



IBM Software Group

Implementing Role Based Access Control and enabling Audit Trail support using WDI v3.3 Client

Jon Kirkwood (kirkwoo@us.ibm.com)
WebSphere Data Interchange L2 support
December 13, 2012



WebSphere® Support Technical Exchange



Agenda

- Overview of WebSphere Data Interchange Client Security
- Role Based Access Control
- Permissions and User IDs
- Access Groups
- Example of a Role Based Solution
- Audit Trail of Changed Objects

Client Security Overview

- Comprised of two components
 - ▶ **Role Based Access Control** is intended to limit access to object types and limit the functions that can be performed on an object type
 - ▶ **Access Groups** is intended to limit which objects a user can see within an object type
- Each component can be used without the other or they can be used together
- Each is controlled by User ID definitions
- Only protects your database from within Client
- Does not override underlying DB2 authorizations

Client Security Overview (continued)

- WDI Server (at runtime on z/OS, AIX, or Windows) does not participate in WDI Client security
 - ▶ except PERFORM IMPORT or DELETE functions which could affect system settings
- Traditional DB2 (grant execute on plan) privileges control WDI Server access to the tables
- DB2 Data Definition Language (DDL) is supplied to support various Roles to limit a user's direct access to tables

<http://www.ibm.com/support/docview.wss?uid=swg27015548>

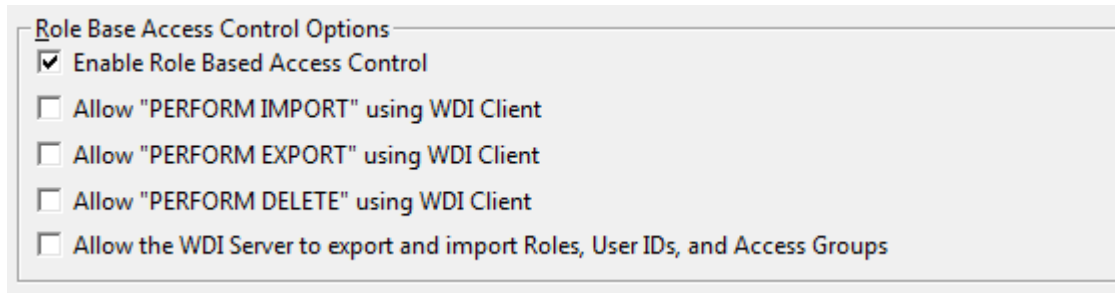
Client Security Overview (continued)

- By default, WDI Client security is disabled
- Configuration and System databases are controlled separately
 - ▶ Configuration database security would be needed only in a shared environment, not for stand-alone wdiclient33cfg.mdb Data Source
 - ▶ Each (DB2) System database, e.g. test vs. production, are controlled separately
- This presentation will focus on the setup of System databases
- Refer to Chapter 2 of the WDI 3.3 Administration and Security Guide:
<http://www.ibm.com/software/integration/wdi/library/pubs/>

Role Based Access Control

- Restricts what object types a user can view
- Restricts what functions a user can perform
- Use the System Editor to enable or disable

View menu -> Administration -> System -> open desired System -> Security Options tab -> Check box "Enable Role Based Access Control"



Note: to open a System's Security Options tab, first connect to the System by opening anything from that system, e.g. open a list of maps

Role Based Access Control (continued)

- You must have authority to update System objects on Configuration database and on target System before you can enable role based access control
- Ensures that you will be able to turn off role based access control if needed

