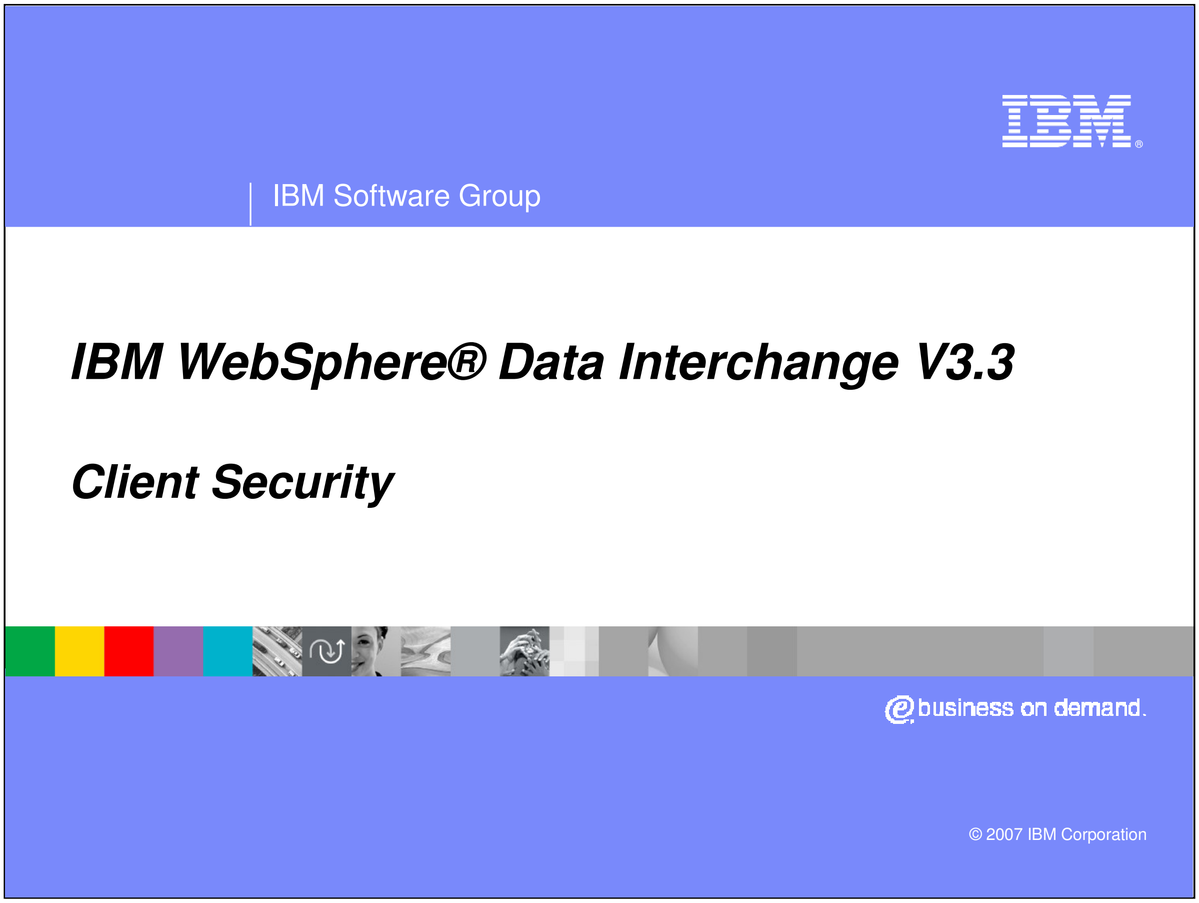


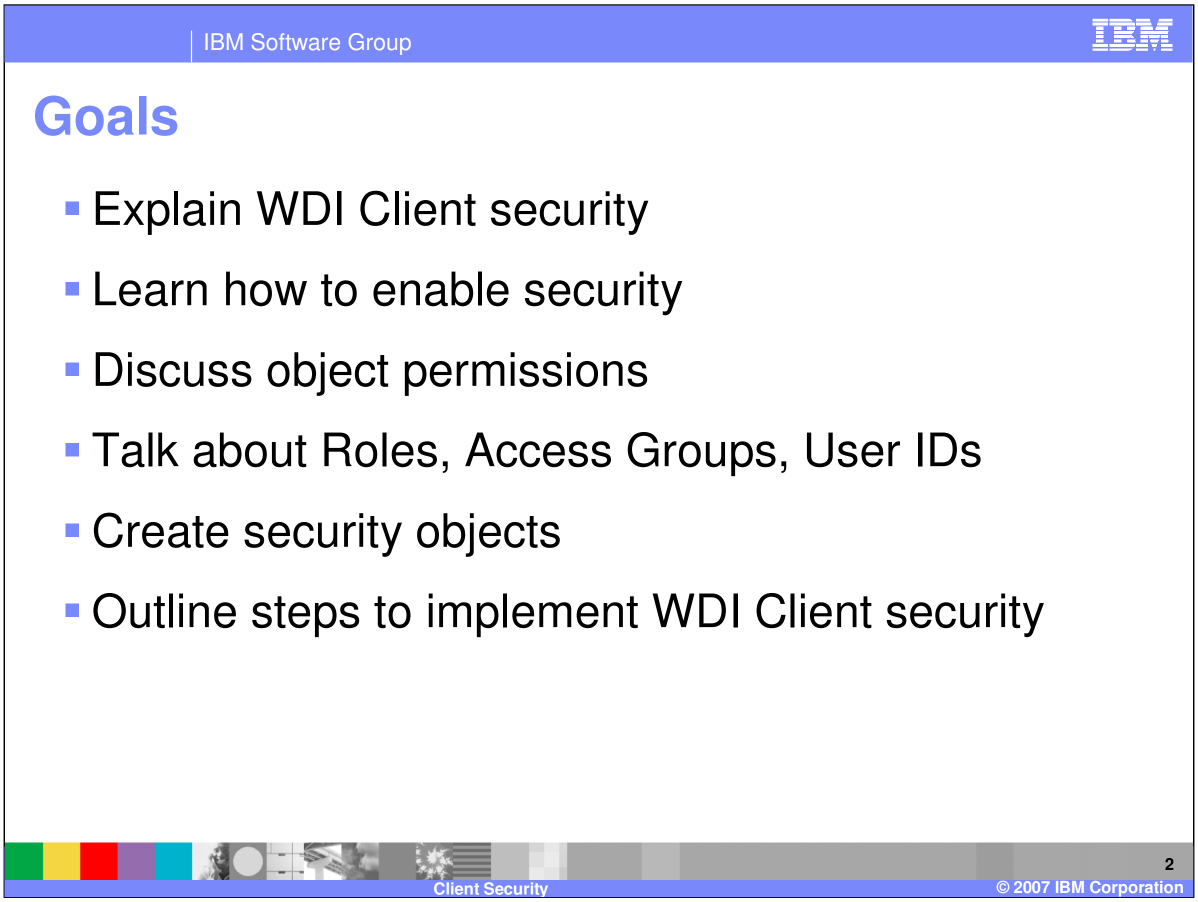
IBM Software Group

IBM WebSphere® Data Interchange V3.3

Client Security

business on demand.

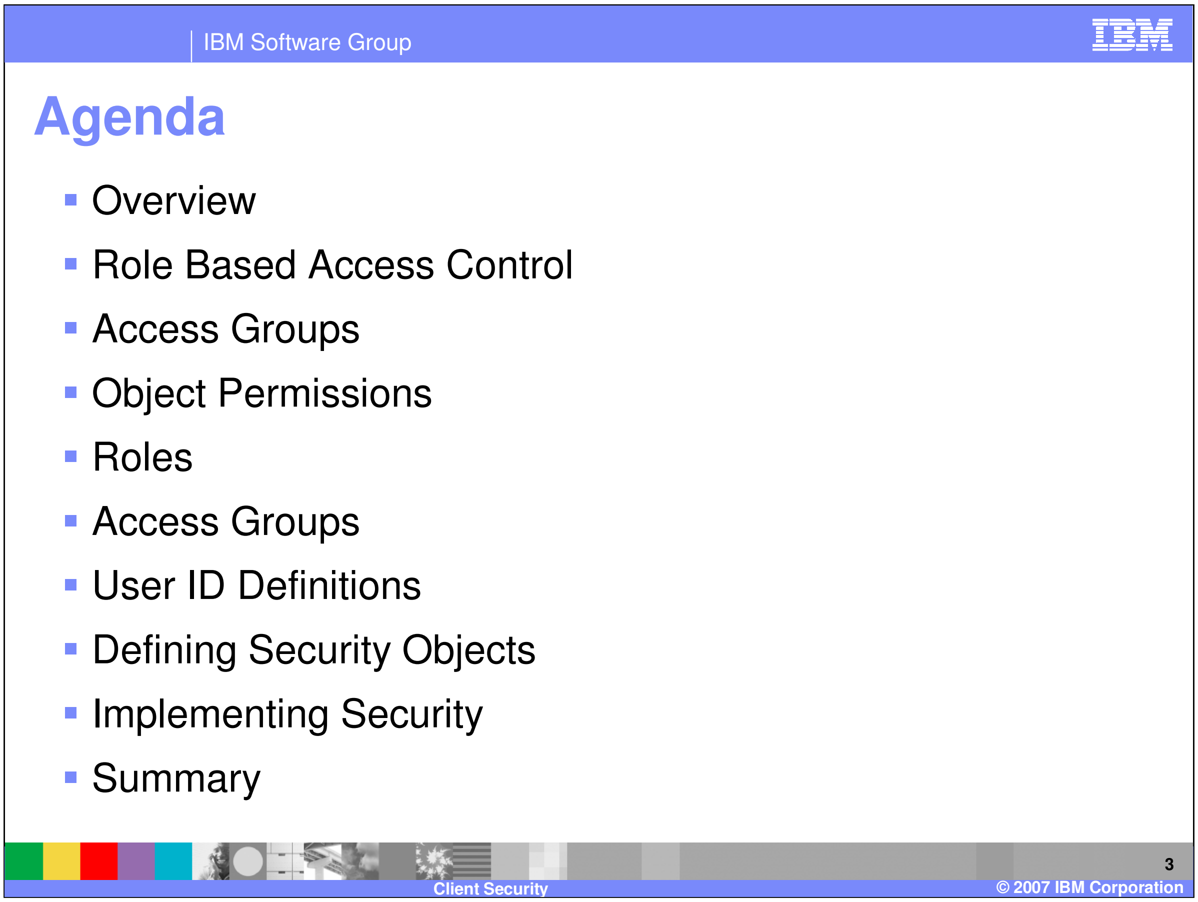
This presentation will provide an overview explaining the two components of WebSphere Data Interchange (WDI) Client security.



