_Analyst
SecureSimple_r_Authors		User Group	Custom_Role_Author
SecureSimple_r_Users		User Group	Custom_Role_User
SecureSimple_r_Viewers		User Group	Custom_Role_Viewer

Simple Scenario: Report Content, cont’d

- Set content-based security at each top-level folder if possible



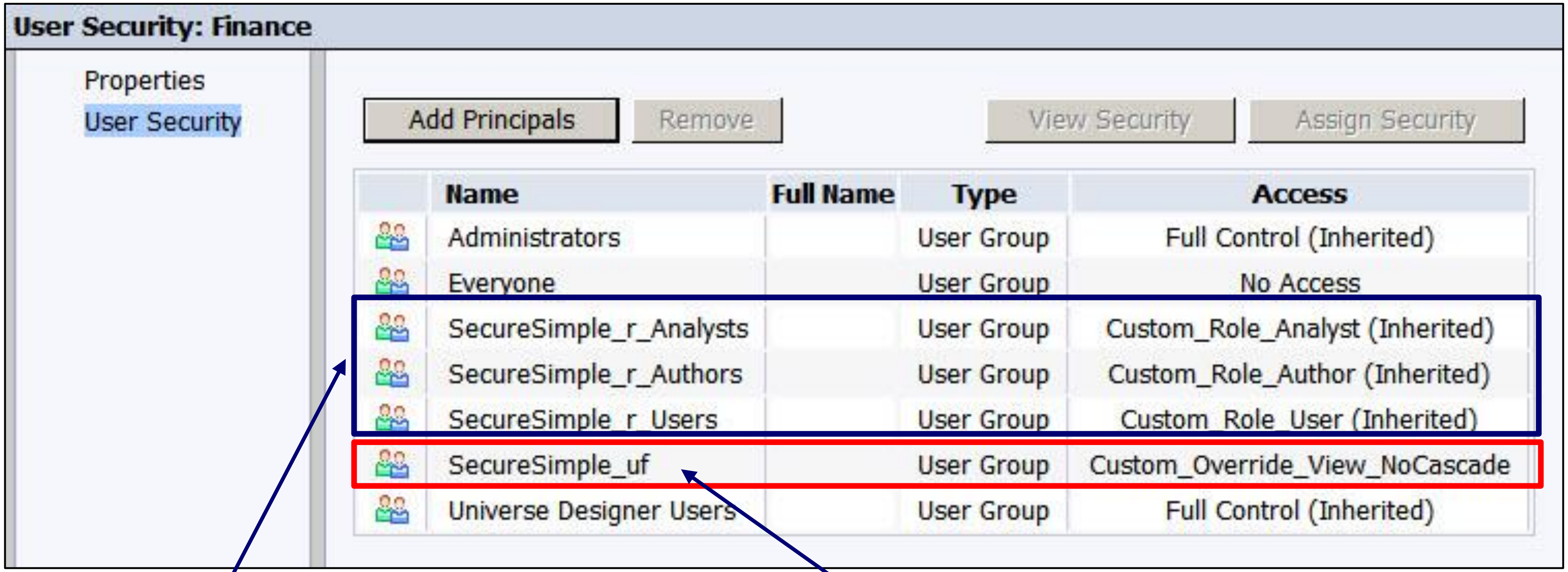
User Security: General Ledger

Name	Full Name	Type	Access
Administrators		User Group	Full Control (Inherited)
Everyone		User Group	No Access
SecureSimple_f_GL		User Group	Custom_Override_View_Cascade
SecureSimple_r_Analysts		User Group	Custom_Role_Analyst (Inherited)
SecureSimple_r_Authors		User Group	Custom_Role_Author (Inherited)
SecureSimple_r_Users		User Group	Custom_Role_User (Inherited)
SecureSimple_r_Viewers		User Group	Custom_Role_Viewer (Inherited)

Role-based privileges are inherited from the root folder for reports

Simple Scenario: Universe Folders

- Set role-based rights at the global universe root folder
- All the universe folder to be viewed by all Finance users



