Step-by-Step Process to Configure LDAP Support for MDM

Applies to:

SAP Master Data Management 5.5 SP06

LDAP (Microsoft Active Directory Server)

For more information, visit the Master Data Management homepage.

Summary

This document explains how we can configure LDAP support for MDM so that LDAP acts the centralized user repository without the need to store user information in MDM.

Author: Shilpa Bhanot

Company: Infosys Technologies Limited

Created on: 15 February 2009

Author Bio

Shilpa Bhanot is working at Infosys Technologies Limited as a NetWeaver-Java Consultant. She has worked on J2EE, SAP-HTMLB, Enterprise Portal and Web Dynpro.

Table of Contents

Introduction

MDM, apart from being a repository of data, has also to store user information like roles, privileges, etc. As the number of users increases, so does the dependency on MDM. There is a need to remove the dependency on MDM for user information and keep its functionality for the sole purpose of data storage, maintenance and retrieval.

LDAP is a sort of database that allows a company to control, configure and distribute user privileges, rights, and access from a single location. Without LDAP, the system manager is forced to maintain familiarity with the proprietary access control mechanism offered by each software product, and to use each one to separately maintain access control information every time an employee is hired, moves, changes job within the organization, and so on.

Imagine a company with thousands of employees and dozens of programs requiring access control, and it becomes clear how much of a burden it can be to manage access control without LDAP. By contrast, by using MDM in conjunction with LDAP, MDM customers can manage access control information in a single location with a common, familiar interface of their choosing. The motive is to centralizing user information outside of MDM repositories.

For MDM to support LDAP, SAP has designated the information that MDM will be querying from and that must be entered and maintained within the customer's LDAP database/directory.

Prerequisites

- Users should exist in LDAP.
- At least one user LDAP must have read access to LDAP.

