



# Solving the User Account Management Dilemma

---

*Tools4ever – User Management Resource Administrator*

White Paper — February 2007

Copyright © 2007, Tools4Ever B.V., All rights reserved. No part of the contents of this user guide may be reproduced or transmitted in any form or by any means without the written permission of Tools4Ever.

DISCLAIMER - Tools4ever will not be held responsible for the outcome or consequences resulting from your actions or usage of the informational material contained in this user guide. Responsibility for the use of any and all information contained in this user guide is strictly and solely the responsibility of that of the user.

All trademarks used are properties of their respective owners.

## Table of Contents

<b>INTRODUCTION .....</b>	<b>1</b>
<b>COMMON ISSUES .....</b>	<b>1</b>
<b>DELEGATION .....</b>	<b>2</b>
<b>AUTOMATIC USER ACCOUNT PROVISIONING .....</b>	<b>3</b>
<b>UMRA SYSTEM CONNECTORS.....</b>	<b>4</b>
<b>BULK AND MIGRATION PROCESSES.....</b>	<b>5</b>
<b>CASE STUDY – CENTRASTATE HEALTHCARE .....</b>	<b>6</b>
<b>ABOUT CENTRASTATE.....</b>	<b>7</b>
<b>ABOUT TOOLS4EVER .....</b>	<b>7</b>

## INTRODUCTION

User account management is a fascinating and ever-changing business. Most network administrators are looking for ways to simplify the management process, delegate tasks to the helpdesk or ways to automate certain jobs. In other words “Solving the User Account Management Dilemma”.

## COMMON ISSUES

### 1. User Account changes

The way an organization notifies its IT department on user account changes can be subject to changing priorities. A new user account simply has to be created in time so the need for notification has priority. However, the notifications for less immediate tasks may decay over time. While the IT department realizes a more immediate benefit from user account cleanup than the organization, how do you ensure the notifications will followed when an employee leaves the company?

### 2. Enforcing company policies

Manual processing of company policies on user account management is often not enforced. To avoid security issues and user account pollution, user accounts should be created and modified only using enforced company standards. How do you enforce company policies when multiple IT personnel are working on different parts of user account management, possibly using their own interpretation of those policies?

### 3. User Accounts throughout the network

An employee requires a user account in multiple systems using different configuration sets, which are managed by various departments. How do you keep user account information up-to-date with information from HR in Active Directory, LDAP, a helpdesk application and an address/phone book?

## The solution

Tools4ever specializes in managing user account information throughout the entire network and offers software solutions to greatly simplify user account management. Our solution “User Management Resource Administrator”, or simply UMRA, offers a wide range of solutions to the issues mentioned earlier.

UMRA is an Identity Management solution and offers Delegation, Automatic User account provisioning, deletion and migration features. UMRA clearly sets the standards for low-cost investment, quick implementation - typically in just a few days, easy maintenance and more than 50 out-of-the-box connectors to source and target information systems.

Tools4ever offers an extensive template database to cover every kind of user account management task. These include templates for organizations of all sizes: small (300-500 employees), mid-size (500-2000 employees), mid-large (2000-15000 employees), large (15000-50000 employees) and enterprise (50000+ employees), and every industry: local/state/federal government agencies, schools, colleges or universities, healthcare, financial services, manufacturing and commercial services.

## DELEGATION

Managing user accounts is a relatively easy process, but strangely enough it can get complex and cumbersome at the same time. A senior administrator has no trouble processing all steps in creating a user account, such as naming conventions, home and profile folders with permissions, group memberships, Exchange mailbox, shares, and synchronizing with other applications or systems.

The problem is that senior administrators are hard to spare and are quite expensive to spend considerable effort managing user accounts. However, you can't just simply give the job to someone with limited technical skills. So how can you have a helpdesk employee perform these tasks without assigning them too much privileges and giving them an extensive operating manual?

The solution to this problem is often found in using Active Directory's "Delegation of Control" or building scripts. However, "Delegation of Control" is complex to setup, doesn't feature an easy-to-use GUI, only delegates permissions on the AD itself thereby leaving the NTFS and other systems untouched, and it cannot enforce company policies on for instance naming conventions. Scripts or any custom developed applications are better solutions but they require considerable effort to develop and maintain, often do not cover all areas of user account management and have a complex interface.

UMRA solves all these problems with its Delegation module. By using the Delegation module, you can specify exactly the way you want to manage your user accounts. Featuring an easy drag-and-drop system, you can pinpoint every detail of the user account creation process in your network. Such a template can then be made available to a helpdesk employee by adding an electronic form to it, allowing input, selection and searches.