User Security: Finance

Properties
User Security

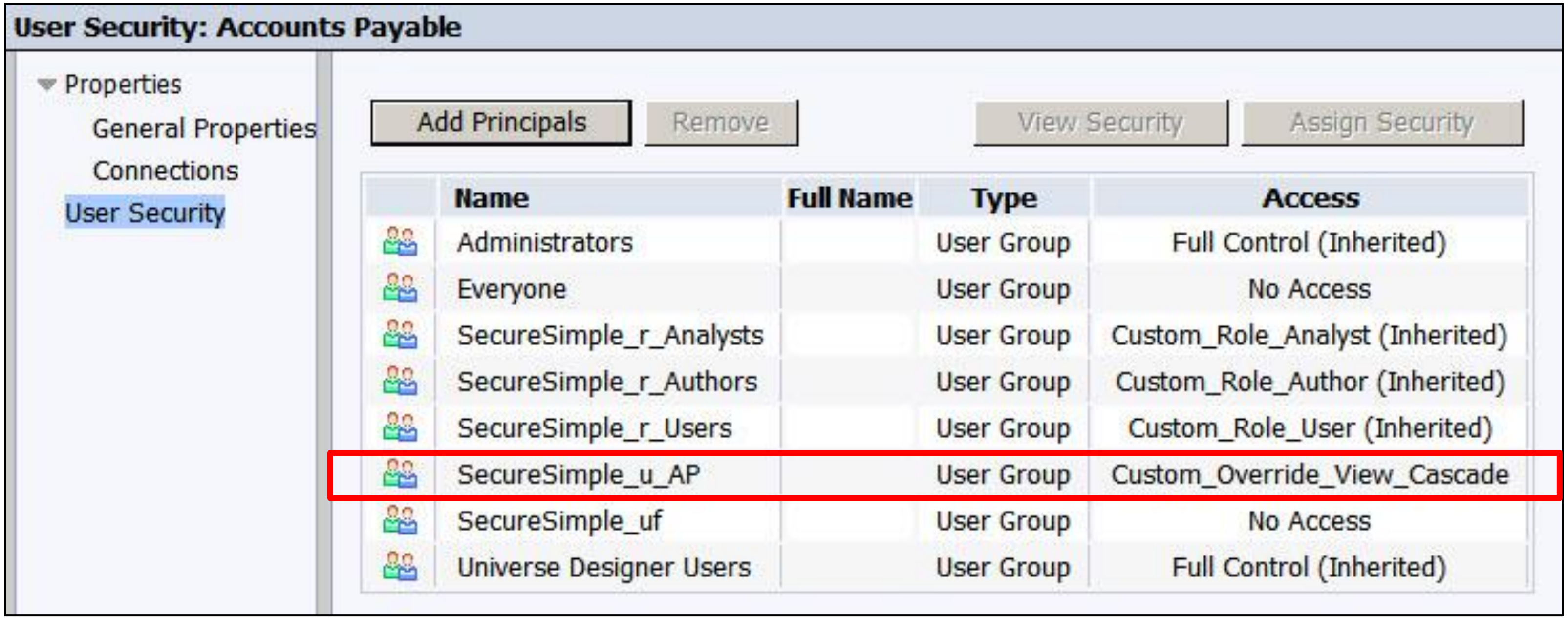
	Name	Full Name	Type	Access
	Administrators		User Group	Full Control (Inherited)
	Everyone		User Group	No Access
	SecureSimple_r_Analysts		User Group	Custom_Role_Analyst (Inherited)
	SecureSimple_r_Authors		User Group	Custom_Role_Author (Inherited)
	SecureSimple_r_Users		User Group	Custom_Role_User (Inherited)
	SecureSimple_uf		User Group	Custom_Override_View_NoCascade
	Universe Designer Users		User Group	Full Control (Inherited)

Viewers were not considered because they cannot refresh.