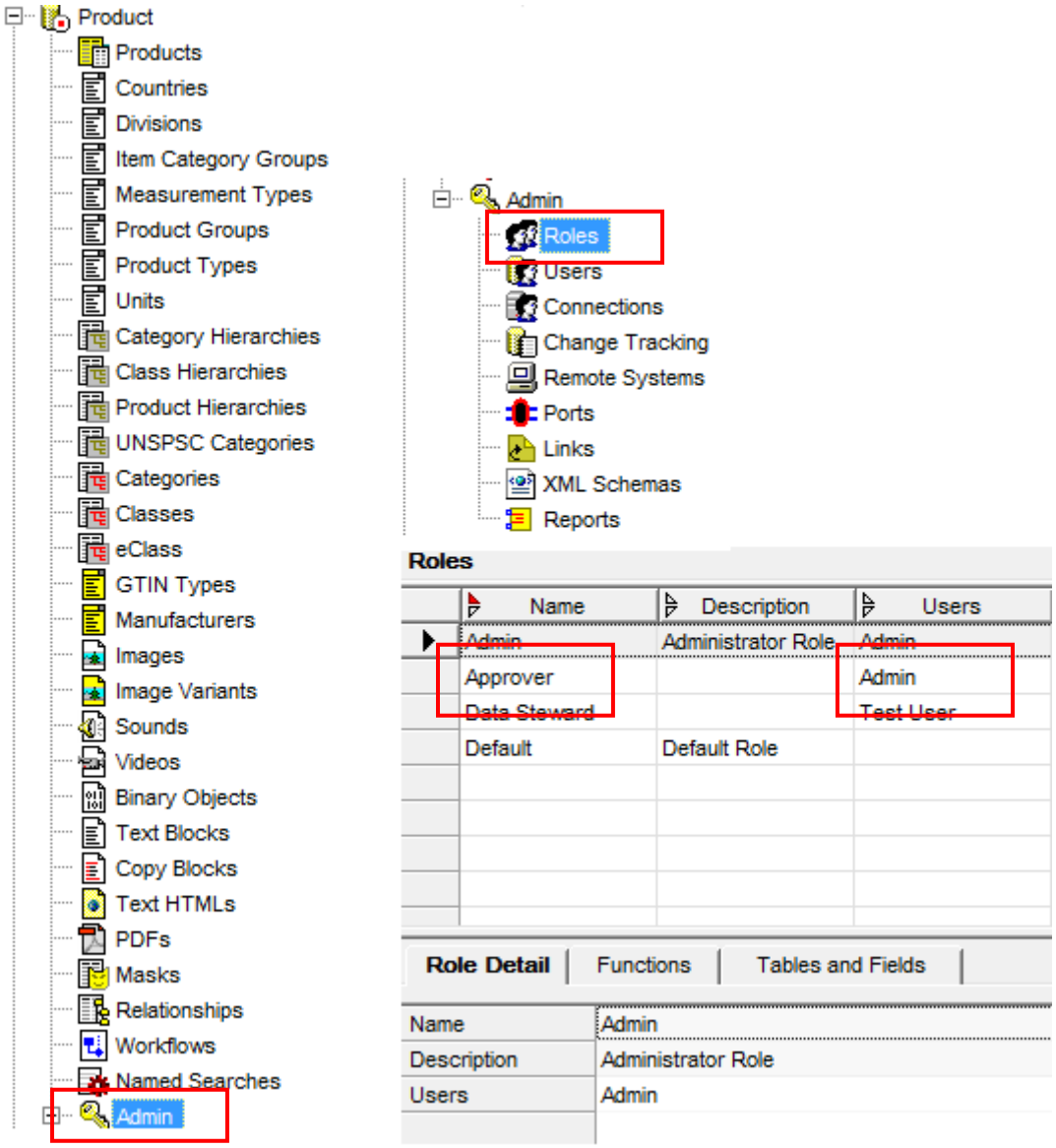
The Step-by-Step Solution

1. Changes in LDAP and MDM

- Remove all the users from MDM. One user can be kept as a fallback user.
- Create requisite roles in MDM.

  Go to MDM Console and login with default user.

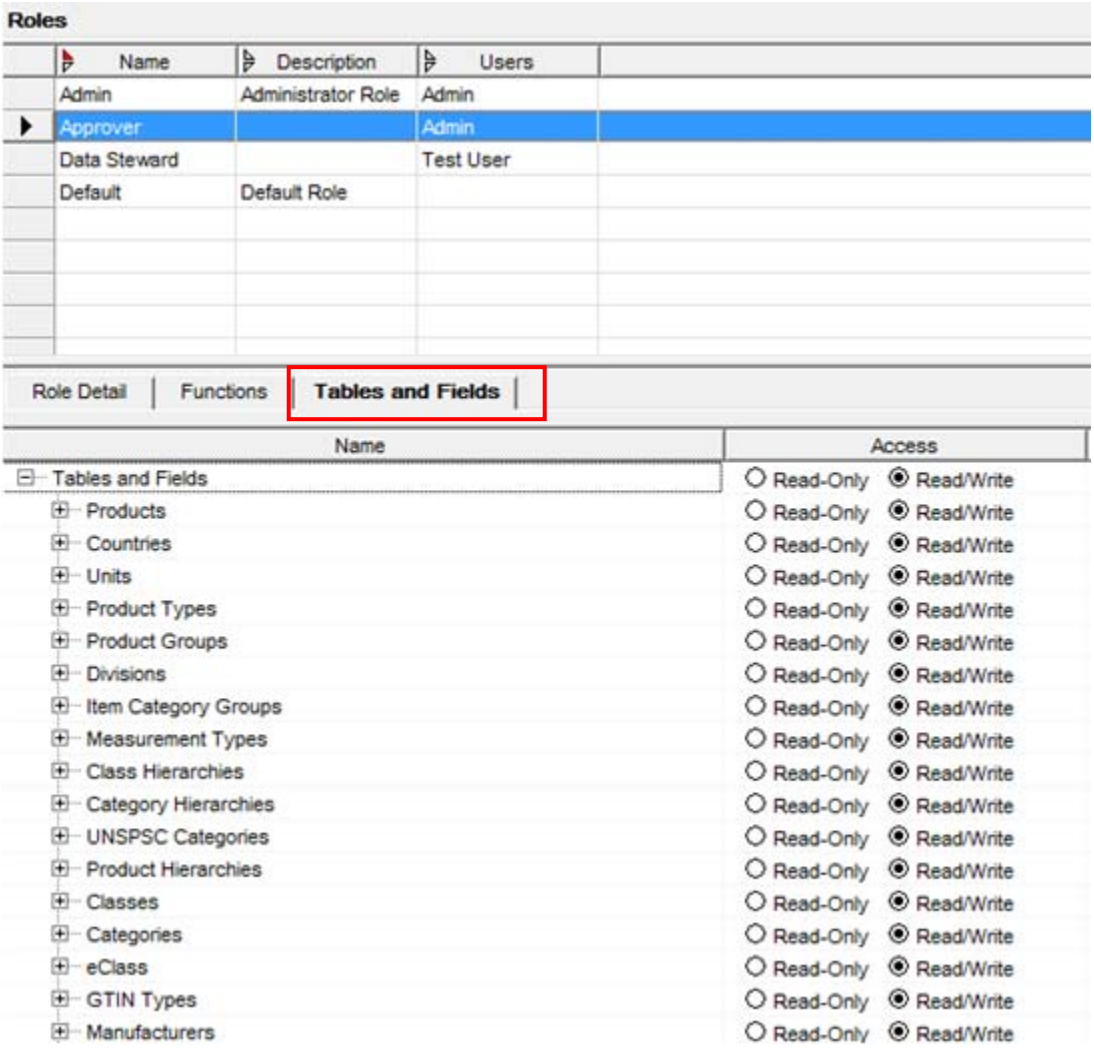
  Navigate to **Repository- >Admin - >Roles**



- Define the roles according the read/write permissions in various **Tables and Fields** in the repository as shown below.

  Here we have two users

1. Admin has been given Approver role.
2. Test User has been given Data Steward role.



MDM LDAP FIELDS

Create MDM LDAP field in LDAP or use existing LDAP field and populate it. Presently, MDM requires the addition of only one attribute field: MDMRoles – a list of role names separated by semi-colons (;).