Goals

- 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

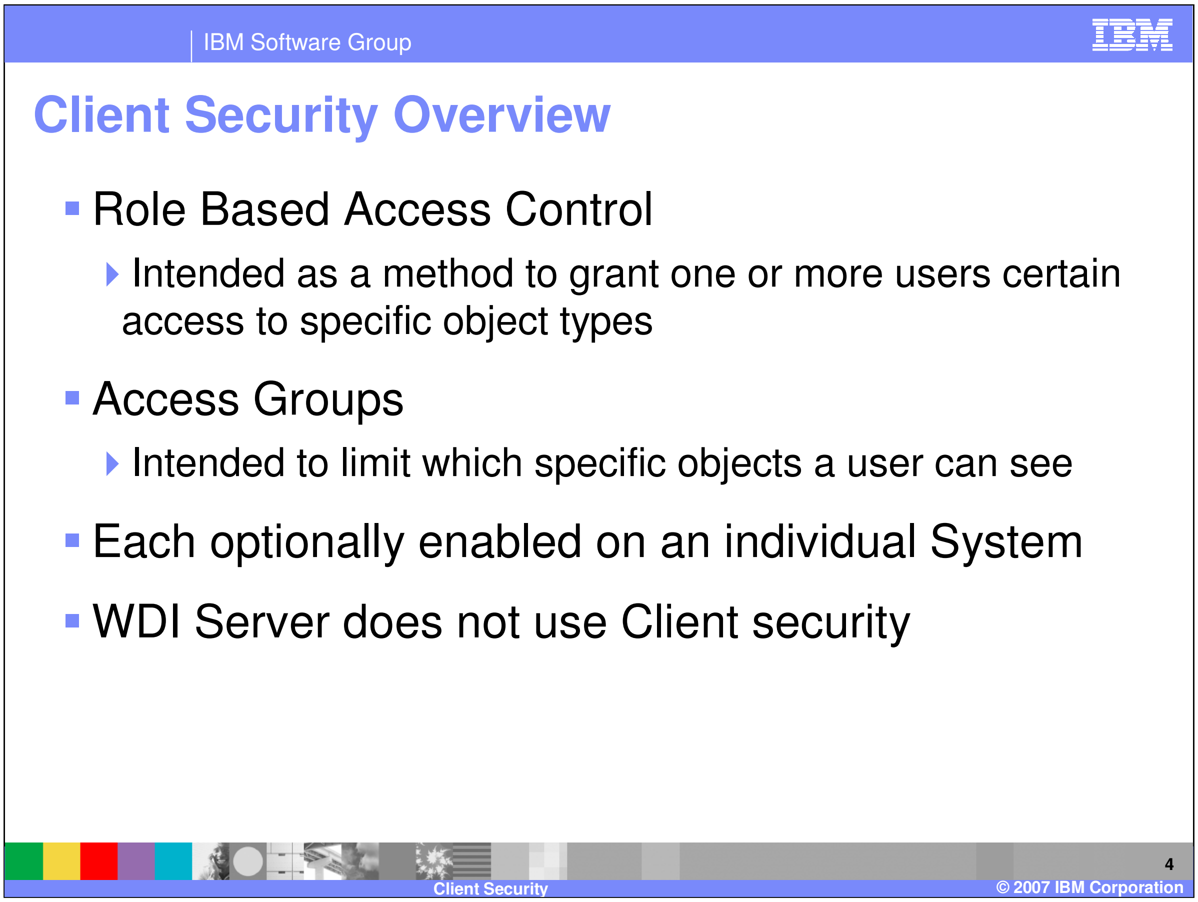
You will learn how to enable security on WDI Client and understand some of the options associated with WDI Client security. Object permissions will be discussed and an understanding of their affects will be gained. Knowledge of the security related object types will be obtained and you will learn how to create the security related object types. Finally, implementation of WDI Client security will be discussed.



Agenda

- Overview
- Role Based Access Control
- Access Groups
- Object Permissions
- Roles
- Access Groups
- User ID Definitions
- Defining Security Objects
- Implementing Security
- Summary

The presentation will give a Client security overview and review role based access control using access groups, object permissions, user definitions, and security objectes.



IBM Software Group

IBM

Client Security Overview

- Role Based Access Control
  - Intended as a method to grant one or more users certain access to specific object types
- Access Groups
  - Intended to limit which specific objects a user can see
- Each optionally enabled on an individual System
- WDI Server does not use Client security

4

Client Security

© 2007 IBM Corporation

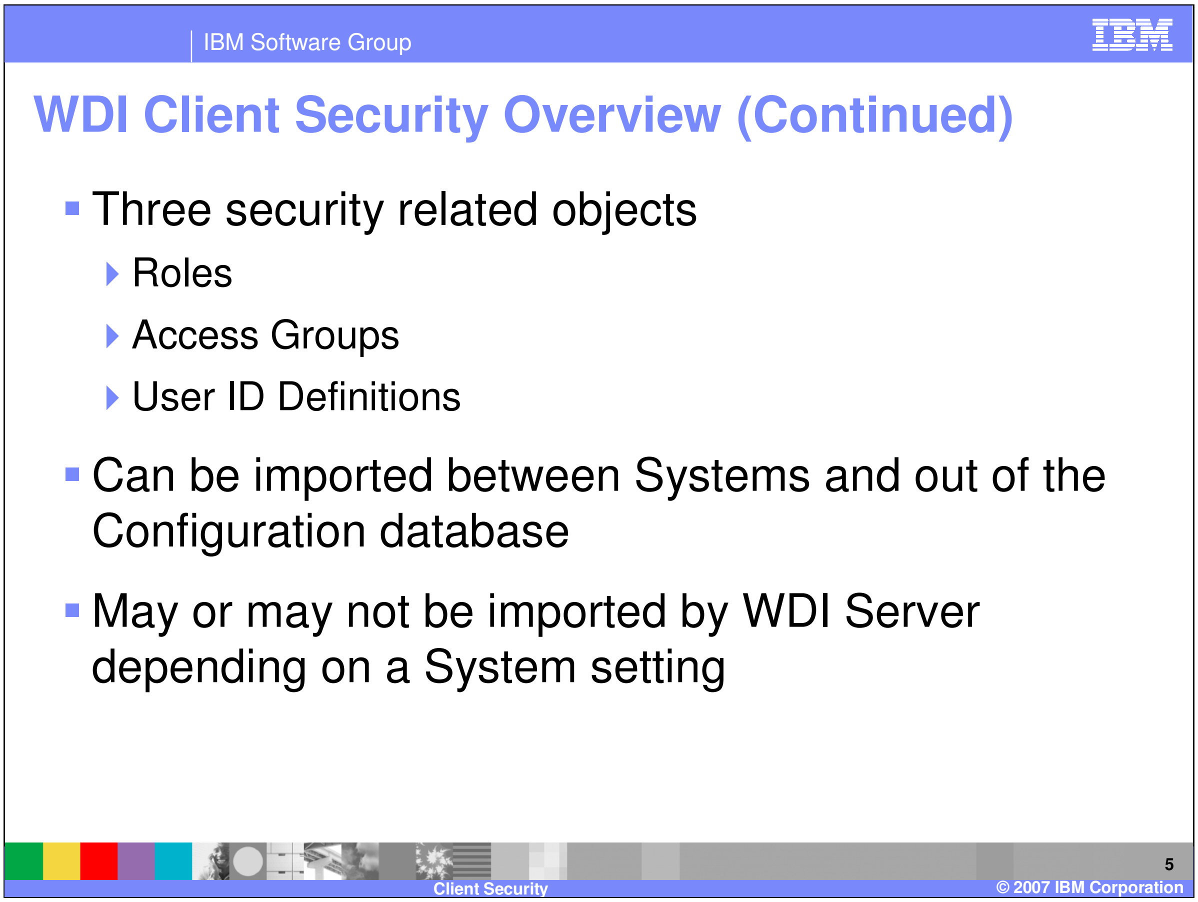
Security on WDI Client consists of two components; “role based access control” and “Access Groups”.

•Role based access control is intended as a method to limit which object types users can access and limit the functions that can be performed on each object type. Users can be assigned to “roles” and will inherit the object permissions provided by the roles. Object permissions can be specified directly for the user.

•Access Groups is intended to limit which specific objects a user can see. For instance, you may want a user to only access objects associated with Asia business. A user can part a part of any number of Access Groups. Objects can be associated with only one Access Group.

•Each component of security is enabled individually on a System. You can use neither component, one component, or both components. Security is System specific and thus can be implemented differently on each System.

•The WDI Server does not participate in WDI Client security. You must use the traditional security measures on the system to secure WDI Server.



