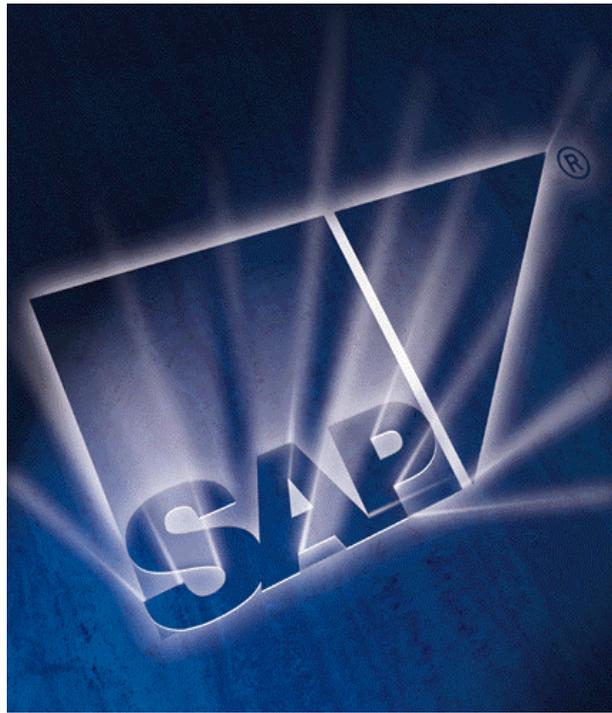


Product and Release Information

Mobile Application Repository



User Management Usage Guide

Release information

Release 4.0

Last Updated: July 2002

Copyright

No part of this document may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT®, EXCEL®, Word® and SQL Server® are registered trademarks of Microsoft Corporation.

IBM®, DB2®, OS/2®, DB2/6000®, Parallel Sysplex®, MVS/ESA®, RS/6000®, AIX®, S/390®, AS/400®, OS/390®, and OS/400® are registered trademarks of IBM Corporation.

ORACLE® is a registered trademark of ORACLE Corporation, California, USA.

INFORMIX®-OnLine for SAP is a registered trademark of Informix Software Incorporated.

UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of The Open Group.

HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Laboratory for Computer Science NE43-358, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02139.

JAVA® is a registered trademark of Sun Microsystems, Inc. , 901 San Antonio Road, Palo Alto, CA 94303 USA.

JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, SAP Logo, mySAP.com, mySAP.com Marketplace, mySAP.com Workplace, mySAP.com Business Scenarios, mySAP.com Application Hosting, WebFlow, R/2, R/3, RIVA, ABAP, SAP Business Workflow, SAP EarlyWatch, SAP ArchiveLink, BAPI, SAPPHERE, Management Cockpit, SEM, are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other products mentioned are trademarks or registered trademarks of their respective companies.

History

Version 1.0
Version 1.1

08-Mar-2002
23-July-2002

Additional Info

Use the CSN component CRM-MT-HLP to provide feedback on this document.

Conventions

This guide has the following conventions to help you understand the type of the content.

Icon conventions

Icon	Meaning
	Example
	Tip or Note
	Recommendation
	Caution
	Syntax

Typographic conventions

Icon	Meaning
<i>Interface Text</i>	Words or characters that appear on the screen. This includes system messages, field names, screen titles, pushbuttons, menu names and menu options.
User Entry	Exact user entry. These are words and characters that you enter in the system exactly as they appear in the documentation.
File name	File names, paths or directories, and screen messages.
<Variable User Entry>	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.
NAME	Name of elements in the SAP system. These include report names, program names, transaction codes, table names.
KEY	Keys on the keyboard. These include function keys, for example, F2 and the ENTER key.
Text	Text in this documentation to distinguish from the typographic conventions used in SAP documentation.