Note: While SAP suggests the name MDMRoles, you are free to choose any name that suits your situation. Since LDAP can allow multiple instances of an attribute, MDM will concatenate multiple entries as though they were in a single record separated by semi-colons.

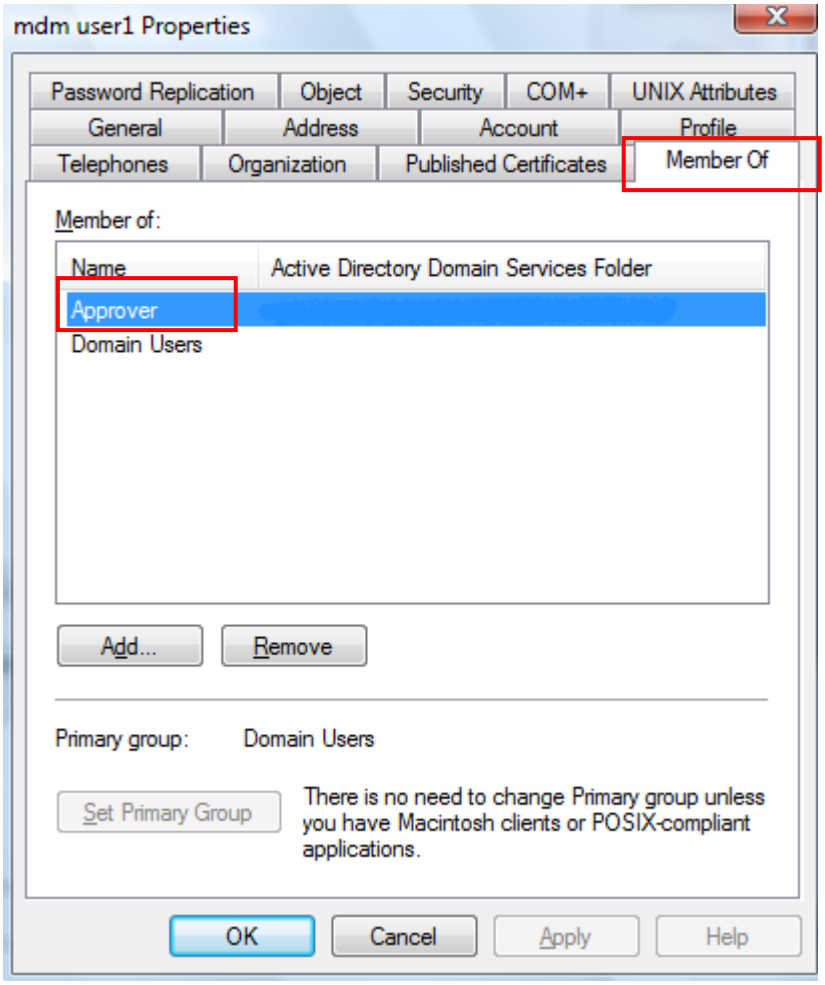
The following examples show MDM authenticating with an MS Active Directory. It uses existing **MemberOf** field of LDAP. Other user directory brands from different providers may offer a similar attribute for group membership.

- Create groups in LDAP of the same name as Roles in MDM and assign them to the users according to the privileges that need to be given to them in MDM for example:

Groups will be :

1. Approver
2. Data Steward

- Assign the users to the groups via **MemberOf** field of LDAP.