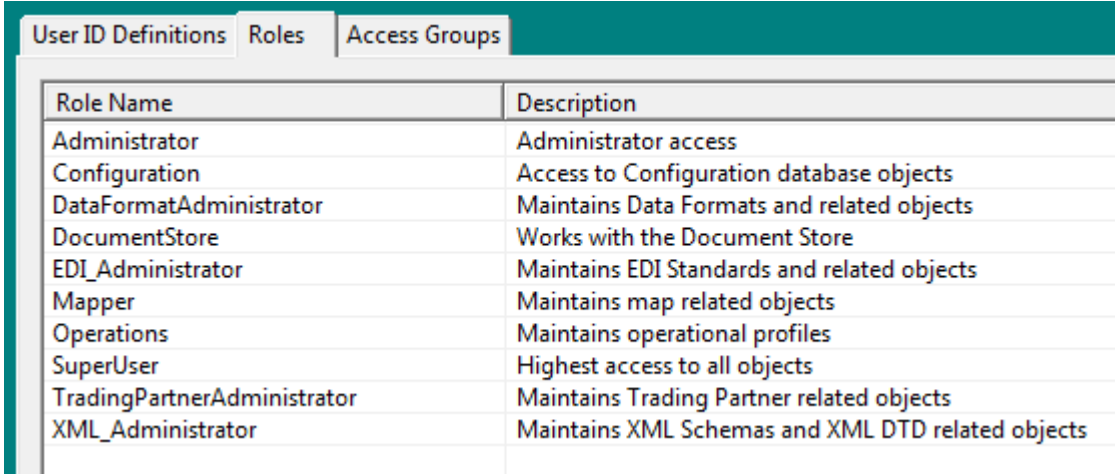
Role Based Access Control (continued)

- Once 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



Role Based Access Control (continued)

- Many preset Roles already defined, such as



Role Name	Description
Administrator	Administrator access
Configuration	Access to Configuration database objects
DataFormatAdministrator	Maintains Data Formats and related objects
DocumentStore	Works with the Document Store
EDI_Administrator	Maintains EDI Standards and related objects
Mapper	Maintains map related objects
Operations	Maintains operational profiles
SuperUser	Highest access to all objects
TradingPartnerAdministrator	Maintains Trading Partner related objects
XML_Administrator	Maintains XML Schemas and XML DTD related objects

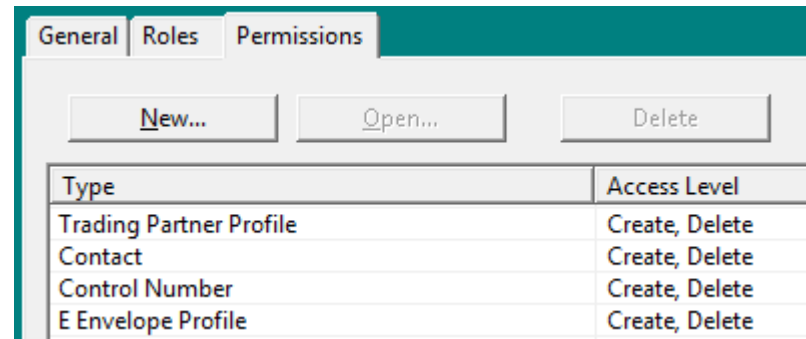
- Update existing Role(s) or define new Roles as needed

Permissions and User IDs

- User IDs are defined for a user that will log-on to an enabled System
 - ▶ Can be assigned to zero or more Roles
 - ▶ Can contain specific object permissions, which override Role permissions
 - ▶ Can be assigned to zero or more Access Groups
- User ID Definitions must be entered exactly as they appear on the System's server – case sensitive

Permissions and User IDs (continued)

- Roles are assigned Permissions for each object type



Type	Access Level
Trading Partner Profile	Create, Delete
Contact	Create, Delete
Control Number	Create, Delete
E Envelope Profile	Create, Delete

- User IDs are assigned to Role(s)
- Default user &WDIUSER (optional) is provided to define general access for any users not specifically defined to the System
- One Role can be nested under another Role, where nested permissions are merged

Permissions and User IDs (continued)

- A User ID can be defined to Role(s) or given specific permissions
- Any specific permissions take precedence over a given role's permissions
- “Summary” button conveniently displays all permissions given to a User ID

Permissions and User IDs (continued)