The parent universe group was given read-only access.

Simple Scenario: Universes

- Set content rights (viewing) per universe



User Security: Accounts Payable

	Name	Full Name	Type	Access
	Administrators		User Group	Full Control (Inherited)
	Everyone		User Group	No Access
	SecureSimple_r_Analysts		User Group	Custom_Role_Analyst (Inherited)
	SecureSimple_r_Authors		User Group	Custom_Role_Author (Inherited)
	SecureSimple_r_Users		User Group	Custom_Role_User (Inherited)
	SecureSimple_u_AP		User Group	Custom_Override_View_Cascade
	SecureSimple_uf		User Group	No Access
	Universe Designer Users		User Group	Full Control (Inherited)

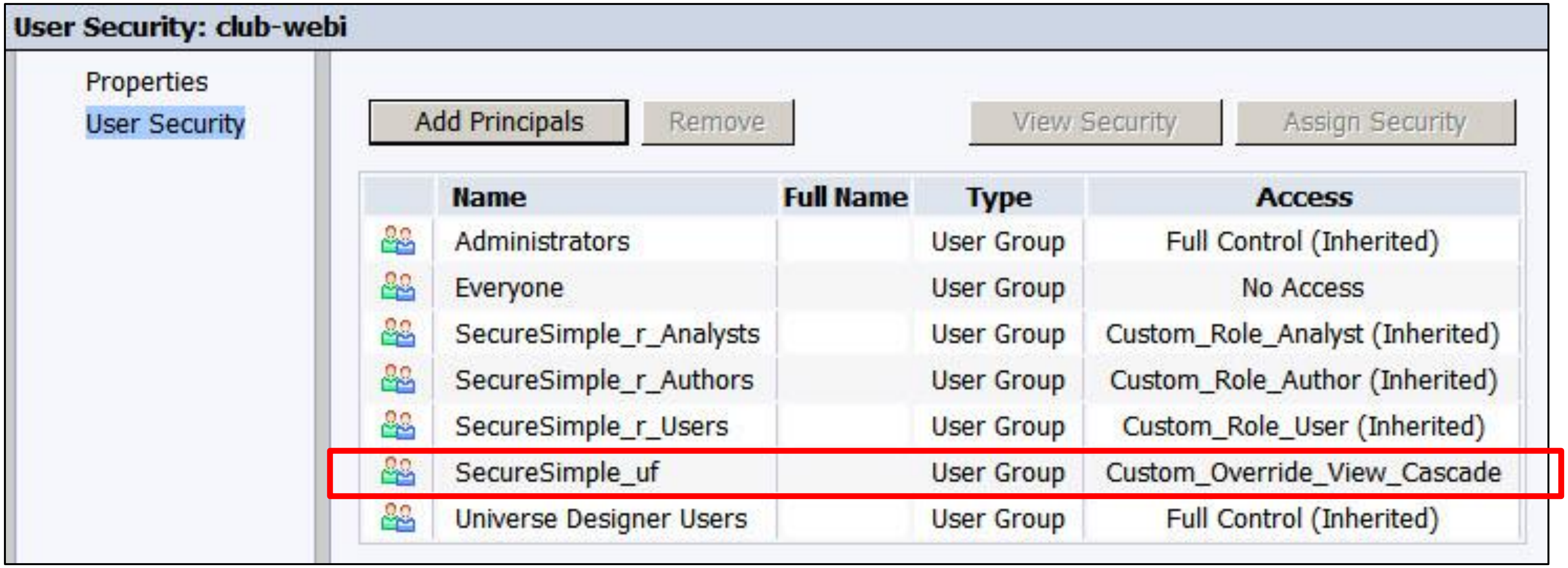
Simple Scenario: Universe Restrictions

- Being a member of the universe restriction group is sufficient
- No explicit security rules for restrictions
  - They do not appear in the CMC
  - Created and visible in the Universe Designer

