

# Managing Active Directory using visual scripting

## User Management Resource Administrator

Managing the content of Active Directory has become increasingly complex with the growing need to manage users, groups, organizational units, file access rights and privacy sensitive data more consistently. User Management Resource Administrator is a possible solution to deal with these challenges. *Jan Reinders*

### Complexity of User Account management

Most employees nowadays have access to many different applications, each with its own user account and corresponding login info. In many cases, the creation and maintenance of these user accounts requires considerable manpower. It is therefore all the more surprising that many companies still create and maintain user accounts in an informal manner. After all, any delay or errors in the creation of user accounts may result in productivity loss.

Apart from the challenge of creating new user accounts, employee data may also change: group memberships, cell phone number, home address, department, etc. These changes obviously have to be reflected in Active Directory.

Another complicating factor is that many organizations store their user data in multiple data repositories. In that case, it becomes crucial to update the data properly across the various different information systems.

In this article, we will review the possible deployment of User Management Resource Administrator, developed by Tools4ever.

### Unique software

User Management Resource Administrator (UMRA) is a unique business application, developed by Tools4ever ([www.tools4ever.nl](http://www.tools4ever.nl)). Using various different UMRA modules, we will try to perform the following:

- MASS module - mass create new users (as opposed to using the built-in Microsoft tools) ;

- Forms & Delegation module - delegating a user management task to a non-administrator (e.g. reception desk) ;
- Automation module - establishing a link with another data store containing personnel data and synchronize the databases.

But first we will take a look at the installation of UMRA and the general user interface.

### Simple installation

Installing UMRA is not very difficult. UMRA has three different modules: MASS, Forms & Delegation and Automation. For Forms & Delegation and Automation a service is installed which checks the authorization of the user and executes the command. During the install you have the option to install one or more modules, depending on your license (which is related to the number of users in your domain). There is no standard retail price for UMRA. A 30-day trial version can be downloaded to evaluate the product, without any limitations. The only exception is for MASS, with which you can only import 5 users in the trial version. See figure 2 for an overview of the UMRA architecture.

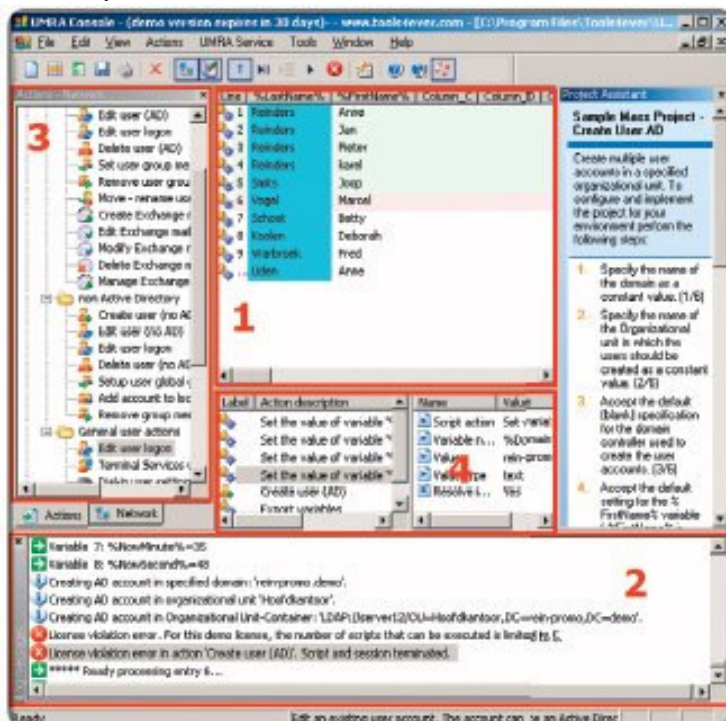


Figure 1  
Overview UMRA interface

1. Imported text file.
2. Import result. This should not contain any errors when you switch from test mode to production.
3. Script actions which can be selected.
4. Created script. In the 30-day evaluation version the import stops after 5 lines. In log pane 2 an error message appears. "Joop Smits" is the last user account which has been imported.

## Console

The console is the main user interface for the administrator. When you create a project in the console, a choice can be made between a bulk project (MASS project), a forms project (delegation project) and an Automation project. To each project, script actions can be visually added as shown in Fig. 1 (item 4). The 'Create User' example shown in Fig. 1 not only creates the user "Reinders" in a specific OU, but also conditionally assigns the user to a group based on information in the .CSV file. The actions can easily be dragged and dropped from window 3 to window 4. These script actions need to be configured by specifying the corresponding properties (e.g. name of an OU or the name of a group). This is the basic principle for all functions in UMRA. The concept of the software may be simple, but the number of actions and options is simply overwhelming which makes the software fairly complex. After a few hours of testing however, more and more options become clear: removing duplicate names, adding sequential numbers to an account, moving home directories and setting file access rights with the correct SID. The most complex scripts can be assembled in this way, for instance moving users and assigning them to another group under certain conditions. Using Wizards in the Tools

menu, scripts can be quickly drafted and fine tuned later on. To practice, several demo projects are available. Be careful when running scripts in a production environment. Make sure to use the simulation mode until you are absolutely certain that the scripts can be safely executed.