■ Permission levels

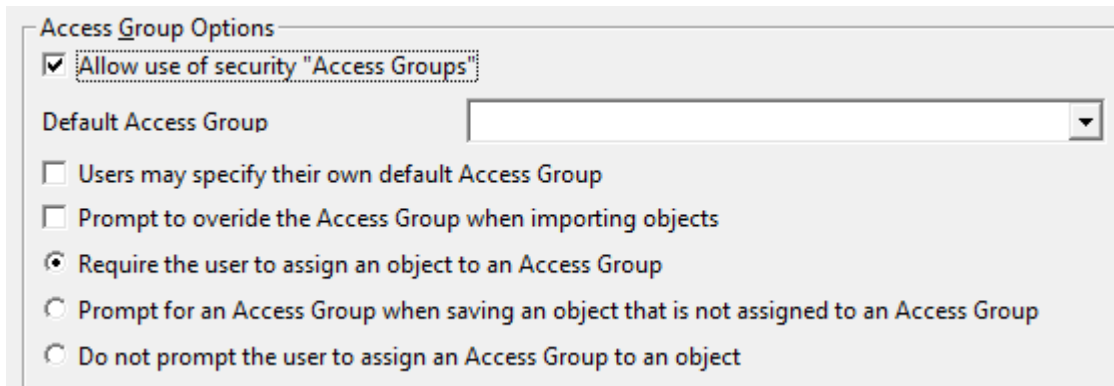
- ▶ None – user cannot access the object type
- ▶ Read – user can view objects within the object type
- ▶ Update – includes “read” access and allows user to perform update actions against the object type
- ▶ Create – includes “update” authority plus the ability to create objects within the object type
- ▶ Delete – ability to delete objects within object type, but also requires “read”, “update”, or “create” permission
- ▶ Submit – applies to object types that can be submitted to WDI Server, but also requires “read”, “update”, or “create”

■ Default is “read” for most object types

Access Groups

- Used to limit which objects a user can see within an object type
- Enable or disable via the System Editor

View menu -> Administration -> System -> open desired System → Security Options tab -> Check box "Allow use of security Access Groups"



Access Group Options

Allow use of security "Access Groups"

Default Access Group

Users may specify their own default Access Group

Prompt to override the Access Group when importing objects

Require the user to assign an object to an Access Group

Prompt for an Access Group when saving an object that is not assigned to an Access Group

Do not prompt the user to assign an Access Group to an object

Note: to open a System's Security Options tab, first connect to the System by opening anything from that system, e.g. open a list of maps

Access Groups (continued)

- 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
- Not available for the Configuration database

Example – Role Based Solution

- Several security scenarios for server access control by Role are provided in the WDI 3.3 Administration and Security Guide Appendix
- A quick and effective scenario will be covered here
- This is also documented as a technote on the WDI support portal:

<http://www.ibm.com/support/docview.wss?uid=swg21592034>

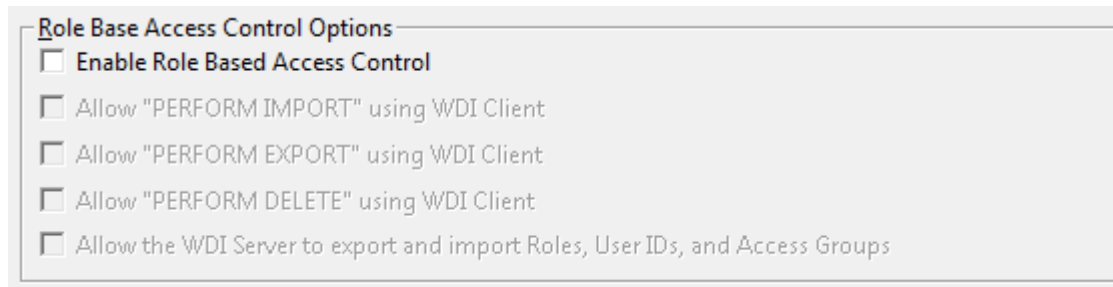
Note: Attachment therein will be referenced later

Example – Role Based Solution (continued)

- Question: How do I enable WDI Client Role based access whereby I have one set of Administrators who need full access to everything and all other users have read-only access?
- Answer: This Role based access requirement can be satisfied by adding specific administrator user IDs which are assigned the highest permission allowed, including delete. And then using default &WDIUSER to accommodate all others, i.e. read only users.