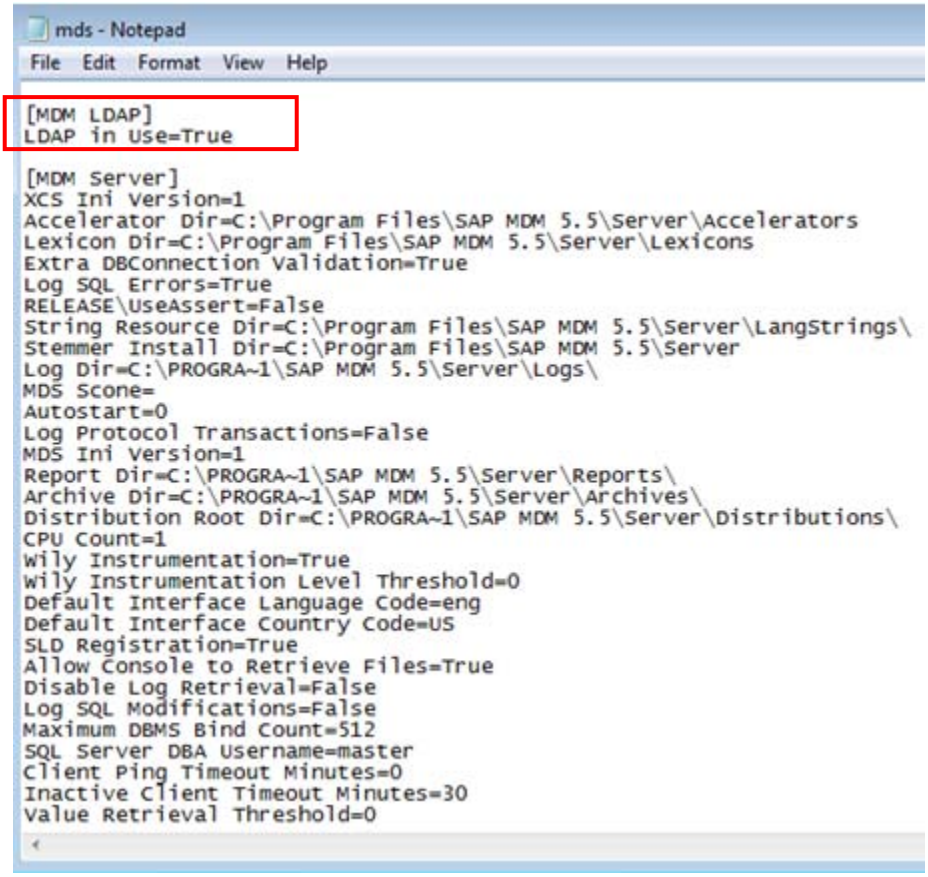


2. Changes in mds.ini File

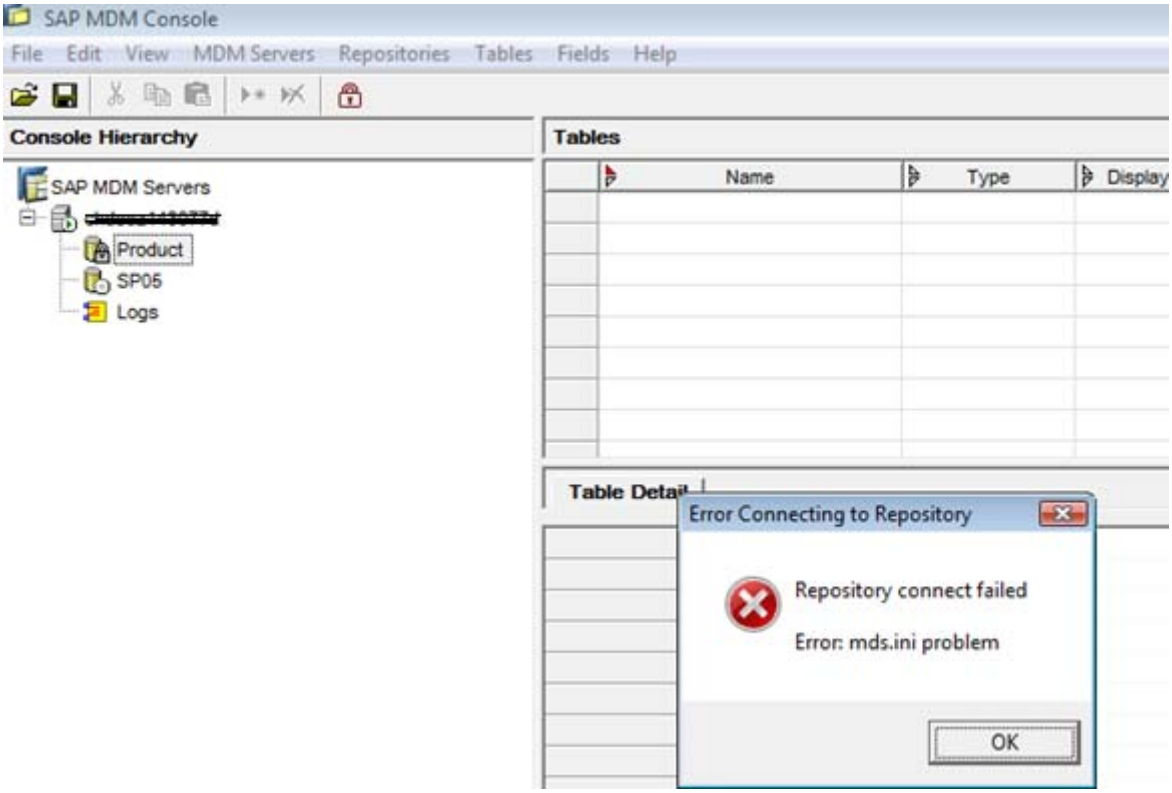
LDAP contact information and other parameters relevant to MDM are maintained in the secure **mds.ini** file in a separate section named: [MDM LDAP]
Locate the mds.ini configuration file in MDM server
Path : **MDM 5.5- >Server- > mds.ini**

If there is no [MDM LDAP] section in mds.ini file or LDAP in Use = False , then LDAP use is disabled.
To enable LDAP support do the following:

- In the beginning of the mds.ini file add
  [MDM LDAP]
  LDAP in Use = True



- Restart the MDM service .
- Login into MDM Console . It will give the following error – **Error:mds.ini problem**



Check the mds.ini file . Server field would have been added to the MDM LDAP section as shown below.

LDAP use is now enabled in MDM.