IBM Software Group

WDI Client Security Overview (Continued)

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

5

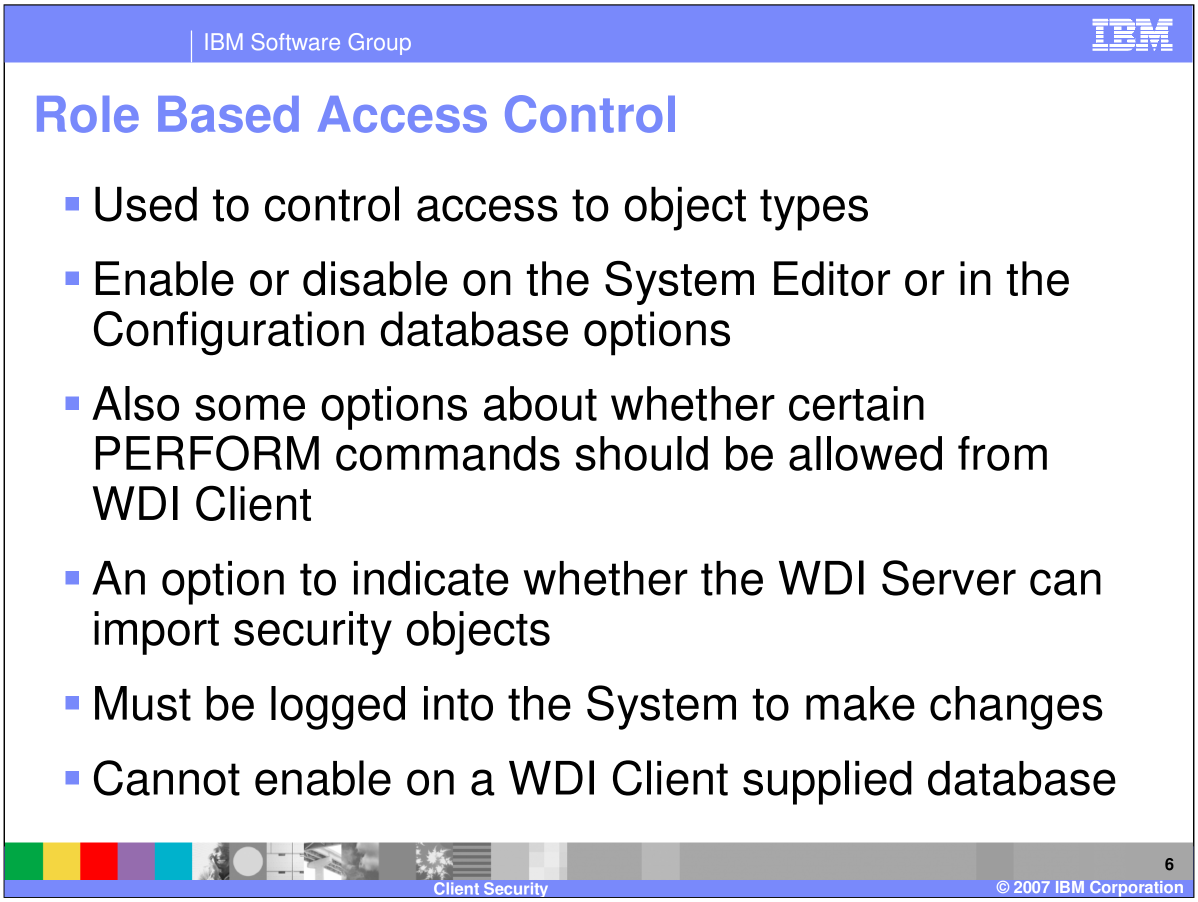
Client Security

© 2007 IBM Corporation

•There are three new object types that are used to implement security. These are Roles, Access Groups, and User ID Definitions.

•Each of the security objects types can exported and imported between Systems. The object types can be exported out of the Configuration database, but not into it.

•The WDI Server may or may not be able to import security related objects depending on a System setting.



IBM Software Group

Role Based Access Control

- Used to control access to object types
- 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
- Must be logged into the System to make changes
- Cannot enable on a WDI Client supplied database

6

Client Security

© 2007 IBM Corporation

•Role based access control is used to control access to object types. You can use role based access control to limit what object types a user can access and also to limit what functions a user can perform against an object type.

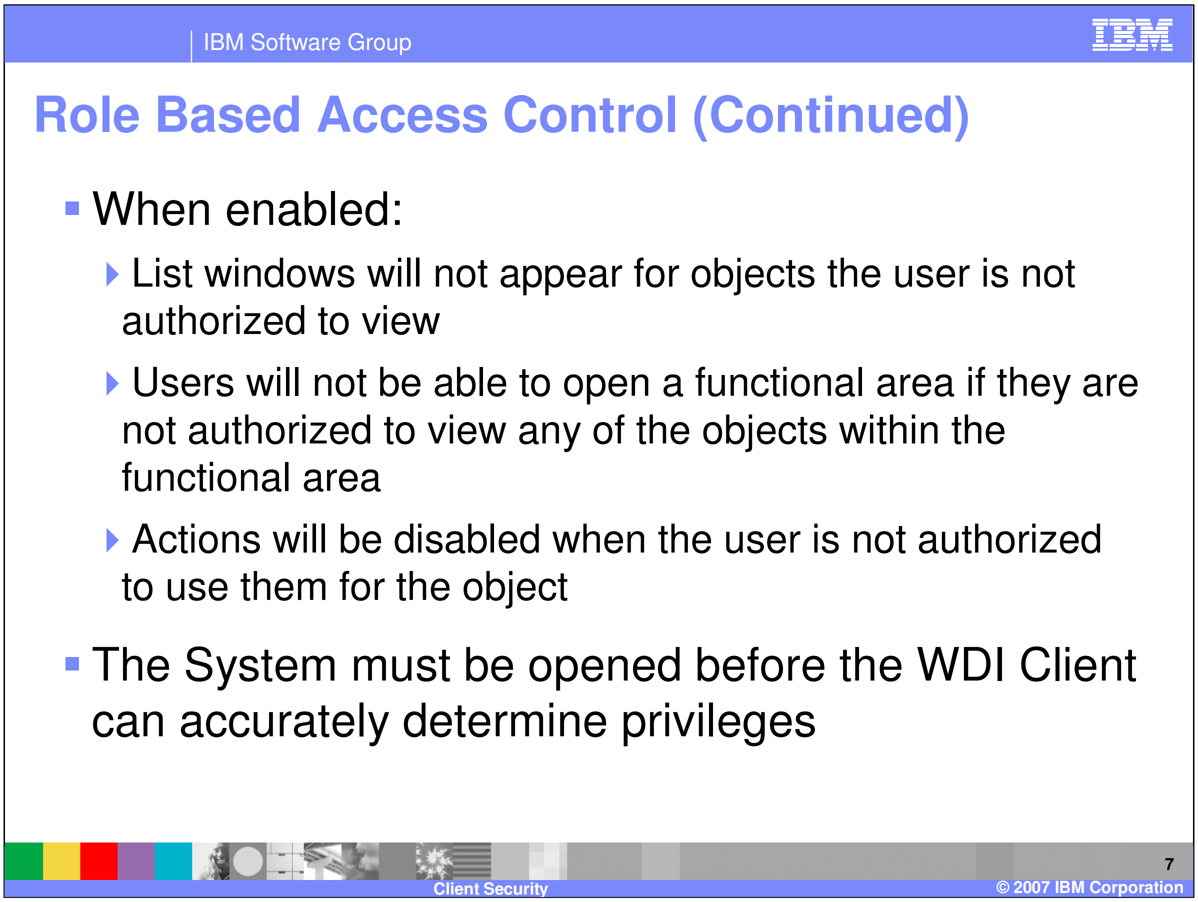
•Enable or disable role based access control on a System by editing the System object in the System Editor and then selecting the corresponding option. Configuration Database Options are used to enable or disable role based access control on the Configuration database. You must have authority to update System objects on the Configuration database and on the target System before you can enable role based access control. This ensures that you will be able to turn off role based access control if needed.

•The System Editor also contains options you can use to indicate whether certain PERFORM commands will be allowed to be submitted from WDI Client. Since WDI Server is not participating in WDI Client security, you may want to restrict submission of the PERFORM IMPORT, PERFORM EXPORT, and PERFORM DELETE commands from WDI Client. These commands can be used to change objects, delete objects, or view object information that the user would otherwise not be authorized to do. These options do not apply to the Configuration database since the WDI Server does not access the Configuration database.

•There is an option available on the System Editor that allows you to indicate whether WDI Server can export and import the three security related object types. You may want to prevent the WDI Server from importing these object types because importing them is a method to change them and WDI Server is not participating in WDI Client security to determine if a user is authorized to change them.

•You must be logged onto the System to make changes to security options in the System Editor.

•Role based access control cannot be enabled on the default WDI Client supplied System since it is intended as a single user database. Security objects can be maintained on the default System and then exported to other Systems.