## Implementing bulk changes

With the MASS

module, thousands of users can simply and safely be added to Active Directory based on a comma separated import file containing user data (CSV file). There is no need to write (low level) scripts. Projects for both MASS and delegation projects are created with the UMRA console using visual scripts. Apart from creating users and groups based on an import file, UMRA can also check the imported data on certain criteria:

- Does a certain record field already exist? ;
- Should unique names be created? ;
- If so, in which structure?

UMRA's MASS module has been especially designed to deal with such complex issues.

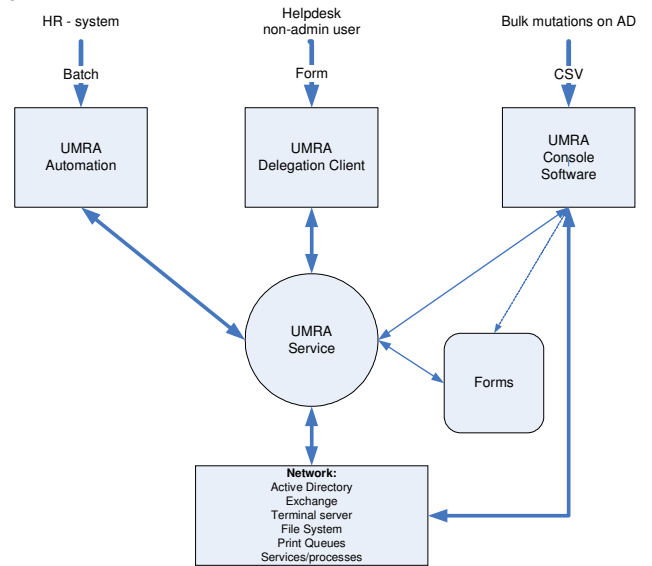


Figure 2 – Overview UMRA architecture

The application comes with many wizards and detailed Help, which makes it relatively easy to see what needs to be done. If a CSV file (containing the names of new students, for instance) is loaded into a MASS project, you first have to specify what you want to do with these data. This is done using script actions. One important action is usually the generation of the account name in Active Directory, when for example the full name Jan Janssen should become JJASN. Depending on the company policy, there are many different possibilities for generating the account name. UMRA comes with many different kinds of algorithms to solve similar problems and if necessary Tools4ever can also deliver a customized name generation solution. Once the project has been defined, it can be tested in simulation mode to check if the created script has the desired result. The result of each action can be traced in the log window. The log files contain a lot of valuable information, which is also helpful for the beginner. Errors in the procedure can easily be traced to their origin. Without the option to run a project in simulation mode, the AD content would run the risk of becoming corrupted. After all, even the most experienced

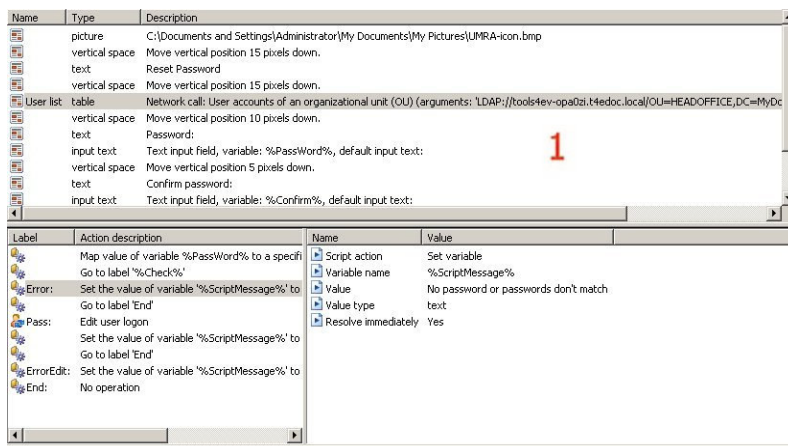


Figure 3 – Form concept

user can make a mistake which may accidentally lead to the deletion of a user. Within half an hour you will be up and running to import the content of a comma separated file into AD, which indicates that this complex application has been well designed. Both the example projects and Tools4ever's live demo are very helpful in getting the user up and running.

When an organization decides to use delegation projects as well, the (tested) MASS scripts can also be incorporated to reduce duplicate work. An UMRA MASS project can also be scheduled to be daily executed, which is especially useful for organizations dealing with frequent updates.