- Now add other requisite parameters to MDM LDAP section. For more information on LDAP parameters see MDM Console Guide .
  With these parameters, LDAP authorization by the MDM Server proceeds according to the following steps:

Note: While SAP suggests the name MDMRoles, you are free to choose any name that suits your situation. Since LDAP can allow multiple instances of an attribute, MDM will concatenate multiple entries as though they were in a single record separated by semi-colons.

MDM receives a connection request from a client process which includes a UserName and UserPassword.

MDM binds to the LDAP Server using five parameters:

A. LDAP_Host

B. LDAP_Port

C. LDAP_AdminDN

D. LDAP_AdminPass

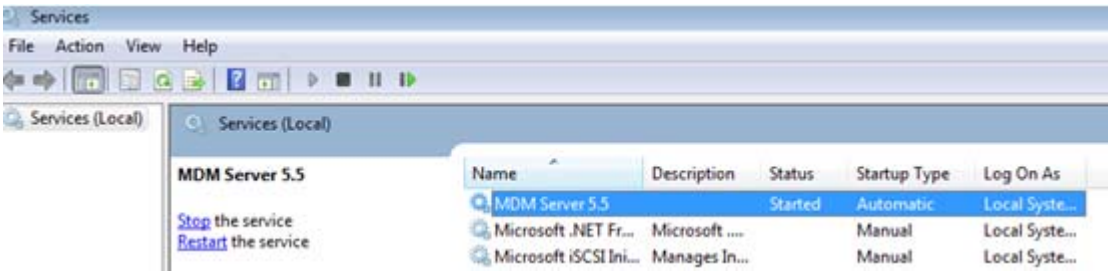
E. LDAP_BaseDN

This can fail if any of the parameter values are inaccurate.

Note: The Admin password needs to be written as
Admin Password = abc123.
After saving and closing the mds.ini file, login into the MDM console. The Admin password will disappear. Instead an encrypted password will take its place in the form:
Admin Password+ = AJFPR23723DFDEOI

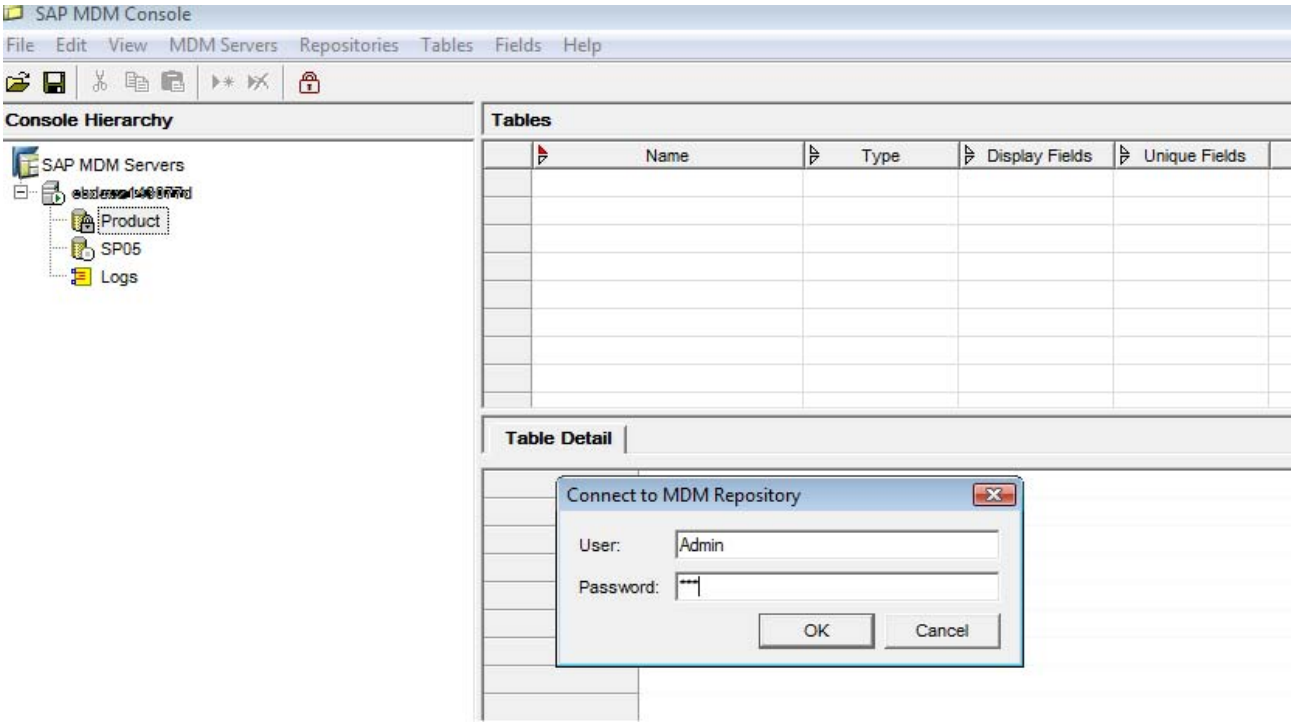
If the Admin Password is left empty, MDM will bind anonymously to LDAP. There is no need to provide and store any passwords in the mds.ini file. But in this case, the user directory must allow anonymous guest bind.