IBM Software Group

Role Based Access Control (Continued)

- When enabled:
  - 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

Client Security

7

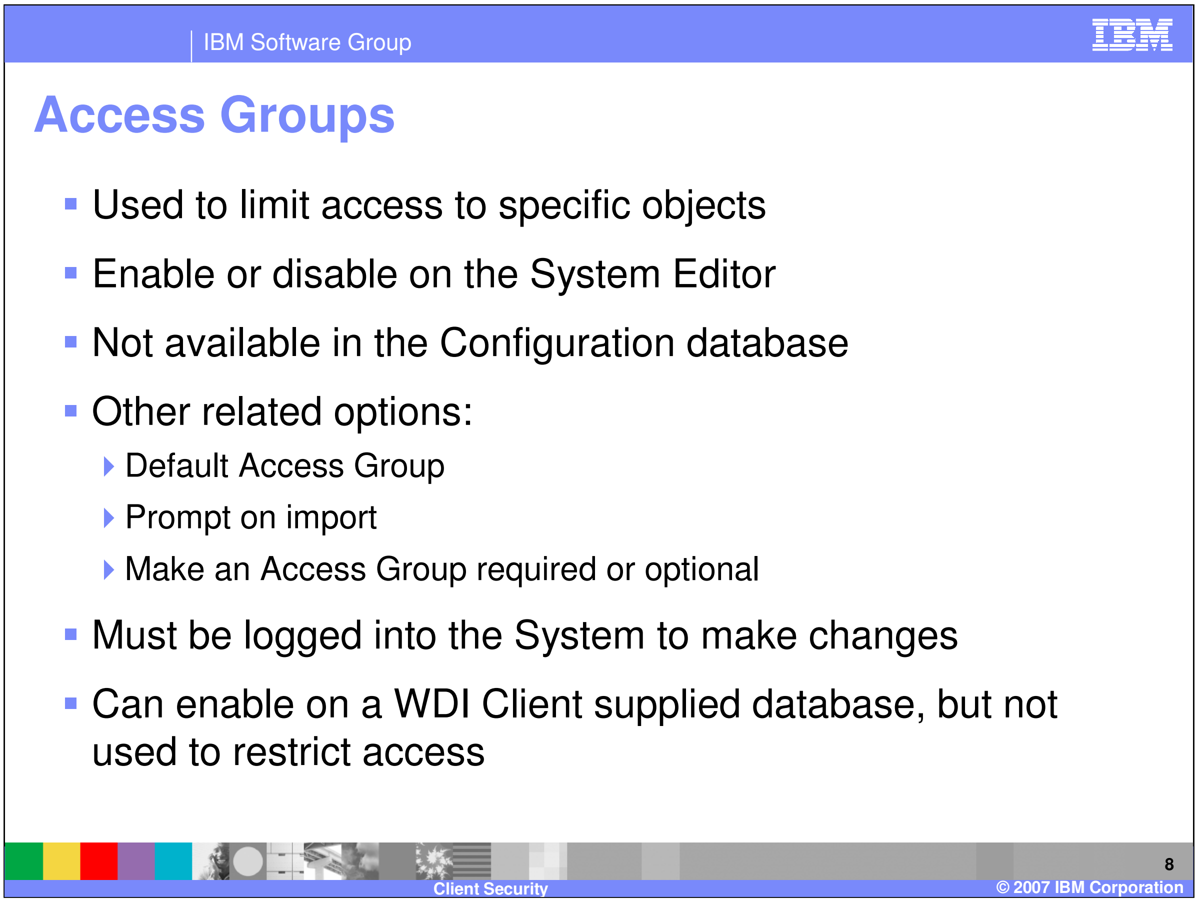
When role based access control is enabled:

•List windows will not be displayed when a user is not authorized to access the object type corresponding to the list window.

•Functional Areas cannot be opened by a user if the user is not authorized to access any of the object types in the functional area.

•Actions will be disabled or not present when the user is not authorized to use the action on an object type.

A System must be opened before WDI Client can accurately determine privileges for a user. Until the System is opened, WDI Client will assume the privileges the user had the last time they were logged onto the System. Adjustments will be made to privileges when the user logs onto the database.



IBM Software Group

Access Groups

- Used to limit access to specific objects
- 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

8

Client Security

© 2007 IBM Corporation

•Access Groups are used to limit access to specific objects. For instance, you may want a user to only see objects associated with Asia business. Access groups are not used to limit the functions that can be performed on an object – use role based access control for that.

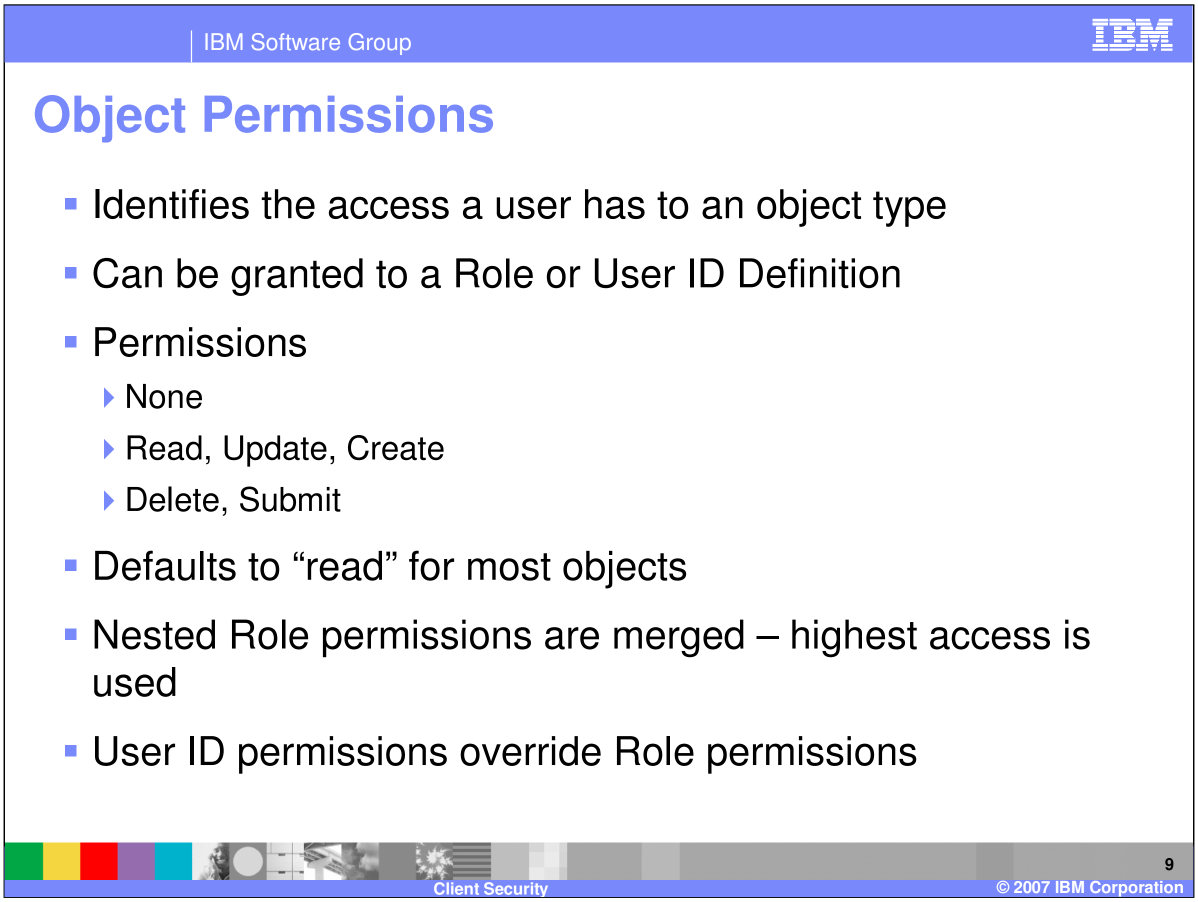
•Enable or disable Access Groups on a System by editing the System object in the System Editor and then selecting the corresponding option.

•Access Groups are not supported on the Configuration database.

•The System Editor also provides several options related to Access Groups. You can identify a default Access Group. New objects will be assigned to the default Access Group. The default Access Group applies to all users on the System. There is an option to allow the user to override the default Access Group by providing their own default Access Group. An option is provided that indicates whether a prompt for an Access Group should be issued at the beginning of an import. When set, the import process will ask how to handle the Access Group during import processing. This is a nifty feature that can aid in implementing Access Groups on your System. Finally, you can indicate whether the Access Group is optional or required. These options can be used to ensure an Access Group is assigned to objects.

•You must be logged onto the System to make changes to security options in the System Editor.

•Access Groups can be enabled on the default WDI Client supplied System, however they are not used to restrict access to object that System. This allows a user to maintain Access Groups on the default System without inadvertently preventing access to objects on the single user database.



Object Permissions

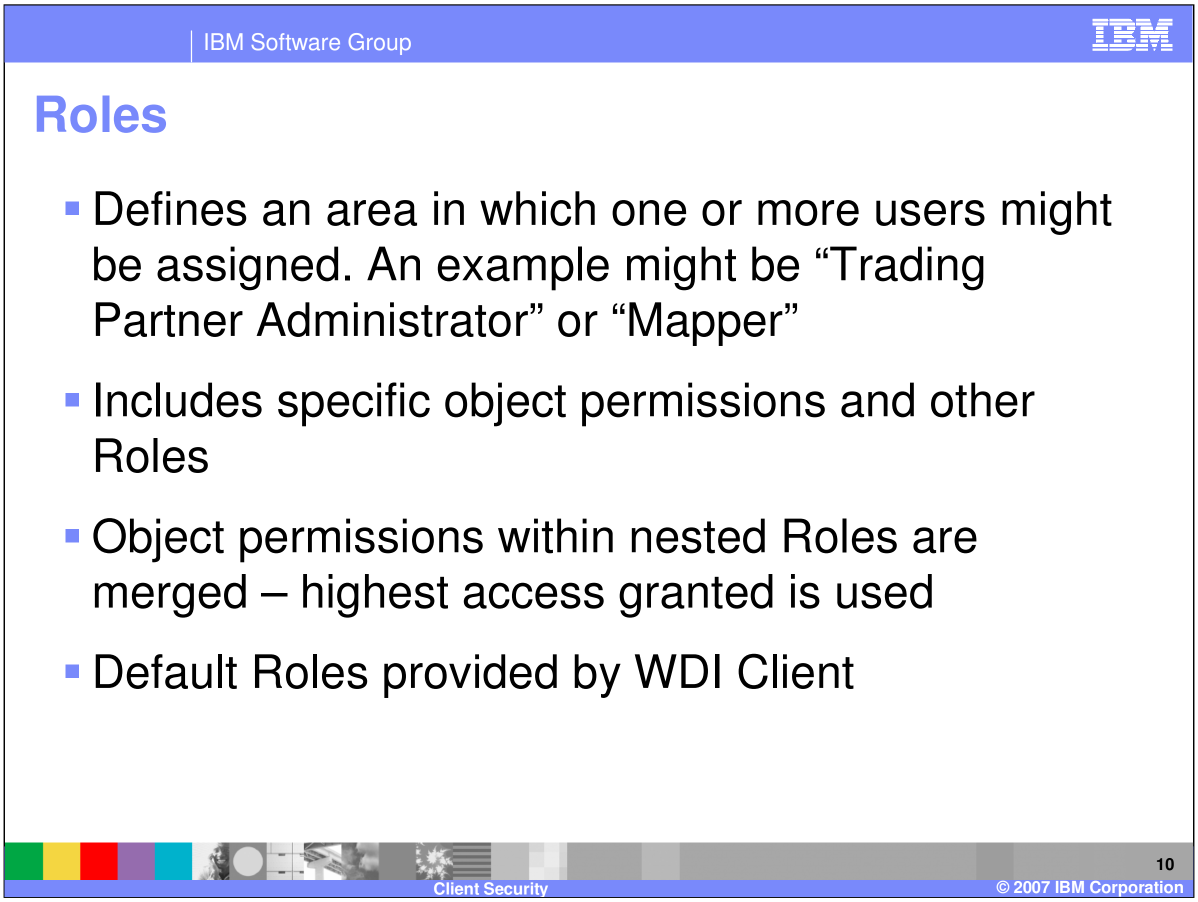
- Identifies the access a user has to an object type
- Can be granted to a Role or User ID Definition
- Permissions
  - None
  - Read, Update, Create
  - Delete, Submit
- Defaults to “read” for most objects
- Nested Role permissions are merged – highest access is used
- User ID permissions override Role permissions