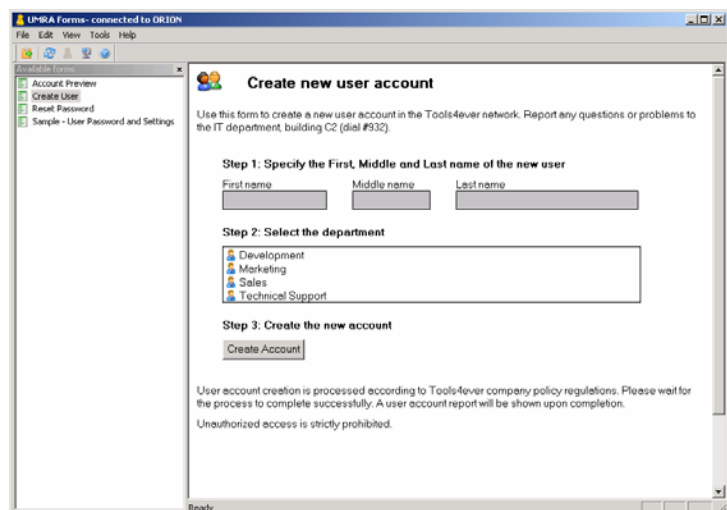
Bottom line: Using UMRA delegated employees never have direct access to sensitive parts of the network and user accounts are managed exactly as the network administrator intended.

### Deploying UMRA

**"The Tools4Ever implementation was one of the most highly valuable, cost effective solutions that I've ever implemented. We have taken the manual intervention out of the equation for many mundane AD /user tasks, such as disabling network accounts. User accounts are now disabled in real-time once terminated in Lawson. This provides us with a greater level of network security, while also assuring compliance with industry standard regulations such as HIPAA. "**

**"We opted for the consulting service for Tools4Ever to provide the initial setup. Configuration and setup was done in 2 days by a Tools4Ever consultant remotely with us providing the local knowledge of the environment."**

Mark Handerhan - IT Manager  
CentraState HealthCare



The screenshot shows a web browser window titled "UMRA Forms - connected to ORION". The main content area displays a form titled "Create new user account". The form includes a sidebar with navigation options: "Account Preview", "Create User", "Reset Password", and "Sample - User Password and Settings". The main form area has three steps: "Step 1: Specify the First, Middle and Last name of the new user" with input fields for "First name", "Middle name", and "Last name"; "Step 2: Select the department" with a list of departments including "Development", "Marketing", "Sales", and "Technical Support"; and "Step 3: Create the new account" with a "Create Account" button. At the bottom, there is a note: "User account creation is processed according to Tools4ever company policy regulations. Please wait for the process to complete successfully. A user account report will be shown upon completion. Unauthorized access is strictly prohibited."

## AUTOMATIC USER ACCOUNT PROVISIONING

One of the advanced features of UMRA is the ability to integrate user account management tasks with existing (HR) applications. This opens the possibility to synchronize user account information in the HR system with the user accounts in a (hybrid) network. This will greatly simplify the manual or delegated process of user account management and strongly reduces the overall costs.

As an example, consider an HR system that is updated when employee leaves the organization. In most cases, different departments take care of the updates in the HR system and the updates of the user account in the network directory service (Active Directory, Exchange, helpdesk application, online phone or address book, Lotus Notes, the ERP System).

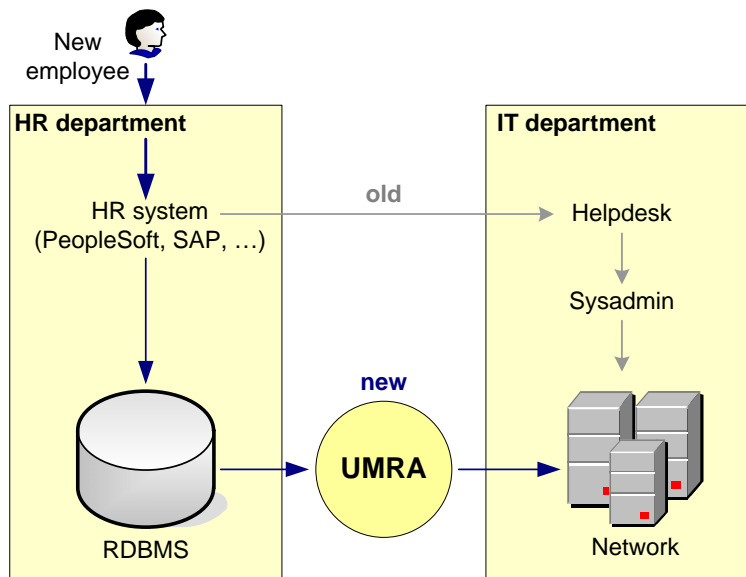
In most cases, the HR system is far better controlled when compared to the user accounts in the network. Rarely do employees receive a paycheck once they have left the company, but in many cases, their user account remains intact. With today's increasing need to control, audit and log these types of services better, it is obvious that this is not the ideal situation. A number of governmental regulations (Sarbanes Oxley, HIPAA etc.) deal with this matter and can be taken into account with UMRA.

