Multi User Single Device Scenario – Need of Mod User Handling Feature, an Introduction

Applies to:

SAP NetWeaver 7.3 release.

Summary

This document aims at explaining scenarios in a multi-user, single device scenario using the feature 'Mod User Handling.

Author: Rashmi B R

Company: SAP Labs India Pvt Ltd

Created on: 29 December 2010

Author Bio

Rashmi is with SAP Labs Pvt. Ltd for the last 3 years working as a Senior Quality Engineer in the SAP Netweaver Mobile Engineering Services team.

Table of Contents

Introduction

Currently when an application is used by multiple users on a single mobile device, the client database updates maybe synchronized with the mobile at once. And always the synchronizing user's context is transferred to the BE, i.e., technically the BAPIs are always called in the synchronizing user's name. Hence the Message Monitoring on NWMA portal always logs the operations done in synchronizing user's name, though the operations might have been done by some other user.

Also in the second scenario, currently the same RFC destination is used for all read and write calls from DOE to BE irrespective of the authorizations of the user configured in the RFC.

Business Context

Scenario 1:

Multiple users may modify data in a Mobile application from the same mobile device (Client/Receiver) and synch with the DOE.

In this context, the user who modifies (Create, update, Delete) the data (Mod User) on the Mobile client and the user who synchronizes data (Sync User) with DOE might be different.

With this feature, DOE can identify two kinds of users Mod User and Sync User. When Mod User updates a record on the client and Sync User synchronizes with the DOE, the feature enables the DOE to transfer the user context of Mod User to the BE though User B had actually done the synchronization.

Scenario 2:

In certain cases, there are applications where a device is shared by multiple users and where applications BE have strict user specific logging and audit functionalities. In such a context, a Mod User and a Sync User have different authorizations.

Hence without this feature enabled, logging and audit functionality do not work as expected, as the BE will always end up updating Sync User to be the changed user where actually it got modified by Mod User.

Scenario 3:

In certain cases, BE application demands separate user with specific rights, to read complete data from BE to DOE. With this feature, new configuration parameter to specify the RFC destination to be used for read calls from DOE to BE is provided. This leads to the fact that the user who invokes a read BE BAPI wrapper call from DOE shall have the right BE authorizations to retrieve the relevant data from BE to be loaded to DOE.

Scope

The scope of the document is to give an overall understanding and the need of the feature for the scenarios that involve multiple users working in tandem using a single device.

The document gives an insight into the operational details of feature using the new configuration parameter SWITCH_TO_MOD_USER along with the usage of BAdi exits in user Authorization Management.

Out of Scope

This document does not cover the usability of feature for application with attachments, application that require a specific user to be configured for BE reads(Scenario 3 explained in the Business Context) and scenarios requiring restart of message.

Assumptions

1. This solution works as expected only in case of systems having trusted relationships.
2. It is expected that the Mod User sent from the client will be a valid user in DOE and has the authorization S_RFCACL object assigned to that user in the trusting system
3. It also assumed that the client framework sends transactional message (single record in a message) and that user who modified the record will be captured and will be part of Data object communication header – MOD_USER field for every message that is sent to DOE.
4. This solution holds good for any custom client implementation provided
   a. It follows one MOD_USER value per upload message
   b. All upload messages are transaction messages(single record in a message)
   c. MOD_USER value filled with user who modified the record

Prerequisites

1. A Data Model containing a Standard Bi-directional Data Object with a BE Adapter supporting ALL the following BAPI Wrappers: getList, getDetail, create, update and delete.

   NOTE: Apart from performing their tasks, all the BAPI Wrappers should log the calling username
2. RFC destination to the BE (which MUST be a different system or different client from DOE) should be a 'Trusted' RFC connection which connects with the logged in user's credentials.
3. An MCD for a Mobile application for the above Data Object that supports all the above functionalities.
4. 2-3 logical devices assigned with the MCD and some users assigned to them
5. A simple DM with a bulk rule to distribute all instances of the Data Objects
6. At least two different users on BE and DOE who have the authorizations necessary to be impersonated by each other (Authorization object S_RFCACL is documented here), and to use a mobile client in DOE. Say USER_A and USER_B
7. At least one other user in BE system which does not exist in DOE system. Say USER_C
8. An active implementation of a BAdI must exist. For the sake of simplicity, a mechanism to verify that the BAdi implementation is executed is sufficient.