Table of Contents

1	Introduction	5
2	Purpose	6
3	Accessing the Mobile Application Repository	7
3.1	Accessing via Internal Logins	7
3.2	Accessing via MAR Profiles	7
4	Difference between current and previous versions of the User Management	10
5	User Management related functionality provided by MAS	10
6	Enabling the User Management feature in MAS.....	11
7	Working with the User Manager of MAS	12
7.1	Allowed Activities for a User with the Administrator Profile	12
7.1.1	Prerequisites	12
7.1.2	Creating a user	12
7.1.3	Changing the Password and Profile of a User	12
7.1.4	Deleting a User	12
7.1.5	Modifying the Login and Password of a Profile	12
7.2	Allowed Activities for a User with any Profile.....	14
7.2.1	Prerequisites	14
7.2.2	Modifying the own Password by a User	14
8	Frequently Asked Questions	15
9	General Recommendations	17
	Index	18

1 Introduction

SAP Mobile Application Studio (MAS) internally uses MAR (Mobile Application Repository) services for application repository support. This support:

- Allows MAS to create users to access the application repository.
- Ensures security of the application repository via controlled user access.



In the current 4.0 release, ARS (Application Repository Services) has been renamed to MAR (Mobile Application Repository) services.

MAR introduced the user management feature with the 3.0 release to provide controlled access to the application repository. This feature provides three MAR profiles to access the application repository. Each MAR user, which you create in MAS must be associated with one of these profiles. As a result, the MAR user can access the application repository only according to the rights defined for the associated profile.

In the current 4.0 release, MAR has enhanced the existing three profiles and added new profiles.

2 Purpose

The user management feature serves the following purposes:

- **Security** -- The MAR users can access the application repository in accordance to the rights defined for the MAR profiles. The passwords of these users are encrypted and cannot be seen by any user.
- **Decentralized maintenance of users** -- The MAR users are now maintained using the *User Manager* in MAS.



Prior to 3.0 release, the MAR users were maintained in the *Microsoft SQL Server* using tools like *Microsoft SQL Server Enterprise Manager*.

3 Accessing the Mobile Application Repository

3.1 Accessing via Internal Logins

MAR has defined the following internal logins to access the application repository. The user management feature uses these logins.

Login	Allows you to:
ARSAdmin	<ul style="list-style-type: none"> ▪ Perform administrative activities in the application repository. ▪ Create and modify development objects in the application repository. ▪ Modify the password of any MAR user.
ARSDeveloper	<ul style="list-style-type: none"> ▪ Create and modify development objects in the application repository. ▪ Modify your own password.
ARSUser	<ul style="list-style-type: none"> ▪ View development objects in the application repository. ▪ Modify your own password.

Besides the above three logins, MAR has defined the following logins for specific purposes:

Login	Purpose
ARSSys	MAR uses this login internally to get information on the application repository and to validate the MAR users.
ARSDb	Allows you to create a DSN for the application repository. The password for this login is arsdb .

3.2 Accessing via MAR Profiles

The access to the application repository has been defined via MAR profiles. Each profile is mapped to one of the internal logins. The available MAR profiles are listed below:



While creating MAR users, you must use these existing profiles only. You cannot create additional profiles.

MAR Profile	Mapped Internal Login	Allows you to:
Administrator	ARSAdmin	<ul style="list-style-type: none"> ▪ Perform administrative activities like creating and maintaining users. ▪ Read and write the repository specific information (ARS_SYSTABLE). ▪ Create and modify development objects in MAR. ▪ Release and revert any change list. ▪ Transfer the ownership of objects to another MAR. ▪ Create link objects to integrate screen level help with the user interface (UI) objects.

		<ul style="list-style-type: none"> ▪ Create and modify objects in the framework repository.
ROGuest	ARSUser	<ul style="list-style-type: none"> ▪ View the development objects existing in MAR. ▪ Modify your own password.
Developer	ARSDeveloper	<ul style="list-style-type: none"> ▪ Read the repository specific information (ARS_SYSTABLE). ▪ Create and modify development objects in MAR. ▪ Release the change list that has been created by you only. ▪ Modify your own password. ▪ Transfer the ownership of objects to another MAR.
SPDeveloper	ARSDeveloper	<ul style="list-style-type: none"> ▪ Read the repository specific information (ARS_SYSTABLE). ▪ Modify your own password. ▪ Create and modify development objects in MAR.  <p>This profile restricts you from releasing any change list, even if it is created by you.</p>
QMResponsible	ARSDeveloper	<ul style="list-style-type: none"> ▪ Read the repository specific information (ARS_SYSTABLE). ▪ Create and modify development objects in MAR. ▪ Modify your own password. ▪ Transfer the ownership of objects to another MAR. ▪ Release and revert any change list.  <p>This profile does not allow you to create any change list.</p>
Coordinator	ARSDeveloper	<ul style="list-style-type: none"> ▪ Read the repository specific information (ARS_SYSTABLE). ▪ Create and modify development objects in the application repository. ▪ Release and revert any change list. ▪ Modify your own password. ▪ Transfer the ownership of objects to another MAR.
Frwkuser		<ul style="list-style-type: none"> ▪ Read the repository specific information (ARS_SYSTABLE). ▪ Create and modify development objects in MAR. ▪ Release the change list you have created. ▪ Transfer the ownership of objects to another MAR.