•Object permissions are used to indicate the access a user has to a specific object type

•Permissions are used in Role objects and in User ID Definition objects.

•The permissions are “none”, “read”, “update”, “create”, “delete”, and “submit”. Not all permissions apply to all object types. Only a few object types use the “submit” permission. Some objects cannot be deleted. Other objects cannot be updated. Which permissions are valid depend on the object type. You will only be allowed to select valid permissions for any given object type.

> •The “none” permission is used to indicate that the user cannot access the object type. No other permission will be allowed when “none” is specified.
>
> •Use the “read” permission to indicate a user can view objects within the object type. The user will not be allowed to make changes to the objects and they will not be allowed to create new objects within the object type. The “read” permission will allow a user to list, view, export, and produce a report on an object type.
>
> •“Update” permission is used to provide “read” access and to further allow the user to perform update actions against the object type. In addition to functions that can be performed with the ‘read’ permission, the user will be able to perform update actions such as edit, rename, and activate.
>
> •The “create” permission is used to provide a user with “update” authority plus give them the ability to create objects within the object type. In addition to functions provided by the “update” permission, “create” allows a user create, import, and copy objects.
>
> •Deleting objects require that you have the “delete” permission to that object type. You must have “read”, “update”, or “create” permission to have the “delete” permission.
>
> •The “submit” permission applies to object types that can be submitted to the WDI Server. You must have the “submit” permission to an object type before you can submit the object to the WDI Server for processing. You must have “read”, “update”, or “create” permission to have the “submit” permission.
>
> •Most object types default to the “read” permission.
>
> •When a user is assigned more than one Role, or a Role is imbedded within another Role, the permissions from the Roles are merged; highest access privilege for each object type is used.
>
> •Permissions specifically assigned to a User ID Definition override the permissions specified in Roles assigned to the user.



IBM Software Group

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

10

Client Security

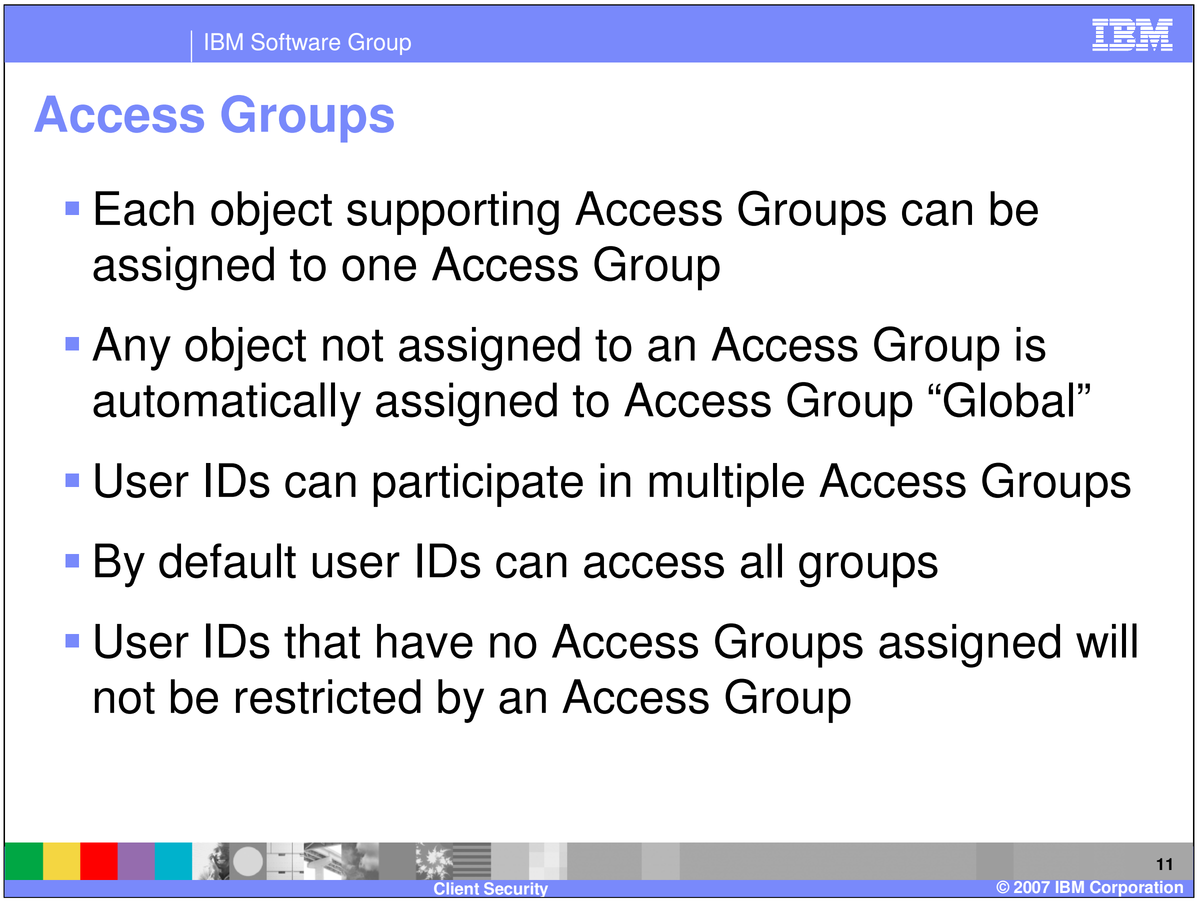
© 2007 IBM Corporation

•Role objects typically define an area of job responsibilities, such as a “trading partner administrator” or a “mapper”. A mapper’s responsibility might be to create, maintain, and test maps. Trading partner related objects, such as Trading Partner profiles, Contact profiles, and envelope profiles, might be maintained by the trading partner administrators.

•Specific object permissions are assigned to roles. Roles can include other Roles. Not all object types must have a permissions assigned. The default permission for an object type will be assumed when a specific permission is not assigned to an object type. The default permission for most object types is “read”.

•Object permissions for a Role are merged with the object permissions of imbedded Roles; highest access privilege for each object type is used.

•WDI Client provides several default Roles. Feel free to change or delete these.



