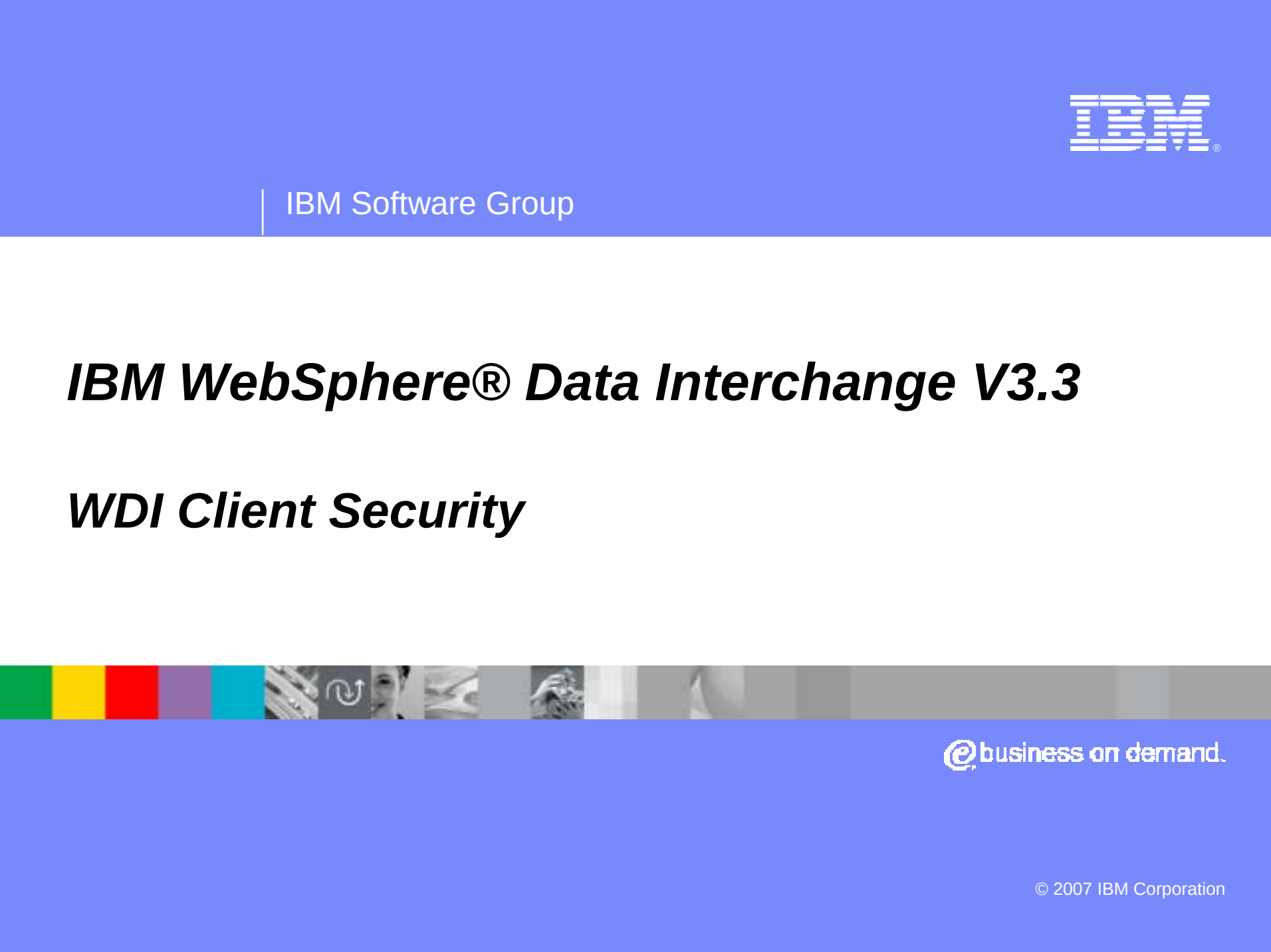
IBM Software Group
IBM WebSphere® Data Interchange V3.3
WDI Client Security
e business on demand.
© 2007 IBM Corporation

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

Agenda

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

WDI 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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