		<ul style="list-style-type: none">▪ Create and modify objects in the framework repository.
Infodeveloper		<ul style="list-style-type: none">▪ Read the repository specific information (ARS_SYSTABLE).▪ Create and modify development objects in MAR.▪ Release the change list you have created.▪ Create link objects to integrate screen level help with the UI objects.

4 Difference between current and previous versions of the User Management

The current version of the user management in 4.0 release provides new MAR profiles in addition to the profiles existing in its previous version in 3.0 release. To find the MAR profiles available in the current version of the user management, refer to the section on [Accessing via MAR Profiles](#).

5 User Management related functionality provided by MAS

The *SAP Mobile Application Studio* (MAS) provides the following functions of the user management:

- Creation of an MAR user, which also includes assigning an MAR profile to the user.
- Modification of an MAR user, which includes changing the existing profile of the user.
- Deletion of an MAR user.
- Modification of an MAR profile, which includes modifying the login or password of a profile.



The system administrator with the **ARSAdmin** user and **Administrator** profile can carry out these activities. In the context of MAS, these MAR users will be referred as MAS users. This is because these users access the application repository via MAS.

6 Enabling the User Management feature in MAS

The following are the preliminary activities to be done by the system administrator to make the user management feature available in MAS.

1. Upgrade the *Mobile Repository Server* with the *ARS Update* of the 4.0 release.
 - This upgrade provides the [MAR profiles](#) that are available and creates two default users. The details of the default users are given below:

User Name	Password	Description
ARSAdmin	"" (empty password)	An admin user, which can be used for the initial logon to the application repository. You can change this password later.
ARSROGuest	"" (empty password)	A read-only user, which can be used to view the development objects in the application repository. You cannot change this password.

- The value for the parameter **UMFRC** in the **ARS_SYSTABLE** is set to **No**.
2. Enable the user management feature. This has to be done by changing the value of the parameter **UMFRC** to **Yes** in the **ARS_SYSTABLE**.
 3. Create a DSN for the application repository by using the repository login **arsdb**. The password for this login is **arsdb**.
 4. Logon to *SAP Mobile Application Studio* (MAS) by using the default admin user **ARSAdmin**. The password for this login is "" (empty password).
 5. Choose *Tools* → *User Manager* to invoke the *User Manager* and perform the following activities:
 - Change the password of the default admin user (recommended, though not mandatory).
 - Change the passwords of the available MAR profiles (recommended, though not mandatory).
 - Create MAR users. These users will be referred as the MAS users.

7 Working with the User Manager of MAS

The *User Manager* is an internal tool in *SAP Mobile Application Studio (MAS)*, which allows you to create and maintain users. The activities that you can perform using *User Manager* are described below. These activities are categorized according to the MAR profiles.

7.1 Allowed Activities for a User with the Administrator Profile

7.1.1 Prerequisites

Make sure that you have done the following before you perform the admin activities:

- You have enabled the user management feature in MAS. For more information refer to the section on [Enabling the User Management feature in MAS](#).
- You have logged on to MAS and chosen *Tools* → *User Manager*.

7.1.2 Creating a user

1. In the *User Manager* window, choose *Create*.
2. In the *User Account* group, enter the user name and password.



You do not have to enter the password, if you have not changed the empty password while enabling the user management feature.

3. Select a profile, which you want to assign to this user.
4. Choose *Save*.
The user that you have created appears in the users list.

7.1.3 Changing the Password and Profile of a User

1. In the *Users* grid of the *User Manager* window, select the required user.
The details of the user appear in the *User Account* group.
2. Choose *Modify*.
3. Enter a new password for the user.
4. Select a different profile from the list of profiles available.
5. Choose *Save*.