Tip

Simple Scenario: Connections

- Top-level security must be set for role groups
- Connection security is set by universe or universe folders
    - Sometimes available to Everyone
    - For the simple scenario, we'll set by universe folder

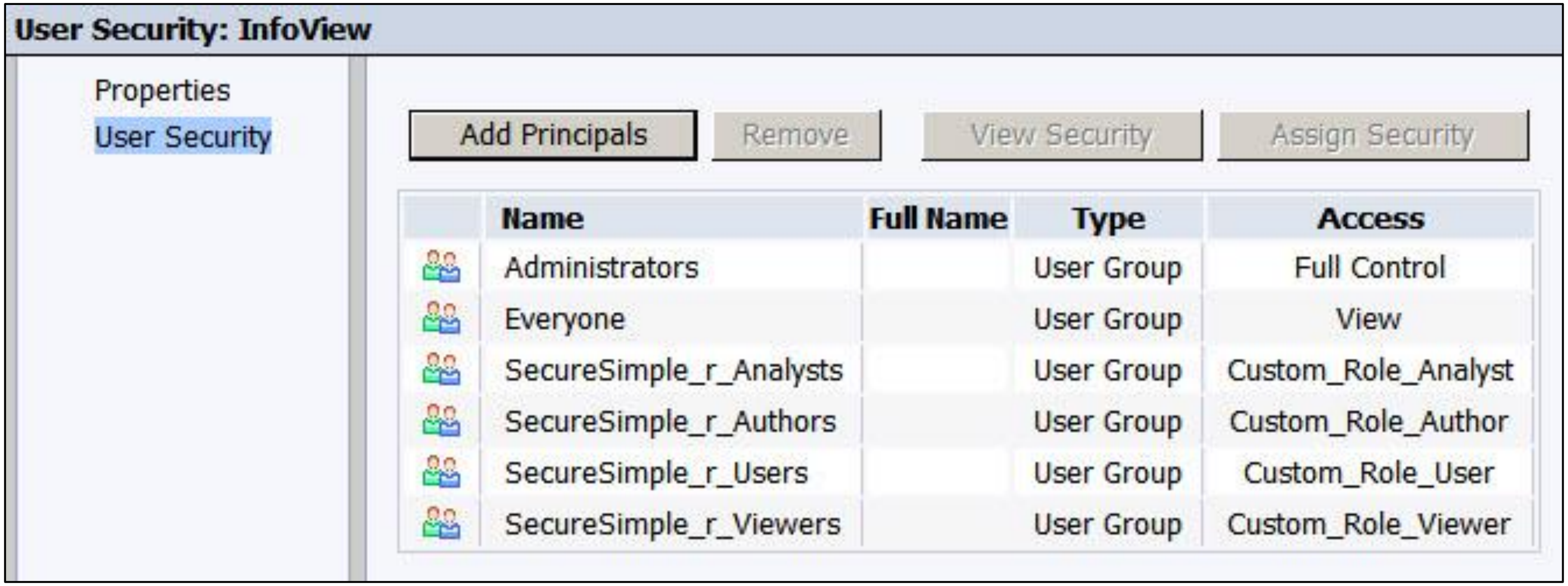


User Security: club-webi

Name	Full Name	Type	Access
Administrators		User Group	Full Control (Inherited)
Everyone		User Group	No Access
SecureSimple_r_Analysts		User Group	Custom_Role_Analyst (Inherited)
SecureSimple_r_Authors		User Group	Custom_Role_Author (Inherited)
SecureSimple_r_Users		User Group	Custom_Role_User (Inherited)
SecureSimple_uf		User Group	Custom_Override_View_Cascade
Universe Designer Users		User Group	Full Control (Inherited)

Simple Scenario: Applications

- Controlled by role groups per application
  - No top-level security group available
  - Simple scenario: Everyone can view the applications