IBM Software Group

Access Groups

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

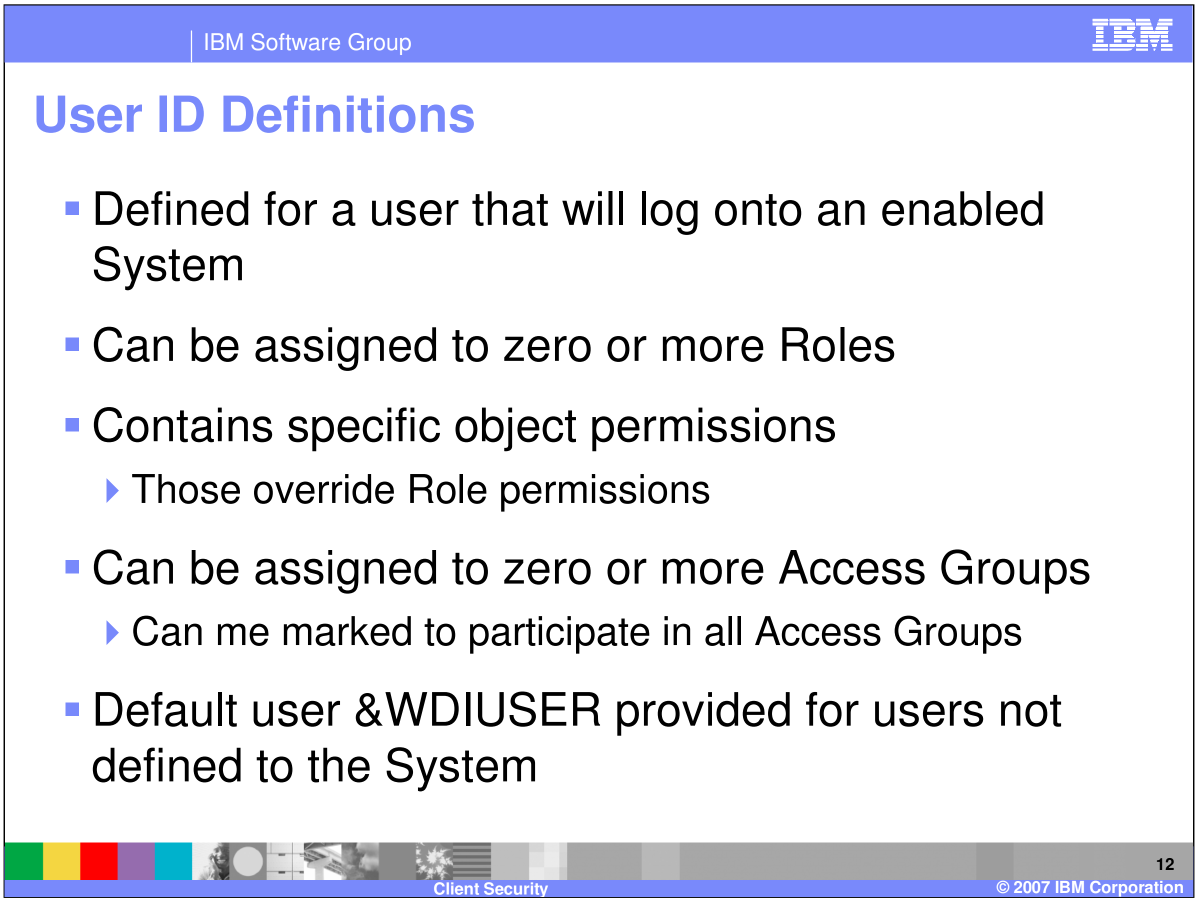
11

Client Security

© 2007 IBM Corporation

Each object type supporting Access Groups can be assigned to only one Access Group. Any object not assigned to an Access Group is automatically assigned to Access Group “Global”. When objects are created, they will be assigned to the default Access Group if one is specified and the user is participating in the default Access Group. If a default Access Group is not specified or the user is not participating in the default Access Group, then “Global” is assigned unless the Access Groups are required. If Access Groups are required, then the user must specify an Access Group they participate in before saving a new object or saving an existing object that does not have an Access Group specified.

User ID definitions can be assigned to many Access Groups. By default, User ID Definitions participate in all Access Groups. A User ID Definition that is not assigned to any Access Group will treated as if they are assigned to all Access Groups.



IBM Software Group

User ID Definitions

- Defined for a 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

12

Client Security

© 2007 IBM Corporation

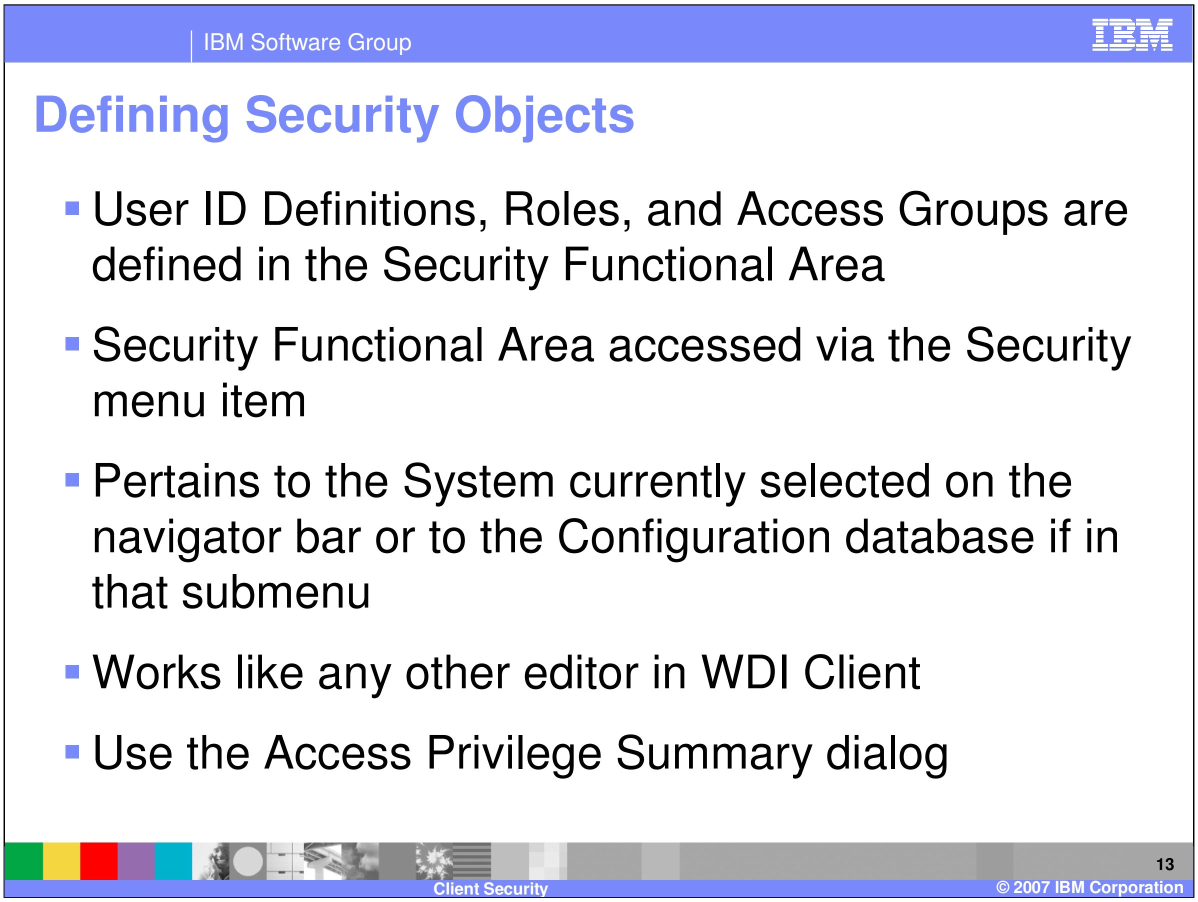
•A User ID Definition equates to a user on a System. The name of the User ID Definition must be the same as user ID used to log onto the database associated with a System. If a user uses a different user ID to log onto different databases, then the user will need a User ID Definition to correspond to each database user ID.

•Any number of Roles can be assigned to a User ID Definition. Object permissions within the assigned Roles are merged; highest access privilege for each object type is used.

•Specific object permissions can be assigned to a User ID Definition. An object permission assigned in a User ID Definition overrides object permissions specified in Roles.

•A User ID Definition can participate in any number of Access Groups. A User ID Definition can be marked as participating in all Access Groups.

•WDI Client provides a default User ID Definition called &WDIUSER. If a user ID used to log on to a System is not defined as a User ID Definition on that System, then the user will get the object permissions assigned to the &WDIUSER User ID Definition. You can modify the &WDIUSER User ID Definition as you like and you can delete it. When the &WDIUSER User ID Definition does not exist, unknown users will not be able to access objects on the System.



IBM Software Group

Defining Security Objects

- User ID Definitions, Roles, and Access Groups are defined in the Security Functional Area
- Security Functional Area accessed via the Security menu item
- Pertains to the System currently selected on the navigator bar or to the Configuration database if in that submenu
- Works like any other editor in WDI Client
- Use the Access Privilege Summary dialog

13

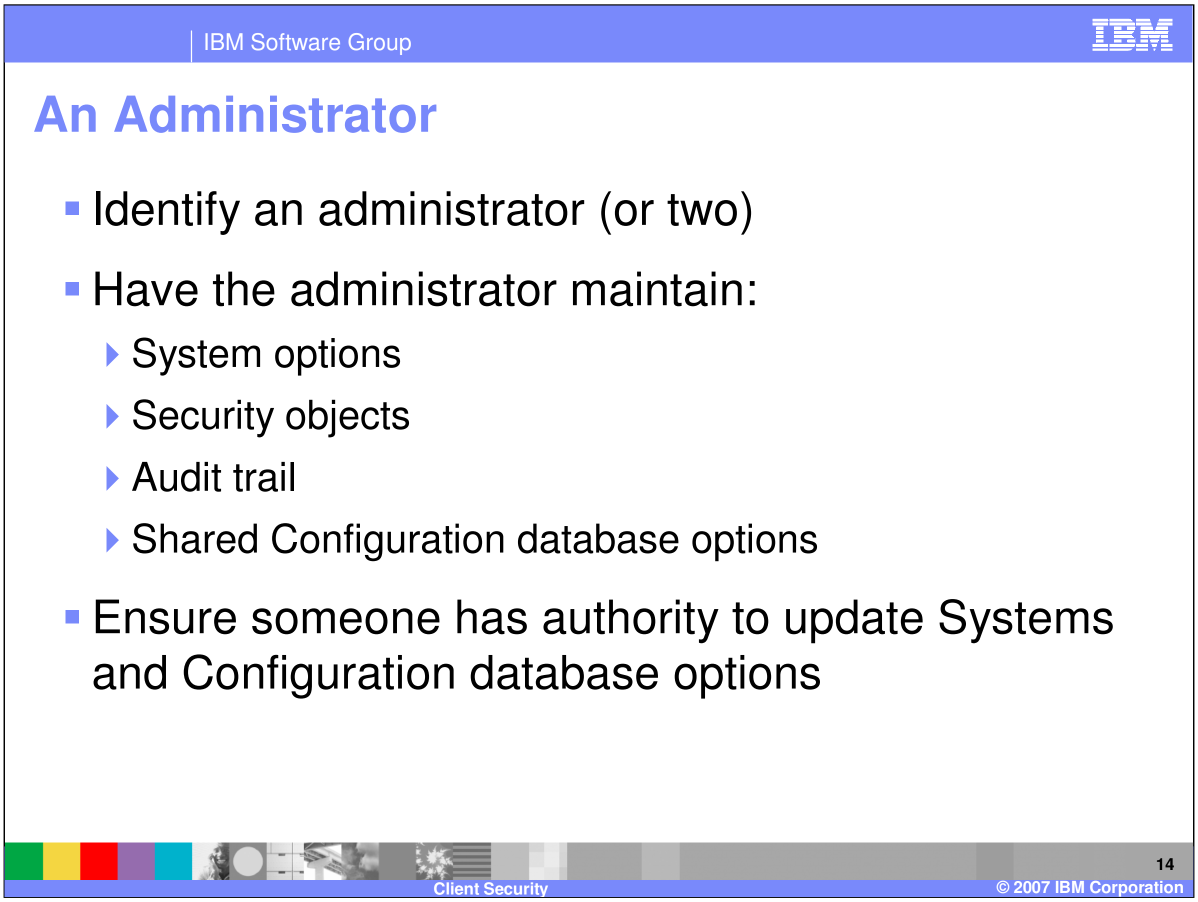
Client Security

© 2007 IBM Corporation

The three security object types are located in the Security Functional Area. The Security Functional Area for a System is accessed by selecting “Security” from the Administration submenu. The Administration submenu is found within the View menu. This will open the Security Functional Area for the System selected in the navigator bar. The Security Functional Area for a System can also be opened by selecting Open Functional Area from the File menu. The Security Functional Area for the Configuration database is accessed by selecting “Security” from the Configuration Database submenu. The Configuration database submenu is found within the Administration submenu.