### Choosing a Solution

**“Union County Public Schools in Western Kentucky needed a product that would; work 24/7, require very little maintenance, and be cost effective. UMRA has been all of those plus more.”**

**“UMRA imports data from our Student Information System and populates new users, their directories, and assigns rights through Active Directory, AUTOMATICALLY”**

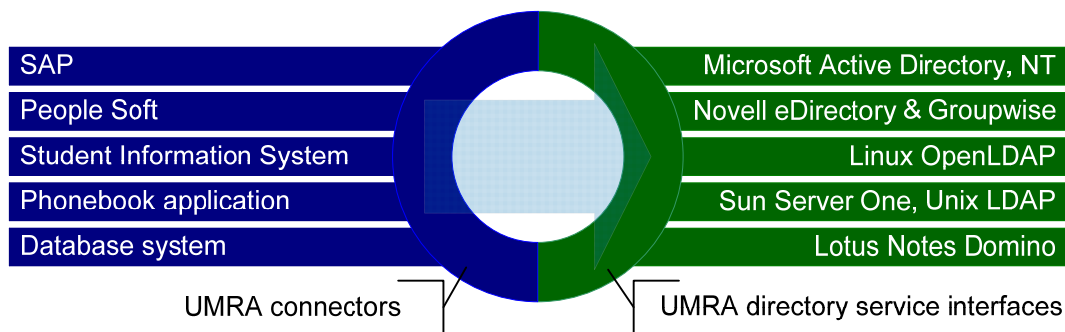
Michael Pruitt, CIO  
Union County Schools, Kentucky



## UMRA SYSTEM CONNECTORS

With UMRA, the HR system and the user accounts in the network can become integrated. Changes in the HR system can propagate automatically to the user accounts in the network. So when the HR system is updated, for example, an employee starts with the organization, UMRA detects the change and updates the user accounts in the network, creating an account in Active Directory and, where applicable, other systems as well. Conversely, when an employee leaves the organization, UMRA also detects this change and disables or deletes the account from Active Directory and other systems.

UMRA uses **Connectors** to integrate existing applications with directory services. UMRA connectors are available to integrate SAP HR, PeopleSoft, ADP and many others with Microsoft Active Directory, Novell eDirectory, Novell GroupWise, Lotus Notes Domino, Linux OpenLDAP, Sun ServerOne and other LDAP based directory services.



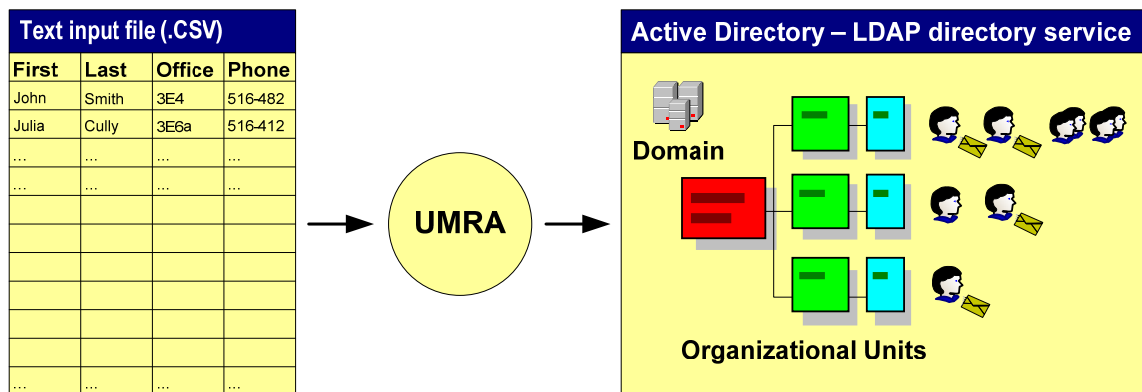
The integration of the various systems simplifies the overall procedure. With an integrated system, fewer and less skilled people are required to complete the same overall procedure. This reduces the overall costs, process execution time and number of errors.

Due to its open architecture, UMRA supports any type of integration. Also, UMRA features extensive reporting and logging capabilities. Out of the box, UMRA provides detailed **who-what-when** reports. These reports describe all the user account management operations that are executed. UMRA can export the reports in various formats and, for instance, send an e-mail every night, to update the administrator and show the latest changes that were executed.