Example – Role Based Solution (continued)

- 1) Ensure role-based access is disabled – go to View menu -> Administration -> System -> open desired System -> Security Options tab
 - ▶ Verify that there is no check mark by "Enable Role Based Access Control"

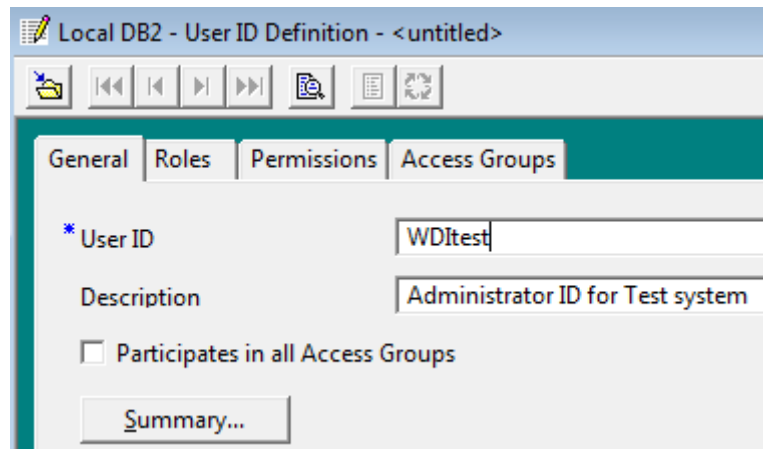


Example – Role Based Solution (continued)

- 2) Verify that the SuperUser role has all permissions set to the highest allowable setting
 - Go to View -> Administration -> Security
 - From Roles tab, double-click "SuperUser"
 - From SuperUser Role Permissions tab, verify settings are all at maximum, including "Delete" wherever possible
 - Alternatively, import SuperUser role in technote attachment:
"SuperUser_Role_highest_permissions.eif"

Example – Role Based Solution (continued)

- 3) Add your own userid as a SuperUser.
- Go to View -> Administration -> Security
 - From User ID Definitions tab, click New
 - Enter your User ID value exactly as it is defined to on the server – it is case sensitive
 - Uncheck “Participates in all Access Groups”



Example – Role Based Solution (continued)

- Move to the Roles tab and move SuperUser from the Unselected Roles list to the Selected Roles list

Select the Roles that the User ID will participate in.

Unselected Roles

Role Name	Description	
Administr...	Administ...	
Configura...	Access to...	
DataForm...	Maintain...	
Documen...	Works wi...	
EDI_Admi...	Maintain...	
Mapper	Maintain...	
Operations	Maintain...	
TradingPa...	Maintain...	
XML_Adm...	Maintain...	

>>
>
<
<<

Selected Roles

Role Name	Description	
SuperUser	Highest a...	

- Save and repeat step (3) to add any other User IDs as SuperUsers who require full access

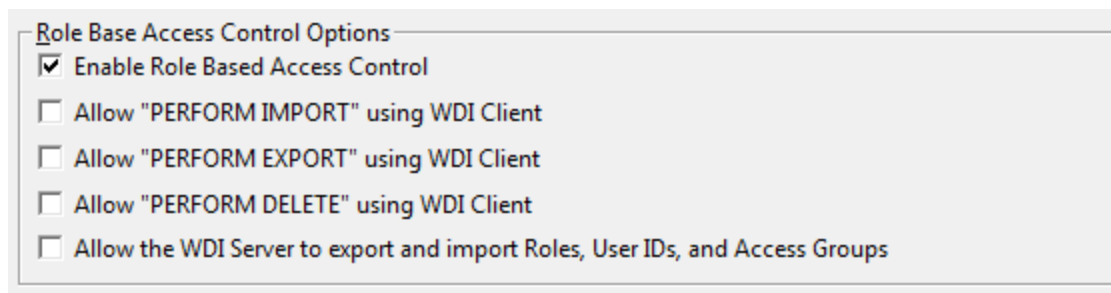
Example – Role Based Solution (continued)

- 4) Update the predefined &WDIUSER User ID such that no Roles and no Permissions are defined
 - Remove any Roles or Permissions if specified – the default is “read” access
 - This special User ID will then be used for all others who access WDI, which will be for “read” only
 - No need to add any User IDs specifically for this set of users

Example – Role Based Solution (continued)

5) Enable Role based access

- Go to View menu -> Administration -> System -> open desired System -> Security Options tab
- Check the box to "Enable Role Based Access Control"



Role Base Access Control Options

- Enable Role Based Access Control
- Allow "PERFORM IMPORT" using WDI Client
- Allow "PERFORM EXPORT" using WDI Client
- Allow "PERFORM DELETE" using WDI Client
- Allow the WDI Server to export and import Roles, User IDs, and Access Groups

Example – Role Based Solution (continued)