7.1.4 Deleting a User

1. In the *Users* grid of the *User Manager* window, select the required user.
The details of the user appear in the *User Account* group.
2. Choose *Delete*.
The system prompts you for the confirmation of deleting this user.
3. Choose *Yes*.

7.1.5 Modifying the Login and Password of a Profile

The login and password of a profile are the actual login and password of the application repository. If you want to modify the login and password of a profile, you have to modify them initially at the MAS level and later at the application repository level. After successfully modifying the details at MAS level, you must make the same modifications at the application repository level. This order is very important, as changing this order will not allow the corresponding users to access the application repository.



We recommend that you **do not modify the details of a profile**, unless it is very much required. This is because, if you do not perform this activity appropriately, the corresponding users cannot access the application repository.

This activity includes two mandatory sub-activities as described below:

7.1.5.1 Modifying the Login and Password of a Profile at the MAS level

1. In the *Profile* group of the *User Manager* window, select the required profile.
The login and password values appear.
2. Choose *Modify*.
3. Enter the new login and password in the corresponding fields.
4. Choose *Save*.

7.1.5.2 Modifying the Login and Password of a Profile at the Application Repository level

7.1.5.2.1 *Modifying the Password of a Profile*

1. In the *Microsoft SQL Server Enterprise Manager*, expand the *Microsoft SQL Servers* → *SQL Server Group* and locate the machine where the application repository exists.
2. Expand the <machine> node and choose *Security* → *Logins*.
3. Select the login, which corresponds to your required profile.
4. Right click and choose *Properties*.
The *SQL Server Login Properties* window appears.
5. In the *General* tab, enter the new password.



The password should be the same as the profile password that you have entered at the MAS level.

6. Confirm the password.

7.1.5.2.2 *Modifying the Login of a Profile*

1. In the *Microsoft SQL Server Enterprise Manager*, expand the *Microsoft SQL Servers* → *SQL Server Group* and locate the machine where the application repository exists.
2. Expand the <machine> node and choose *Security* → *Logins*.
3. Right click on *Logins* and choose *Delete*.
The login is deleted.



The *Microsoft SQL Server Enterprise Manager* does not allow you to modify any login. So, the alternative to modify any login is by deleting the existing login and creating a new login.

4. In the right-hand pane, right click and choose *New Login*.
The *SQL Server Login Properties* window appears.
5. In the *General* tab, enter the required values for the respective groups as given below:

Group	Required values
<i>Login</i>	New login name (Should be same as the profile login entered at the MAS level)
<i>Authentication</i>	Password for the <i>SQL Server Authentication</i> (Should be the same as the profile password entered at the MAS level)
<i>Defaults</i>	Application repository name and language

6. If the login is **ARSAdmin**, in the *Server Roles* tab, select all the server roles except **system Administrators**; otherwise continue with the following step.
7. In the *Database Access* tab, select the *Permit* field for the required application repository.
8. Select the required database roles that are listed below based on the login in the *Permit in Database role* list.



We recommend you to assign the database roles as defined in the table below:

Database Role	ARSAdmin	ARSDeveloper	ARSUser
Public	✓	✓	✓
db_owner	✓	x	x
db_accessadmin	✓	x	x
db_securityadmin	✓	x	x
db_ddladmin	✓	x	x
db_backupoperator	✓	x	x
db_datareader	✓	✓	✓
db_datawriter	✓	✓	x
db_denydatareader	x	x	x
db_denydatawriter	x	x	x

A new login is created with a new password.

7.2 Allowed Activities for a User with any Profile

The following is the only activity, which can be performed by the users with any profile besides **Administrator** profile.

7.2.1 Prerequisites

Make sure that you have done the following:

- You have enabled the user management feature in MAS. For more information refer to the section on [Enabling the User Management feature in MAS](#).
- You have logged on to MAS and chosen *Tools* → *User Manager*.

7.2.2 Modifying the own Password by a User

1. In the *Users* grid of the *User Manager* window, select the required user. The details of the user appear in the *User Account* group.
2. Choose *Modify*.
3. Enter a new password for the user.
4. Choose *Save*.

8 Frequently Asked Questions

1. How does a user with any profile can change his or her own password?

Refer to the section [Modifying the own Password by a User](#).

2. What to do if a user having a profile other than Administrator forgets his or her own password?

A user with `Administrator` profile should logon to MAS and reset the password of the user to blank using the *User Manager*. Later, the respective user can change the blank password to the required password.