### Delegation and administrator access

Why does the IT department in most organizations also manage user related data such as group memberships, password, login name and home town? The answer is that administrative rights are required for tools giving access to this kind of mutations. Only systems administrators are allowed such access rights. Microsoft Active Directory does have a (native) option for delegation, allowing non-administrative users to reset passwords for instance. In practice however, this option is not very appealing. If the delegation needs to be reverted, ACL entries have to be edited which is simply too cumbersome for even the most ardent system administrator. With the Microsoft method, a user can get privileges to reset the password of all users in a specific organizational unit through delegation on an OU. Using UMRA, delegation can be performed on task level and much more elegantly. It makes it all the more surprising that this kind of functionality is not standard available on Windows Server 2003.

### UMRA forms and delegation

Delegation forms allow non-administrative users (such as helpdesk employees) to manage only a certain task (e.g. resetting a password or creating a new user). They do not get access to any other parts of Active Directory. UMRA forms is the front end application for the delegate user (Helpdesk employees and all other non-administrators who have been authorized to make certain changes in Active Directory). A delegate user could also be a personnel officer with access to UMRA forms to safely make changes in Active Directory without the need for any technical knowledge.

A delegate form project can be made part of the standard HR procedures, relieving the IT department from any non-core tasks. The delegation client software, UMRA Forms, connects to the UMRA service using a predefined TCP/IP port. UMRA has been developed as a 32 bits Windows application, but Tools4ever has announced a web interface by the end of 2005.

In the UMRA console, form projects are created in the same way as mass projects (File menu > New form). The resulting form projects can then be used by employees who have been authorized to run the form.

Somewhere in your network, the UMRA service must be running which can be realised using the console software. You can also specify the TCP/IP port which should communicate with the UMRA service (e.g. 56814). The UMRA service will be running under a newly created

account which must be a member of the domain admins group in Active Directory. In the next section we will show you how to create a simple form. The most common implementation is a form to reset passwords for users who have lost their password. Upon request, reception desk employees are allowed to issue a new password. The interface for creating form projects is similar to the one for MASS projects. Figure 3 shows the forms project with the form layout defined in window 1 (tables, buttons, input boxes, etc.) .

### Designing a form

The top window in Fig. 3 now displays the layout for a form project instead of the content of a CSV file. In the window below, the visual script can be found with the corresponding properties for each action on the right hand side. The most important form elements are tables and buttons. In a table, a selection can be made of a certain part of Active Directory. For instance, a table can be based on an LDAP query which only retrieves the users in the "Headquarters" OU Active Directory. Defining such queries is simply a matter of doubleclicking and adjusting the table properties. It is also possible to link a table to a database (e.g. MS Access, SQL server, ODBC), allowing



Figure 4 – A delegation form for resetting passwords. A user can be selected from a predefined OU.

for more complex procedures. Table data can be prepared in the correct structure before applying the changes to AD. When you finally press the (OK) button, the project script is executed. In this case it means that the selected users will receive a new password. Figure 4 shows the form as it is presented to the reception desk.

### UMRA automation

Active Directory has always been some kind of duplicate personnel database. All users are present in Active Directory, but as a rule they are primarily managed outside Active Directory in a personnel database. From an information technological point of view this is incorrect, since it results in duplicate storage. A link between the primary personnel database and Active Directory would be very helpful and UMRA Automation offers this possibility.

As soon as you have gained experience with mass imports and forms, it is quite likely that you want to automate tasks even further. An information system containing personnel data may create a .CSV file every day which you want to be processed automatically to update Active Directory. This can be realized using the UMRAConsole Command Line interface. A project can be executed as a CMD batch file and scheduled in the Windows task scheduler.

Furthermore, every application supporting the component object model (COM), such as IIS and Office, can be integrated with UMRA. The integration is established using the **umracom.dll** which is part of the AUTOMATION module. Finally, it is also possible to write scripts which are executed via the UMRA service in the network using UMRACMD.EXE. Software developers can thus fully integrate the UMRA functionality with their own environment, without having to define this functionality themselves.

### Good results

Using UMRA software we can successfully streamline the daily management of Active Directory. At first sight this application only seems suitable for larger organizations due to the steep learning curve. But even for a smaller organization it may be worthwhile to use delegated forms for repetitive tasks which will lead to a reduced IT effort for AD changes. Using UMRA also increases consistency with the option to read and write data from and to other repositories. It guarantees that changes in Active Directory are applied according to a predefined set of rules. UMRA is not an out-of-the-box solution for a complex AD problem. With consultancy from the software supplier however, you will soon achieve the desired results and in many cases the costs for AD management will be drastically reduced.

Product: [User Management Resource Administrator \(UMRA\)](#)  
Company: [Tools4ever](#)  
Website: [www.tools4ever.com](http://www.tools4ever.com)  
Price: On request

- + Considerable cost reduction feasible; updating AD content without programming
- Steep learning curve; Consultancy needed at project start