- 6) Save the Security Options and restart WDI Client for any changes to be effective
- 7) Issue DB2 GRANT statements as appropriate for the Role
 - While Role based security controls what options the user can see, and opens objects accordingly, DB2 GRANT permissions control the underlying database table security

Example – Role Based Solution (continued)

- See the base WDI Server installation paths for all-inclusive GRANT statements:
 - ▶ Windows installation path:
C:\Program Files\IBM\WDIServer\V3.3\ddl\grntec33.ddl
 - ▶ AIX installation path:
/opt/IBM/WDIServer/V3.3/ddl/grntec33.ddl
 - ▶ z/OS installation Partitioned Data Set (PDS) and member name:
EDI.V3R3M0.SEDISQL1(EDISGRNT)

Example – Role Based Solution (continued)

- Administrators require full authority as provided for tables and views therein
 - ▶ Change “PUBLIC” or “USER0x” to specific administrator ID(s)
- For all other non-administrator User IDs, i.e. those not specifically defined via WDI Client
 - ▶ Copy and modify GRANT statements to only allow SELECT (read) authority on each object
 - ▶ Change “PUBLIC” or “USER0x” to specific User ID(s)

Audit Trail of Changed Objects

- Optional Audit Trail support keeps an audit trail of changed database objects
- Audit entry created for any configuration change events
- System specific, e.g. Test or Production
- Also support for the Configuration database
- Applies to all users of the System



Audit Trail of Changed Objects (continued)

- Records User ID and date/time for each time an object is changed, not just the last updated date/time
- Records the “Action” that was taken, e.g. Create, Update, Compile, etc.
- Supports server import functions



Audit Trail of Changed Objects (continued)

- Use System Editor or Configuration database options to enable or disable

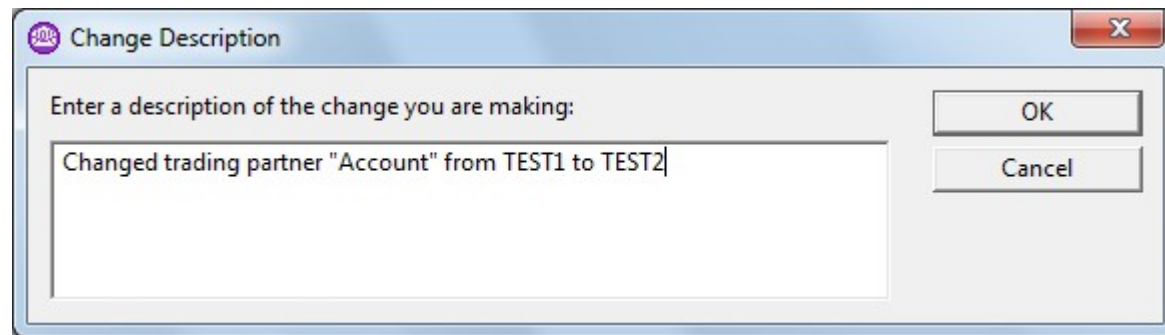
View menu -> Administration -> System -> open desired System -> Audit Trail tab -> Check box "Enable Audit Trail"

The screenshot shows a configuration dialog box with the following elements:

- Tabbed interface with tabs: General, User Options, System Options, **Audit Trail**, Security Options.
- Section: **Audit Trail**
- Check box: **Enable Audit Trail**
- Section: **Audit Trail Entry Descriptions**
- Radio buttons:
 - Require the user to enter a description of the change
 - A prompt will be displayed to collect an optional description
 - A prompt will not be displayed to collect a description
- Check boxes:
 - Release Migration documents each object imported
 - Import documents each object imported
 - WDI Server writes to the Audit Trail
 - Purge old Audit Trail entries
- Text input field: Keep Audit Trail entries for this number of days

Audit Trail of Changed Objects (continued)