- Restart the MDM server service. (optional)

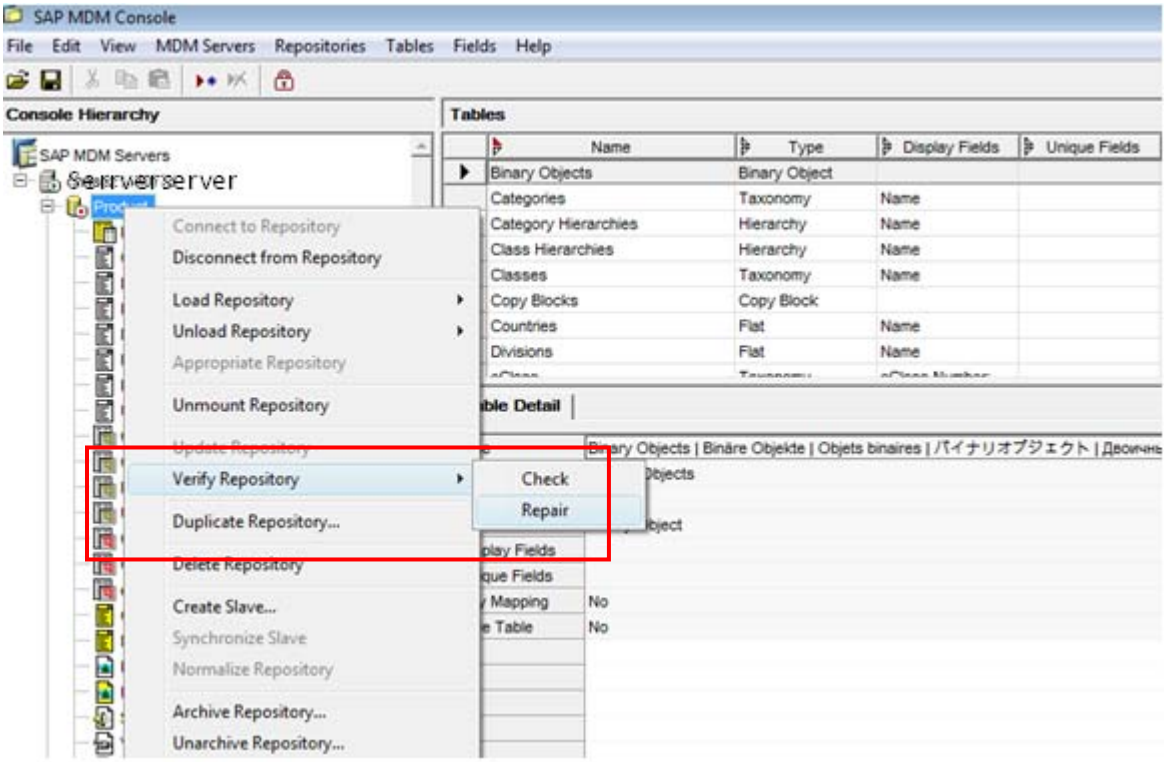


3. Changes in MDM Console

- Login to a repository in MDM Console with a user in LDAP. The user will be able to login into MDM.



- Go to Repository . **Right click the Repository->Verify Repository- >Repair.**



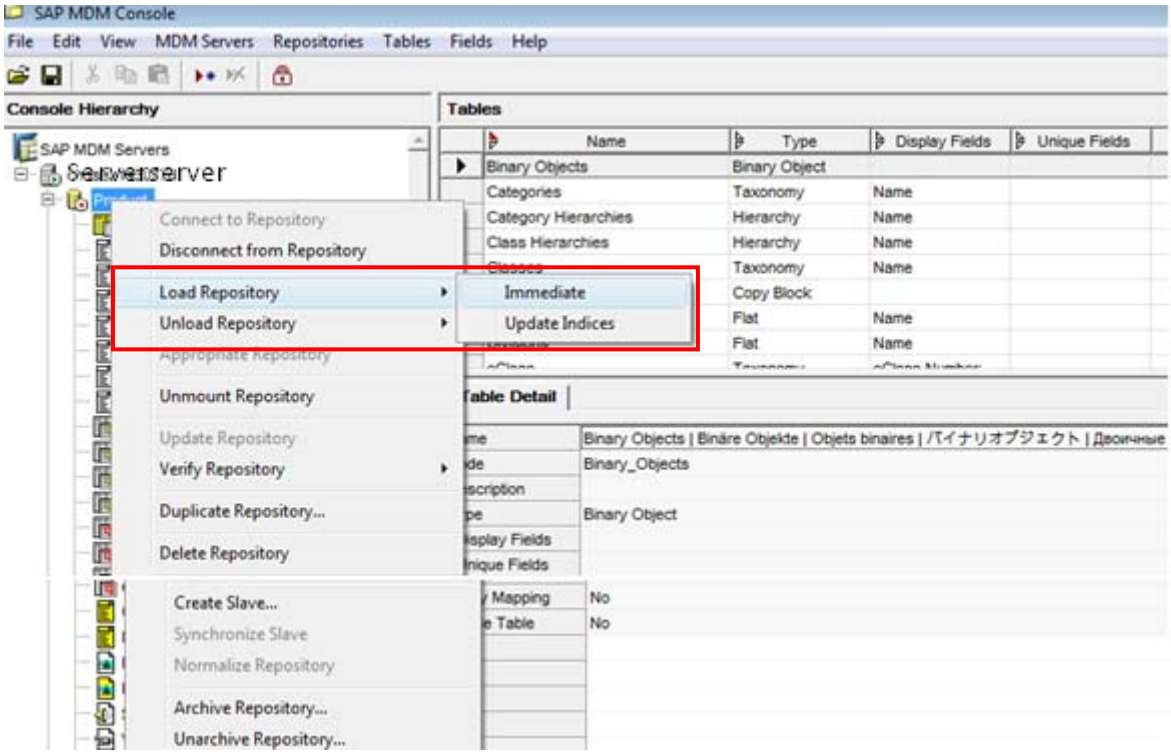
Perform this step to all the repositories.