	Name	Full Name	Type	Access
	Administrators		User Group	Full Control
	Everyone		User Group	View
	SecureSimple_r_Analysts		User Group	Custom_Role_Analyst
	SecureSimple_r_Authors		User Group	Custom_Role_Author
	SecureSimple_r_Users		User Group	Custom_Role_User
	SecureSimple_r_Viewers		User Group	Custom_Role_Viewer

Simple Scenario: All Other Content

- This includes:
  - Events
  - Server Groups
- Security can usually be covered by using the universe folders and visibility overrides

Simple Scenario: Demonstration

Demo

What We’ll Cover …

- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

Advanced Scenario: Multiple Roles

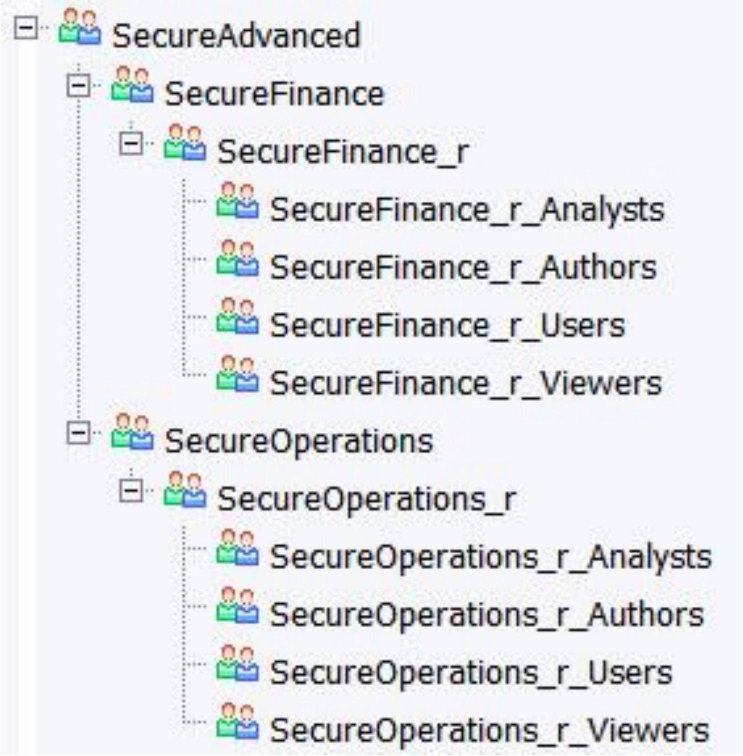
- Users want to have multiple roles based on the business area they are working
  - Analyst role for Finance
  - User role when working with Operations content
- A user may be assigned to many role and content groups

User

Analyst

Advanced Scenario: Access Levels

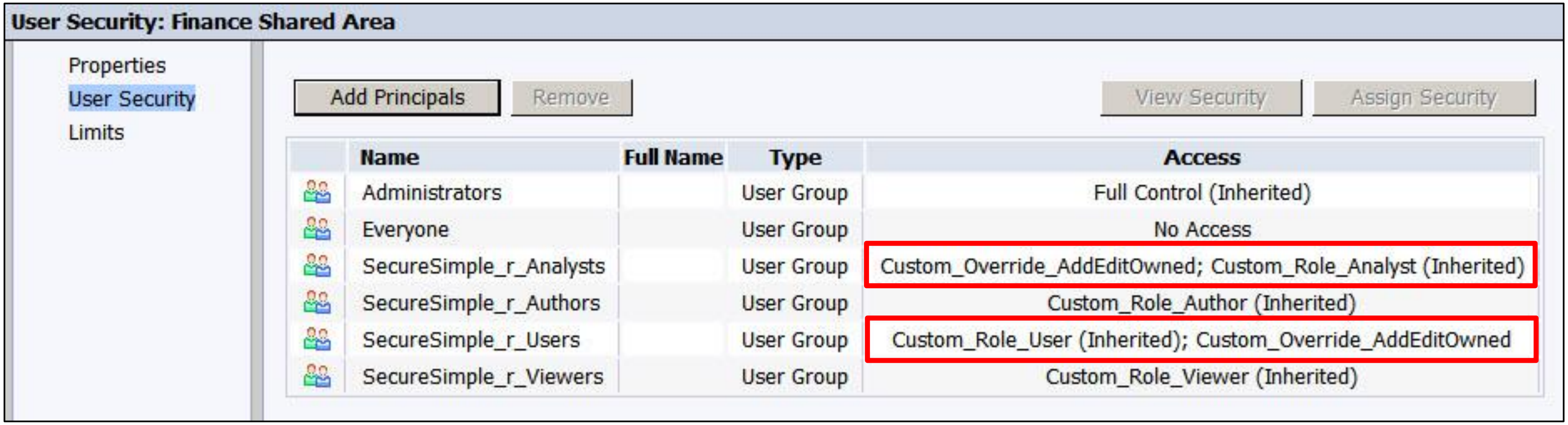
- Create role-based groups per business area



```
⊟ SecureAdvanced
  ⊟ SecureFinance
    ⊟ SecureFinance_r
        SecureFinance_r_Analysts
        SecureFinance_r_Authors
        SecureFinance_r_Users
        SecureFinance_r_Viewers
  ⊟ SecureOperations
    ⊟ SecureOperations_r
        SecureOperations_r_Analysts
        SecureOperations_r_Authors
        SecureOperations_r_Users
        SecureOperations_r_Viewers
```