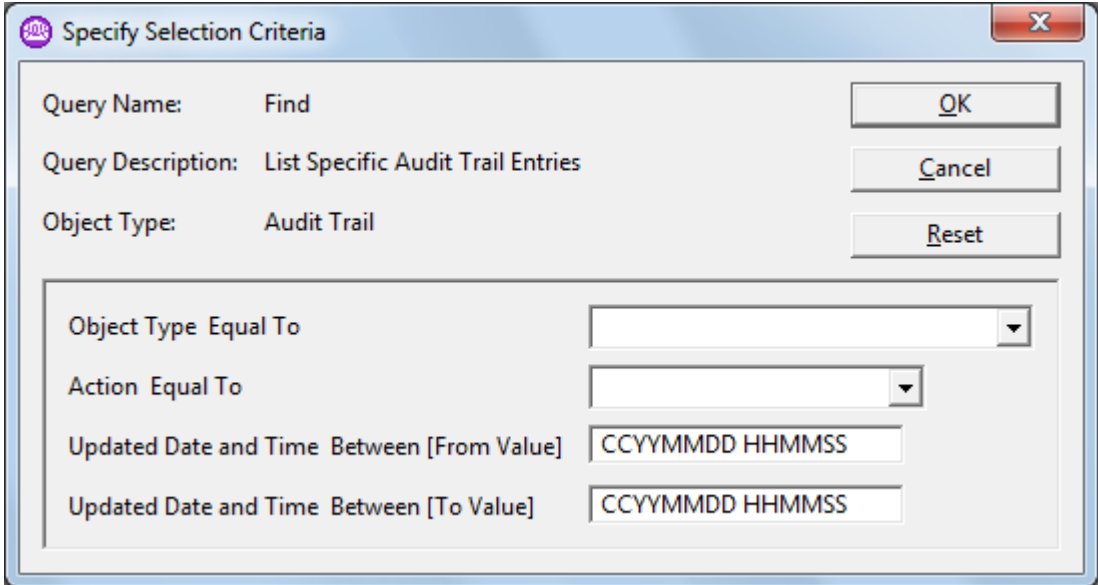
- While there is no attempt in the Audit Trail to document old and new values, the user can be forced to enter a description of the change



- The Audit Trail cannot be used to automatically restore altered or deleted objects

Audit Trail of Changed Objects (continued)

- Query the Audit Trail log from View menu -> Audit Trail



The dialog box 'Specify Selection Criteria' contains the following fields and controls:

- Query Name: Find
- Query Description: List Specific Audit Trail Entries
- Object Type: Audit Trail
- Buttons: OK, Cancel, Reset
- Object Type Equal To: [Dropdown menu]
- Action Equal To: [Dropdown menu]
- Updated Date and Time Between [From Value]: CCYYMMDD HHMMSS
- Updated Date and Time Between [To Value]: CCYYMMDD HHMMSS

Audit Trail

Object Type	Object Name	Action	Updated User ID	Updated Date and Time	Description
Trading Partner Profile	SAMPLE_PARTNER	Update	JonKirkwood	11/27/2012 4:19:56 PM	Changed trading partner "Account" from TEST1 to TEST2
Data Transformation Map	POXML5SR-EDI	Compile	JonKirkwood	11/27/2012 4:19:24 PM	Compiling map

Audit Trail of Changed Objects (continued)

- Audit Trail entries are stored in DB2 table:
EDIENU33.EDIAUDITHDR
- “Purge old Audit Trail entries” option only available for local Windows database, e.g.
wdiclient33dev.mdb
- Once enabled, plan to do periodic maintenance to keep the table from filling-up, e.g.
 - ▶ PERFORM REMOVE AUDIT TRAIL WHERE
LOGDATE(*-9999) TO(*-30)

Summary

- You can now secure WDI Client related data according to business needs
- Use Roles to control users who perform similar tasks
- Use Access groups to further limit which objects a user can see within an object type
- Plan your security implementation
- You can also now utilize WDI Audit Trail features

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
<http://www.ibm.com/developerworks/websphere/community/>
- Join the Global WebSphere Community:
<http://www.websphereusergroup.org>
- Access key product show-me demos and tutorials by visiting IBM® Education Assistant:
<http://www.ibm.com/software/info/education/assistant>
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
<http://www.ibm.com/software/websphere/support/d2w.html>
- Sign up to receive weekly technical My Notifications emails:
<http://www.ibm.com/software/support/einfo.html>

Connect with us!

1. Get notified on upcoming webcasts

Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe

2. Tell us what you want to learn

Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com

3. Be connected!

Connect with us on [Facebook](#)

Connect with us on [Twitter](#)

Questions and Answers