Note: Verify and repair on every repository must be done every time the authentication method in MDM is switched forth or back to LDAP. In general you do this exactly once when you decide to for LDAP in MDM.

- Load the repository .

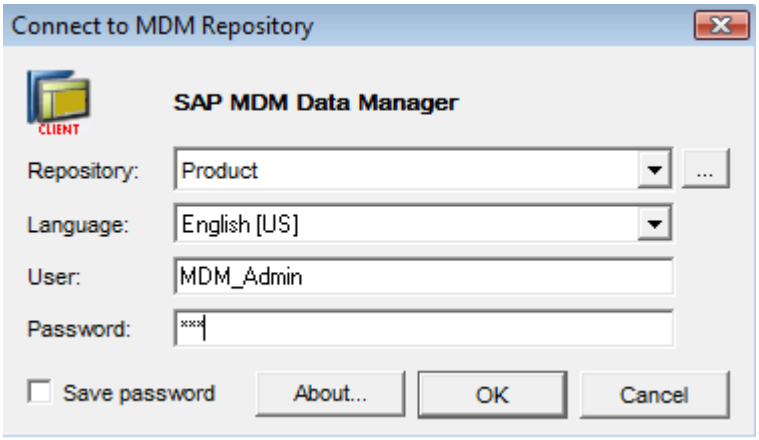
  Right click the Repository->Load Repository->Immediate

  A green arrow appears on the repository after it has been loaded.



4. Login to MDM Data Manager with LDAP user and password

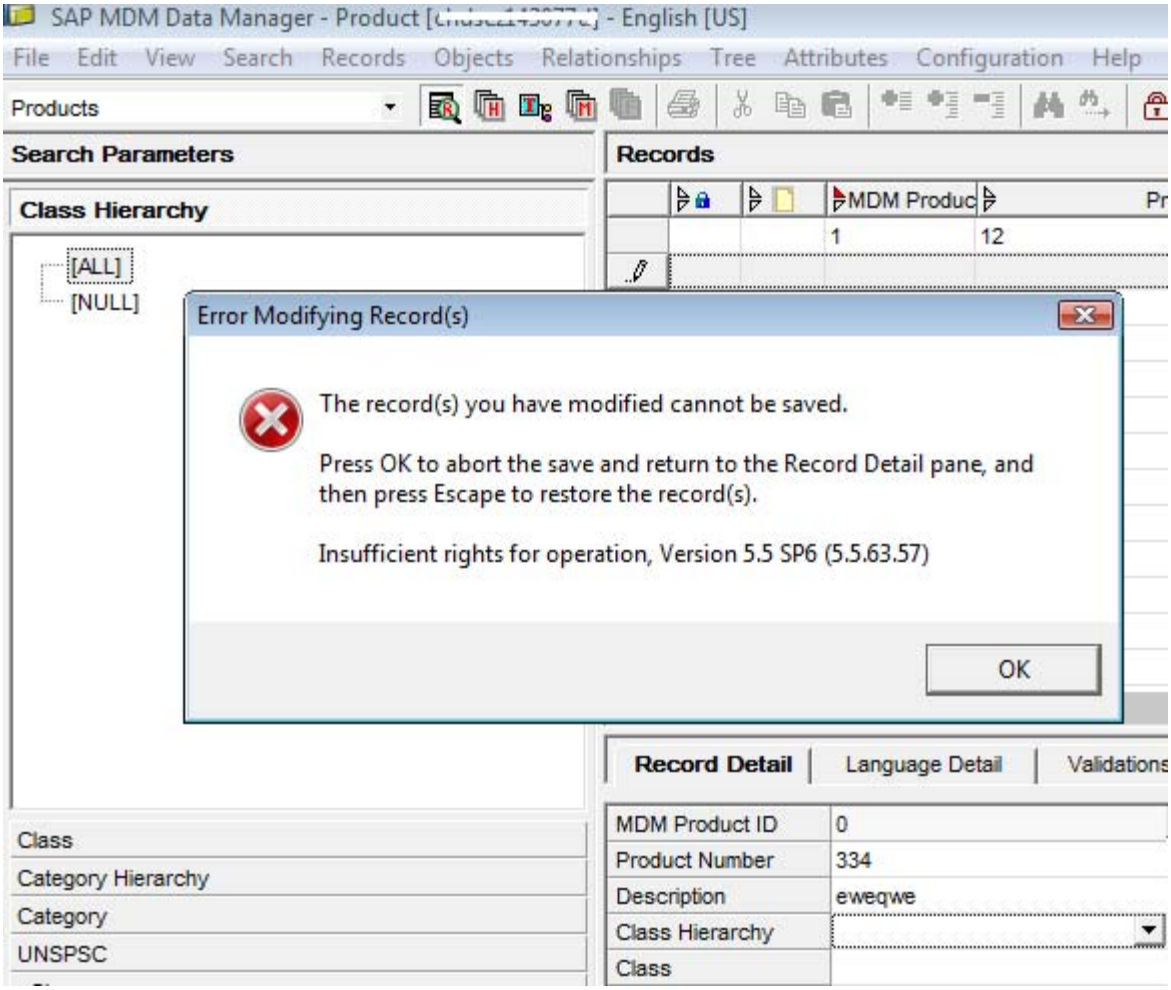
- Login to the MDM Data Manager with LDAP user to whom roles have been assigned.



