IBM Software Group

2006 B2B Customer Conference

B2B – Catch the Next Wave

Client Role Base Access Control

© IBM Corporation

Objectives

- Explain WDI Client security
- Learn how to enable security
- Discuss object permissions
- Talk about Roles, Access Groups, User IDs
- Create security objects
- Outline steps to implement WDI Client security

© IBM Corporation

WDI Client Security Overview

- Role Based Access Control
  - Intended as a method to grant one or more users certain access to specific object types
  - Never enabled on WDI Client supplied database
    - Though security objects can be maintained there
- Access Groups
  - Intended to limit which specific objects a user can see
- Each optionally enabled on an individual System

© IBM Corporation

WDI Client Security Overview (Continued)

- Three security related objects
  - User IDs
  - Roles
  - Access Groups
- Can be imported between Systems and out of the Configuration database
- May or may not be imported by Server depending on a System setting

© IBM Corporation

WDI Client Security Overview (Continued)

- List windows will not appear for objects the user is not authorized to view
- Users will not be able to open a functional area if they are not authorized to view any of the objects within the functional area
- Actions will be disabled when the user is not authorized to use them for the object
- The System must be opened before the WDI Client can accurately determine privileges

© IBM Corporation

Enabling Role Based Access Control

- Enable or disable on the System Editor or in the Configuration database options
- Also some options about whether certain PERFORM commands should be allowed from WDI Client
- An option to indicate whether the WDI Server can import security objects
- These additional options do not apply to the Configuration database
- Must be logged into the System to make changes
- Cannot enable on a WDI Client supplied database

© IBM Corporation

Enabling Access Groups

- Enable or disable on the System Editor
- Not available in the Configuration database
- Other related options:
  - Default Access Group
  - Prompt on import
  - Make an Access Group required or optional
- Must be logged into the System to make changes
- Can enable on a WDI Client supplied database, but not used to restrict access

© IBM Corporation

Object Permissions

- Permissions
  - None
  - Read, Update, Create
  - Delete, Submit
- Defaults to “read” for most objects
- Can be granted to a Role or User ID
- Nested Role grants are merged – highest access is used
- User ID grants override Role grants

© IBM Corporation

Roles

- Defines an area in which one or more users might be assigned. An example might be “Trading Partner Administrator” or “Mapper”
- Includes specific object permissions and other Roles
- Object permissions within nested Roles are merged – highest access granted is used
- Default Roles provided by WDI Client

© IBM Corporation

Access Groups

- Each object supporting Access Groups can be assigned to one Access Group
- User IDs can participate in multiple Access Groups
- Any object not assigned to an Access Group is automatically assigned to Access Group “Global”
- By default user IDs can access all groups
- User IDs that have no Access Groups assigned will not be restricted by an Access Group

© IBM Corporation

User IDs

- Defined for each user that will log onto an enabled System
- Can be assigned to zero or more Roles
- Contains specific object permissions
  - Those override Role permissions
- Can be assigned to zero or more Access Groups
  - Can me marked to participate in all Access Groups
- Default user $WDIUSER provided for users not defined to the System

© IBM Corporation

Defining Security Objects

- User IDs, Roles, and Access Groups are defined in the Security submenu
- Pertains to the System currently selected on the navigator bar or to the Configuration database if in that menu
- Works like any other editor in WDI Client

© IBM Corporation

An Administrator

- Identify an administrator (or two)
- Have the administrator maintain:
  - System options
  - Security objects
  - Audit trail
  - Shared Configuration database options
- Ensure someone has authority to update Systems and Configuration database options

© IBM Corporation

Implementing Security in WDI Client

- Create the user IDs that will be the administrators
  - Make sure the administrator has access to all security related objects, Systems and Configuration database options
- Define or update the Roles
- Define the Access Groups
- Define the user IDs
- Assign Access Groups to all existing objects
- Turn on security

© IBM Corporation

Implementing Security in WDI Client - Hints

- Import can be used to assign an Access Group to a large number of objects
- Access Group “defaults” can also help to assign Access Groups to a large number of objects
- To implement security for one group of users at a time:
  - Start by providing all users access to all objects
  - Then restrict selected groups of users when you are ready
- Users with no Access Group assigned to them are not restricted by Access Groups

© IBM Corporation

Summary

- You can now secure WDI Client related data according to business requirements (or not)
- Use Roles to restrict users performing similar tasks to the needed objects types
- Implement Access Groups to restrict users to the specific objects they should be working with
- Having an administrator is a good idea
- Plan implementation – all at once or phased

© IBM Corporation