3. What to do if a user with Administrator profile forgets his or her own password?

Try one of the following options:

- If there is another user with `Administrator` profile, logon to MAS using that user and reset the password to blank.
- If you remember the `Administrator` profile password, logon to *Microsoft SQL Server Query Analyzer* using the corresponding login and password. Now, you locate the script `User_Management_RestoreDefaultAdminUser.sql` (from the MAS installation path under the folder *ARSUserManagement*) and execute it. This script creates the default admin user with blank password.
- If you are not able to carry out any of the above two options, you will have to execute the complete user management script `User_Management_For_ars40.sql` (can be found in the MAS installation path under the folder *ARSUserManagement*). This script deletes all users and creates only the [default logins](#) and [default profiles](#).

4. What do I need to do when I backup the application repository (with users created) and restore it on another machine (as another application repository in the system landscape)?

Logon to *Microsoft SQL Server Query Analyzer* using the `Administrator` profile and execute the script `User_Management_AfterDBRestore.sql` (can be found in the MAS installation path under the folder *ARSUserManagement*). This script will reset the:

- Password and names of all the MAR profiles to initial values.
- Password of all the users to blank.



If the login or password of a profile has been changed from its default values, the same will have to be reset to their initial values using the *Microsoft SQL Server Enterprise Manager*. Otherwise, the corresponding users cannot access the application repository. For more information, see [Modifying the Login and Password of a Profile](#).

5. Is it possible to create new profiles?

No.

6. If I want to view any entries in the ARS_SYSTABLE, which profile must I use?

You must use `ARSUser` profile.

7. If I want to modify some entries in the ARS_SYSTABLE, which profile must I use?

You must use the `Administrator` profile. In the context of MAS, the user account is `ASRAdmin`, which has this profile.

8. What should I do if I am not able to access the application repository after it has been restored using the release 4.0 backup?

Logon to *Microsoft SQL Query Analyzer* using the admin profile and execute the script *User_Management_AfterDBRestore.sql* (can be found in the MAS installation path under the folder *ARSUserManagement*). This script will reset the:

- Password and names of all the MAR profiles to their initial values.
- Passwords of all the users to blank.

9. I have successfully logged in to MAS, but I am not able to invoke User Manager via Tools → User Manager. Why?

Access the ARS_SYSTABLE using the *Administrator* profile and check whether the value set for the parameter *UMFRC* is *Yes*. If it is *No*, then change it to *Yes*.

10. As a system administrator, I have deleted one MAS user by mistake. The user has made some changes to the development objects in a change list. How to release this change list?

The change list, in which the user is working on the development objects, is still open. As the system administrator, you can login to MAS and release the change list. Else, you can create the same user account again by using the *User Manager* in MAS. Any user can login to MAS and release the change list by using this user account.

11. What is the final solution for me, if I cannot resolve the problems related to User Manager?

Re-execute the script *User_Management_For_ars40.sql* (can be found in the MAS installation path under the folder *ARSUserManagement*) only if you cannot resolve problems. This operation deletes all the MAR users and restores the default users.



If you have decided to perform this option, remember that you have to create the MAR users again using the *User Manager* in MAS.

9 General Recommendations

1. Change the password of the default admin user (**ARSAAdmin**), when you logon to MAS for the first time.
2. Change the passwords of all the profiles as per the instructions given in section [Modifying the Login and Password of a Profile](#).
3. Avoid modifying the login of any MAR profile. This is prone to errors.
4. Avoid modifying the passwords of **ARSSys** and **ARSDb**.
5. Remember the passwords of all the MAR profiles. This is required and useful if you:
 - Want to view the parameters in the ARS_SYSTABLE (if necessary) using the *Microsoft SQL Server Query Analyzer*.
 - Forget the password of the admin user.

Index

- application repository
 - access via internal logins, 7
 - access via MAR profiles, 7
 - default users, 11
 - internal logins, 7
 - MAR profiles, 7
- MAR profile
 - modify details, 12
- MAS user, 10
 - create, 12
 - delete, 12
 - modify password and profile, 12
- SAP Mobile Application Studio
 - application repository support, 5
 - user management, 10
- user management
 - enable in MAS, 11
 - purpose, 6
- user with administrator profile
 - activities allowed, 12
- user with any profile
 - activities allowed, 14