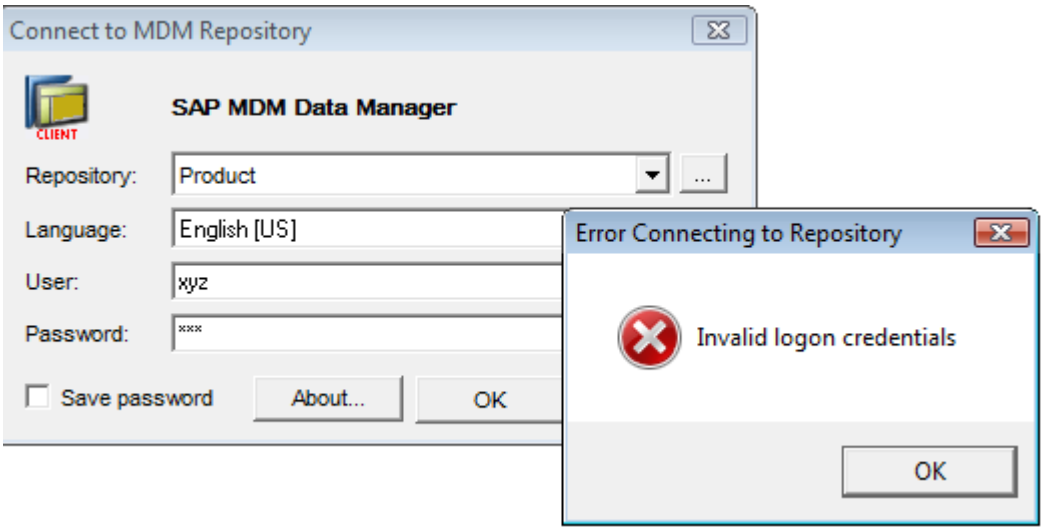
The user is able to perform operations in Data Manager according the groups he is member of (Roles in MDM).

Some Errors while Authentication through LDAP in MDM Data Manager

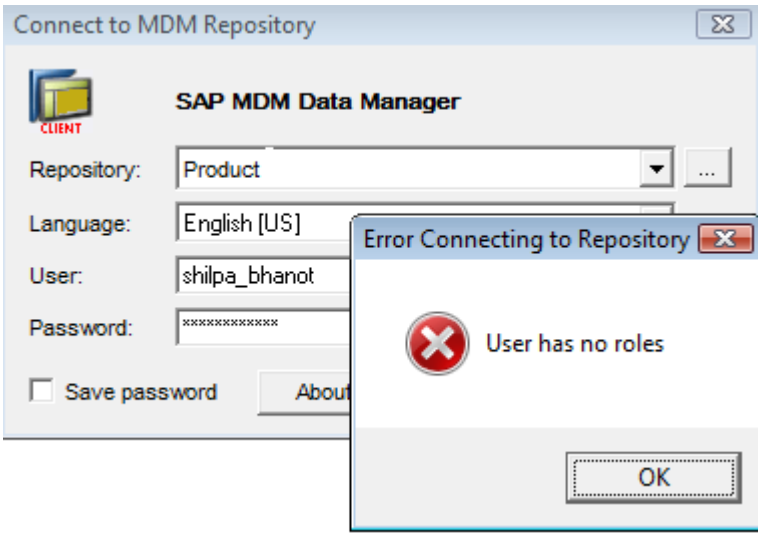
1. If the user doesn't have sufficient rights on MDM.



2. User not existing in LDAP



3. Users existing in LDAP but not having roles for MDM access



Related Content

MDM Console Reference

SAP Note – MDM LDAP with Fallback Settings

SAP Note – Check in Check Out in MDM with LDAP authentication

For more information, visit the Master Data Management homepage.

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.