Creating new objects works like most other object types in WDI Client. Select the list window for the object type you wish to create in the Security Functional Area, then press the “new” button on the toolbar or select “New” from the File menu. Editing an object in the Security Functional Area is also done like most other objects in WDI Client. Select an object on a list window, then press the “open” button on the toolbar or select “Open” from the File menu.

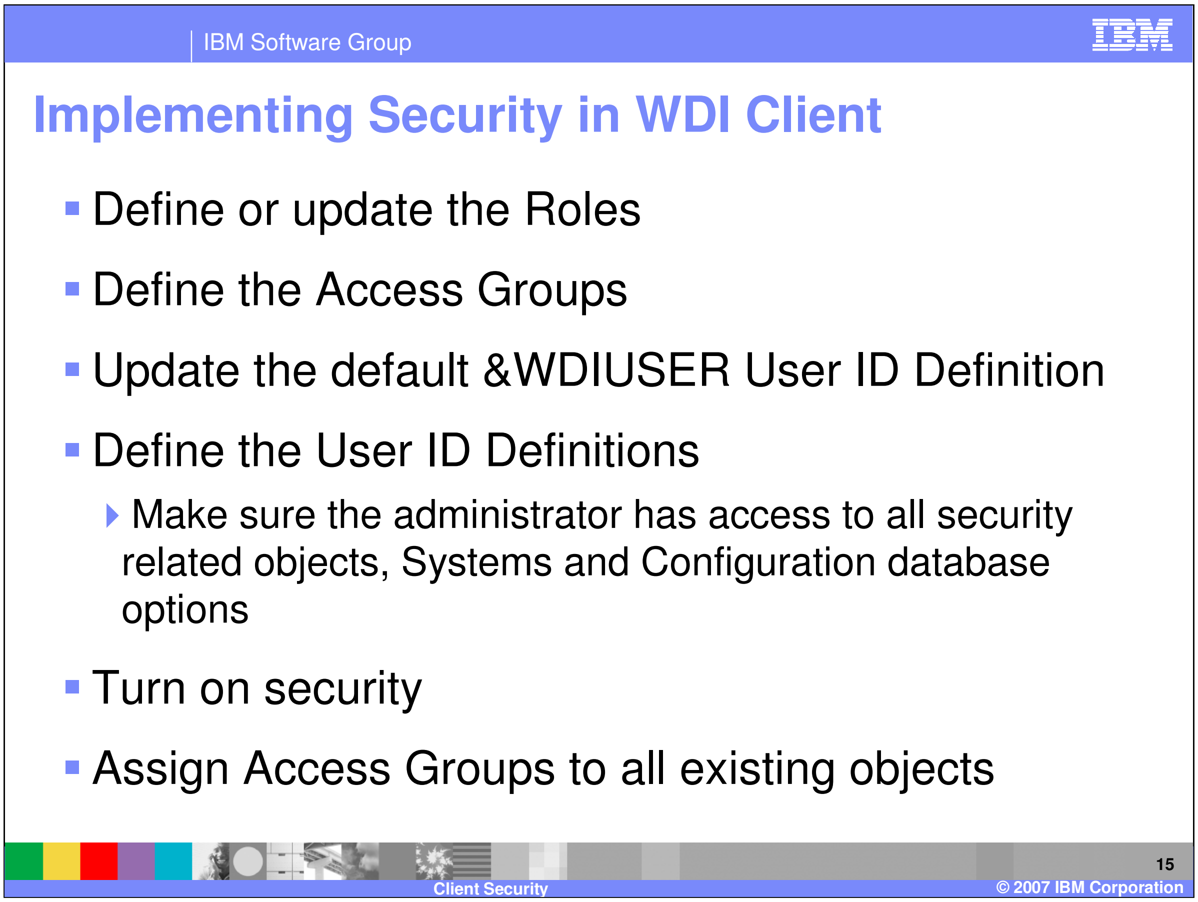
While creating or editing a Role or User ID Definition object, display the Access Privilege Summary dialog to see the access privileges that will be in place for the Role or User ID Definition. It is a good way to see the result of your changes before you save the Role or User ID Definition.



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

You should define some security administrators. Administrators should maintain System options, security objects, the Audit Trail, and Configuration database options. Ensure that someone always has authority to update Systems on the Configuration database and on each System. This is necessary so you can change System options, such as enabling or disabling role based access control and Access Groups. You should also ensure that someone can update User ID Definitions. WDI Client will not make these checks as you change security options and security objects. WDI Client will ensure that you cannot enable role based access control for a System unless you are authorized to update Systems on the Configuration database and on the target System. This ensures you will be able to disable role based access control if needed.



IBM Software Group

Implementing Security in WDI Client

- Define or update the Roles
- Define the Access Groups
- Update the default &WDIUSER User ID Definition
- Define the User ID Definitions
  - Make sure the administrator has access to all security related objects, Systems and Configuration database options
- Turn on security
- Assign Access Groups to all existing objects

15

Client Security

© 2007 IBM Corporation

To implement security within WDI Client on a System or on the Configuration database:

•Update or create the Role objects you will use.

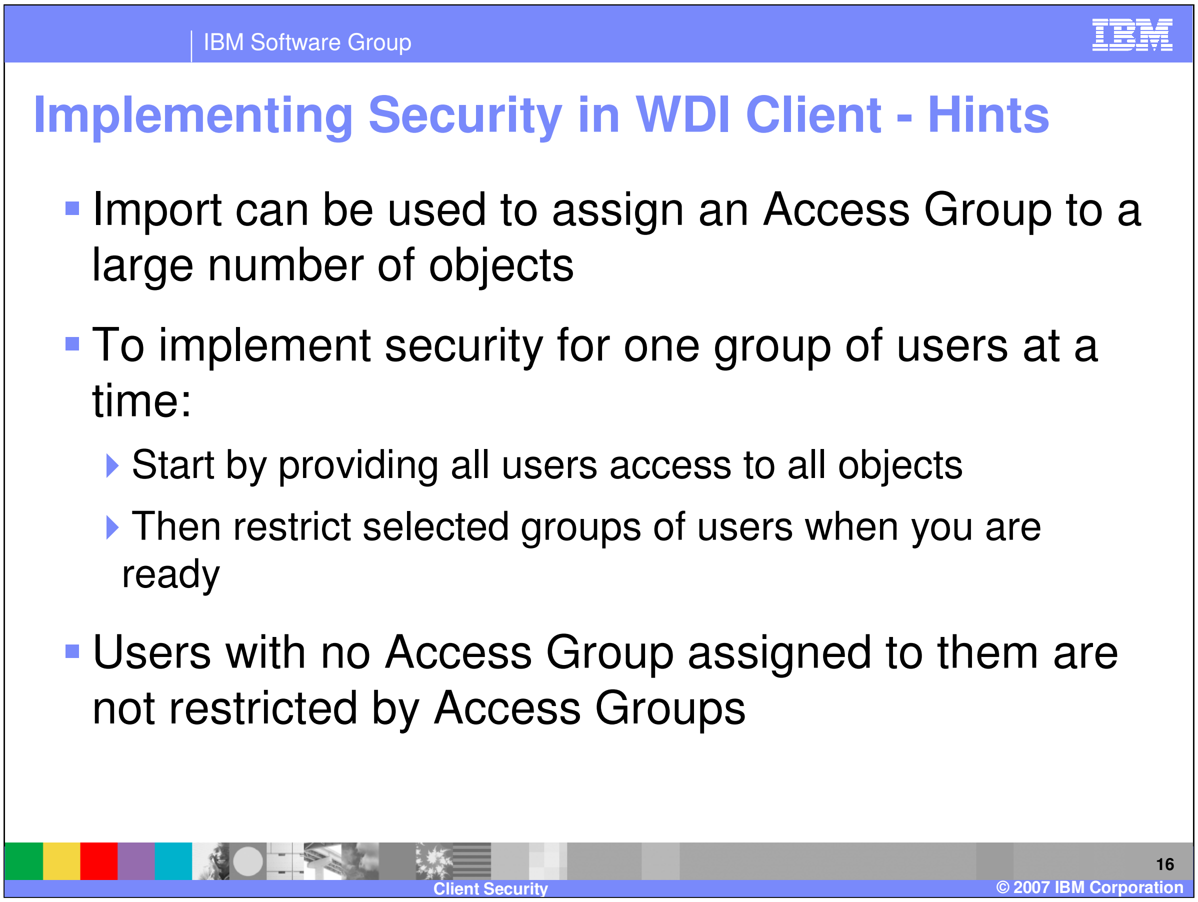
•If implementing Access Groups on a System, define your Access Groups (does not apply to the Configuration database)

•Update the default &WDIUSER User ID Definition as needed. You can delete this User ID Definition now or in the future when you no longer want to provide default access for unknown user IDs.