## BULK AND MIGRATION PROCESSES

Periodically the network administrator needs to perform large scale changes on the directory, mailboxes and the file system. These changes usually are caused by 1) technical changes: OS updates or other directory services are being implemented, 2) organizational changes: takeovers, mergers, department changes, alliances or 3) security and overhead: ex-employees still have an active user account, naming convention hasn't been enforced properly, and OU structures don't match with the organization.

Without UMRA the network administrators can perform all of these operations manually or using VB scripts. Manually, the workload is enormous and errors easily occur. On the other hand, VB scripts also have enormous drawbacks: they are hard to develop and to maintain, and scripts have no built-in reporting and error handling capabilities. UMRA combines the best of both worlds: easy to use, the user has full control and built-in error handling and reporting capabilities are available. UMRA offers out-of-the box templates to support almost any kind of large scale modification on any directory object or attribute, mail boxes and/or file system.



The complexity of bulk maintenance projects varies from simple straightforward user account creation, modification and deletion, to complex conditional migration tasks.

## CASE STUDY – CENTRASTATE HEALTHCARE

**CentraState HealthCare System** recently embarked on a project to find a secure and automated method for managing user account lifecycle in Active Directory and Exchange for their employees at six locations. When the search started, CentraState IT staff was managing the process manually utilizing Microsoft Active Directory Users and Computers.

The reasons for automating the process were as follows:

- Seamlessly manage User accounts by linking with the Lawson Human Resource application for new hires and terminations and avoid manual intervention.
- A need for the account name and other relevant information in Lawson.
- Easily create Users in the proper Organizational Unit based on location and department and avoid errors.
- Create email accounts on the proper server/store based on location.
- Immediate disabling of user accounts upon termination for greater regulatory compliance.

CentraState selected the Tools4ever User Management Automation module along with professional services to complete the bi-directional link between Lawson and Active directory.

### About the Solution

As employees are hired by CentraState, their pertinent information is entered into the Lawson HR system that currently runs on an IBM *i-series* (AS 400) computer. Conversely, as employees resign, a termination date is placed in the HR system.

On a regularly scheduled basis, the User Management application starts a query to capture all employee data and begin the process of updating Active Directory. If the account already exists in AD, any updates, such as name, location or department changes are appropriately processed. If the account does not exist, it is created along with an Exchange mailbox, home directory and assigned to the appropriate Group Profiles based on job title and department. If the employee start date is in the future, the account is created but put in a disabled state until the date is reached when it is activated.

CentraState's naming requirements for both Active Directory and Exchange mailboxes were handled automatically by the application as were the iterations required, when necessary, for uniqueness. Business logic was also defined within the product to allow the automatic placement of users into the correct OU based upon their specific location and department. This location and department information is also utilized to insure mailboxes are created within the proper server and store. When an employee termination occurs, the information is processed by User Management and accounts are appropriately disabled on the date and then deleted after a specific period of time has passed.

Information that is created during the Active Directory processing, such as User Account Name and e-mail address, is fed back to the Lawson database twice a day. This is done to insure that Lawson is accurate information when anything has changed in Active Directory without requiring manual intervention.

### Advantages

Approximately 2 weeks after commencement, the entire project was implemented and operational. The reduction in time spent by the staff managing user account lifecycle was tremendous. Commenting on the project,

Mark Handerhan, IT Manager, stated, *“The Tools4ever implementation was one of the most highly valuable, cost effective solutions that I’ve ever implemented. We have taken the manual intervention out of the equation for many mundane AD /user tasks, such as disabling network accounts. User accounts are now disabled in real-time once terminated in Lawson. This provides us with a greater level of network security, while also assuring compliance with industry standard regulations such as HIPAA.”*

In summary, the IT staff at CentraState can spend more time on mission critical support and planning while eliminating the requirements to spend time on routine user account tasks.

## ABOUT CENTRASTATE

**CentraState Healthcare System** is a non-profit community health organization consisting of an acute-care hospital, three senior living centers, a health education and activities center, a family medicine residency program, and a charitable foundation. It is a member of the Robert Wood Johnson Health Network and a clinical research affiliate of The Cancer Institute of New Jersey.

## ABOUT TOOLS4EVER

**Tools4ever** is a leading provider of scalable productivity solutions for the Windows system administrator with the main focus on User Provisioning and Life Cycle management, Identity Management, Active Directory management and employee self service. For additional information, please visit our website: [www.tools4ever.com](http://www.tools4ever.com) , email us at [uksales@tools4ever.com](mailto:uksales@tools4ever.com) or call on 01452 384 870.