Use cases covered

1. Use Mod User context while replicating data to backend incase Sync User and ModUser are different using trusted RFC connections.

2. Enablement of Authorization Management for mobile users: Scenario where BAdi exits can be implemented for SWCVs to manage authorization for mobile users.

When two or more users share a device, they must have the authorization to make RFC calls on behalf of each other. BAdi implementation can dynamically assign requisite authorizations to users sharing a device whenever a user is assigned to un-assigned to it. The implementation will be called each time a user is added to or deleted from a device which has MCDs corresponding to one or more context switch enabled (Mod User Enabled) SWCVs. The implementation must then assign or un-assign the necessary field values in the authorization object S_RFCACL to all the affected users

Use cases in Detail:

Use Case 1:

1.1 Switch on/off parameter SWITCH_TO_MOD_USER:

The Configuration parameter SWITCH_TO_MOD_USER can be switched ON/OFF on the NWMA portal. The parameter can be located under the Backend Configuration in the Configuration tab. This Configuration needs to be set for a specific SWCV/DO/Adapter.

1.2. Sync User Context processing (i.e. with parameter switched off):

By default, when the parameter SWITCH_TO_MOD_USER is switched OFF, there is no differentiation between the Mod User and Sync User i.e., e.g. if User_A had updated a record on the client and User_B sync with the DOE, the BAPIs are called in User_B context and hence the message monitoring on the NWMA portal shows the updates in User_B's name.

1.3 Mod User Context Processing (i.e. with parameter switched on):

When the parameter SWITCH_TO_MOD_USER is switched ON, User_A modifying a record is propagated to the BAPI call which might be done in a later point in time. Hence if a User_B synchronizes with the DOE, BAPIs are called in User_A's context. This enables logging the actual information on NWMA portal that may be required for audit and other such requirements.

Also on the NWMA portal, inside Logs and Traces, under the environment FLOW, a message is logged indicating the user context was switched from User_B to User_A.

1.4 Mod User Context processing with invalid DOE User/ Mod User Context processing with insufficient authorizations:

When User_C that is non-existent on the DOE updates a record in the application and User_A synchronizes, the inbound queue of the logical device gets blocked with relevant error message. An appropriate message will be logged to be available for Monitoring in the Queue Tracking section on the NWMA portal's Monitoring tab.

Use Case 2:

A BAdi implementation implementing the methods of the interface SDOE_USER_GROUP_MGMT_INTF has to be written. The methods CREATE_DEVICE, MANAGE_DEVICE_USER_GROUP, DELETE_DEVICE have to be implemented with the suitable enhancement definitions to manage user authorizations.

2.1 Switching ON the configuration parameter SWITCH_TO_MOD_USER.

CREATE_DEVICE will be called for all the devices to which your MCD is assigned.

MANAGE_DEVICE_USER_GROUP will also be called for all the devices to which the MCD is assigned.

2.2With the configuration parameter SWITCH_TO_MOD_USER switched on.

2.2.1 Assign MCD to the device:

The BAdi Method CREATE_DEVICE and MANAGE_DEVICE_USER_GROUP will be called.

2.2.2 Assign User to the device:

The BAdi Method MANAGE_DEVICE_USER_GROUP will be called.

2.2.3 Unassign User to the device:

The BAdi Method MANAGE_DEVICE_USER_GROUP will be called.

2.2.4 Unassign MCD to the device:

The BAdi method DELETE_DEVICE will be called.

2.2.5 Delete Device to the device:

The BAdi method DELETE_DEVICE will be called.

2.3 Switching OFF the configuration parameter SWITCH_TO_MOD_USER.

The BAdi method DELETE_DEVICE will be for all the devices to which the MCD has been assigned.

Abbreviations

BE	Back End
NWMA	NetWeaver Mobile Administration
DOE	Data Orchestration Engine
RFC	Remote Function Call
BAPI	Business Application Programming Interface
BAdi	Business AddIns
DO	Data Object
SWCV	Software Component Version

Related Content

http://www.sdn.sap.com/irj/scn/weblogs?blog=/pub/wlg/17393

http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/d0456c54-0901-0010-f0b3-cd765fb99702

http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/a0f05426-bde5-2d10-12aa-ac96fdb560f0

Copyright

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.