•Create a User ID Definition for each user that you want to provide access privileges for. Ensure some has authority to update Systems and Configuration database options.

•Enable role based access control and Access Groups, if desired, using the System Editor or Configuration Database Options.

•Assign an Access group to all existing object if you are enabling Access Groups. You may want to update User ID Definitions after this so they participate only in certain Access Groups.



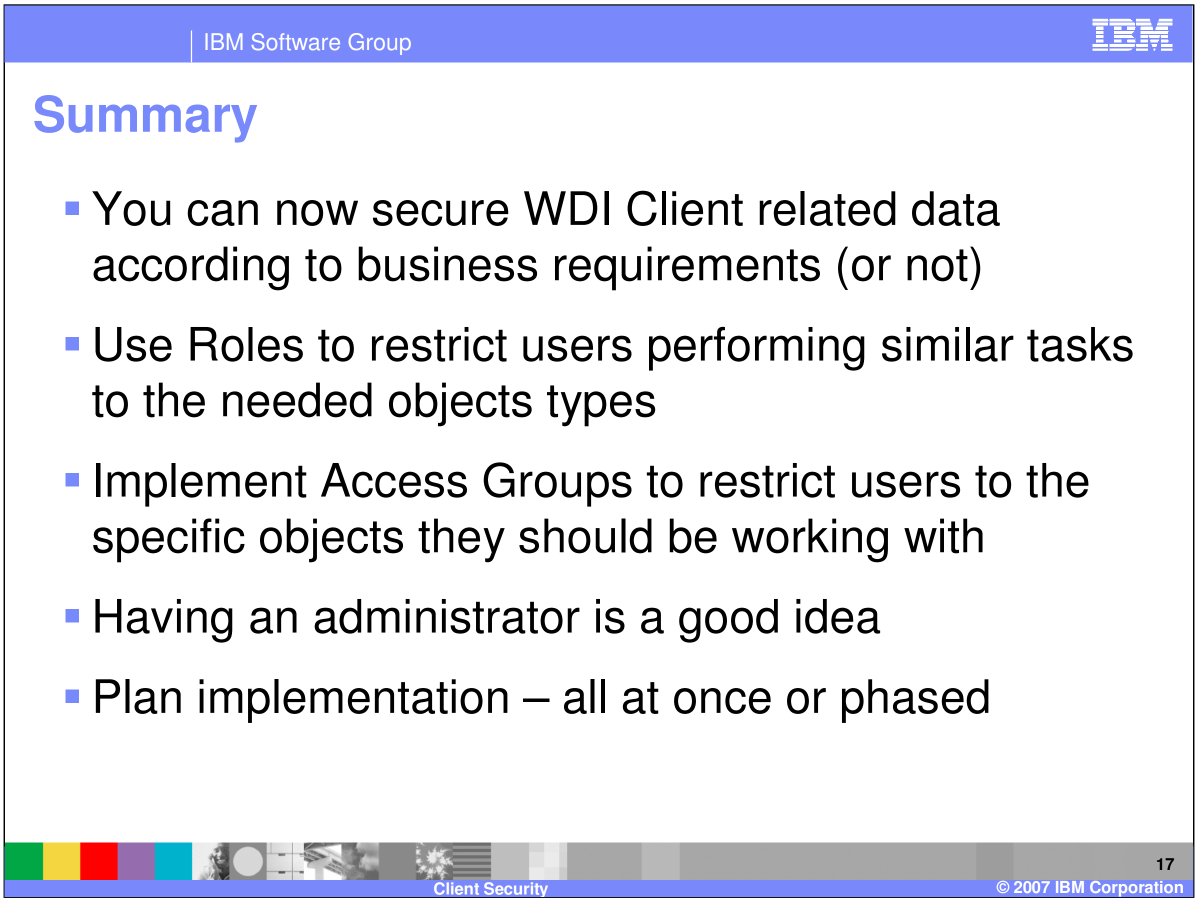
Implementing Security in WDI Client - Hints

- Import can be used to assign an Access Group 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

•Import can be used to assign an Access Group to a large number of objects. Ensure the System option to cause import to display a prompt for the Access Group is set. Export all objects to be assigned to the same Access Group to a single file. Import the contents of the file choosing the desired Access Group when prompted. Repeat the export and import for each Access Group.

•Security can be implemented one group at a time. Update the Default &WDIUSER User ID Definition so it can access all objects. This will make enabled security transparent for users that do not have a corresponding User ID Definition. Update or create your Roles as needed. Assign Access Groups to all of your objects if Access Groups will be enabled. Create the User ID Definition for the first group of users. This will cause security to be imposed on those users. The first group of users should be the administrators. At this time access privileges for security objects, Systems, and the Configuration database should be reduced or removed on the &WDIUSER User ID Definition. Once you are ready, create the second group of User ID Definitions. Repeat for each group when ready. Once security is implemented for all groups, reduce or remove the privileges on the &WDIUSER User ID Definition so unknown users do not get unintentional access to objects.

•Remember, User ID Definition assigned to no Access Groups will have access to all Access Groups. This is the same as indicating the User ID Definition has access to all Access Groups.



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

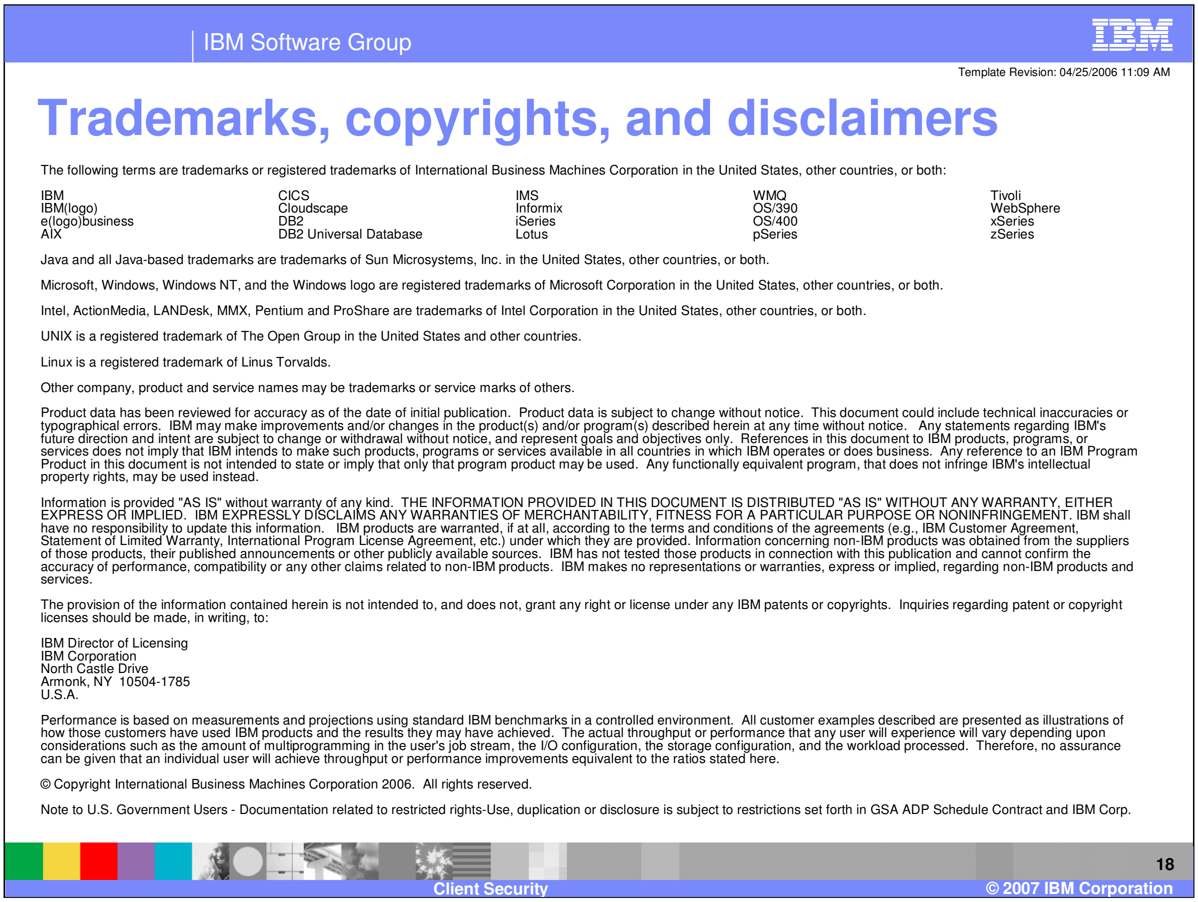
•WDI Client now supports security. Security is optional for each System and the Configuration database.

•Use Roles to restrict access to object types and to restrict what functions can be performed on those object types.

•Access Groups are use to limit which specific objects within an object type can be seen by a user.

•Always ensure that someone, an ‘administrator’, has update access to Systems, the Configuration database options, and User ID Definitions. With this access the administrator will be able to make changes to security as needed.

•Plan your security implementation. There are a large number of ways to implement security. Think it through before charging forward.



Template Revision: 04/25/2006 11:09 AM

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM(logo)
e(logo)business
AIX
CICS
Cloudscape
DB2
DB2 Universal Database
IMS
Informix
iSeries
Lotus
WMQ
OS/390
OS/400
pSeries
Tivoli
WebSphere
xSeries
zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.