Advanced Scenario: Sandboxes

- Sandboxes represent shared public folders that almost anyone can post content
- Can be set up many different ways
  - Overrides added for users and analysts below
  - Viewer not allowed to post, and authors can by default



User Security: Finance Shared Area

Properties
User Security
Limits

	Name	Full Name	Type	Access
	Administrators		User Group	Full Control (Inherited)
	Everyone		User Group	No Access
	SecureSimple_r_Analysts		User Group	Custom_Override_AddEditOwned; Custom_Role_Analyst (Inherited)
	SecureSimple_r_Authors		User Group	Custom_Role_Author (Inherited)
	SecureSimple_r_Users		User Group	Custom_Role_User (Inherited); Custom_Override_AddEditOwned
	SecureSimple_r_Viewers		User Group	Custom_Role_Viewer (Inherited)

Advanced Scenario: Demonstration

Demo

What We'll Cover …

- Security Overview
- Introducing Template-Based Security
- Customizing Access Levels
- Optimizing Groups
- Putting Theory Into Practice – Simple Scenario
- Putting Theory Into Practice – Advanced Scenario
- Wrap-up

Where to Find More Information

- Dwayne Hoffpauir, “XI 3.0 Security for Mere Mortals” (GBN 2008 BusinessObjects Conference, October 2008)
  - Paper describes how to use access levels as basic building blocks for a security model
- Jorn Van den Driessche, “BusinessObjects XI: Security made easy”
  - (http://www.element61.be/e/resourc-detail.asp?ResourceId=219)
- SAP BusinessObjects Enterprise Administrator's Guide (http://help.sap.com/boall_en/)
  - Follow BusinessObjects Enterprise ➞ XI 3.1 Service Pack 3
- Business Intelligence Platform Administrator’s Guide (http://help.sap.com/boall_en/)
  - Follow Business Intelligence Platform ➞ SAP BusinessObjects 4.0

7 Key Points to Take Home

- Understand how traditional BusinessObjects security works
- Simplify security rules through the use of template-based design techniques
- Avoid working with individual rights by creating your own custom access levels
- Use security group hierarchies to manage who has access to what
- Learn the difference between role and content-based security
- Model real-life scenarios from simple to advanced
- Make future security requests as easy as adding users to a group

Don't Forget

Your Turn!

Questions?

How to contact me:
Alan Mayer
alan.mayer@solidgrounded.com

Please remember to complete your session evaluation

Disclaimer

SAP, R/3, mySAP, mySAP.com, SAP NetWeaver®, Duet®, PartnerEdge, 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 in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP.