Effective Ways to Manage User Life Cycle in Active Directory

by

Derek Melber, Group Policy and Active Directory MVP

ManageEngine ADSolutions Technical Evangelist

What's this whitepaper about?

Although Active Directory is a powerful and popular directory service, there are significant gaps between its user management features and administrators' needs, much of which could be owed to its lack of built-in functionality for common tasks. This commercial whitepaper authored by Derek Melber, Group Policy and Active Directory MVP, illustrates how key aspects of user lifecycle management are addressed by ManageEngine tools.

About the author:

Derek is Technical Evangelist for the ADSolutions team at ManageEngine. As one of only 12 Microsoft Group Policy MVPs in the world, Derek is sought after for his knowledge, insight, and keen understanding of the Windows product line. Derek writes for, speaks to, and educates thousands of IT professionals all around the world every year. You can reach Derek at derek@zohocorp.com.

Provisioning, Managing, and De-provisioning User Accounts Through a Life Cycle

Every organization has to deal with employee turnover. “People come and people go” as they say. Along with the turnover, the user accounts for all of those employees must also be managed. When employees are hired, new user accounts must be created. On the other end, when employees leave the organization, their user accounts must be disabled and eventually deleted.

When a single user is hired or leaves the company, those tasks seem minor and quite simple. And they are. But what about an organization with an employee population of 5,000 to 10,000 or 100,000 – or more? Now, the turnover is not just one employee at a time. It’s more like hundreds of employees at a time.

The management of user accounts must also coincide with the management of groups, computers, domain controllers, services, security, applications, files, and everything else that must be managed on a typical corporate network. Managing user accounts through the life of the account can be both taxing and unrelenting. However, some solutions manage users from creation, through changes over their employment, to removal when the user account is no longer needed. Such systems reassure administrators that all user accounts will be correctly managed and the daily tasks of user life cycle management will be addressed.

User Account Life Cycle Overview

All administrators are fully aware of what it takes to take a user account from inception to elimination. What most administrators aren’t fully aware of is the user account life cycle management procedure as a whole. Figure 1 illustrates what is required to manage a user account from the time it is created to the time it must be deleted from the system. Each stage has many moving parts and details that can get lost in daily activities, and that makes it vital to investigate a solution that will help take users from one stage to the next.

Figure 1. User account life cycle.

What Microsoft Active Directory Solutions Provide for User Life Cycle Management

Everyone that has Active Directory is aware of the tools that Microsoft provides with the solution such as Active Directory Users and Computers, Active Directory Domains and Trusts, and tools that manage DNS, DHCP, and other network services. Microsoft even offers tools that are not 100% Active Directory related, such as System Center and PowerShell, which can be leveraged to help manage the Active Directory environment.

What about user account management? What does Microsoft provide to the administrator to manage user accounts from creation through deletion? Let's look at each key area of user account life cycle management to determine what Microsoft provides to help with the process.

Creating User Accounts

Microsoft provides Active Directory Users and Computers as the main tool for managing user accounts. The tool is designed to be a single view of a single domain, so you can see how the users are organized within the organizational units. When it comes to single user creation, Active Directory Users and Computers gets the job done – but not as seamlessly as most administrators would like.

Due to the structure of the schema and the limitations of the user creation wizard, only a few of the most basic (and necessary) properties can be established during the creation of a user account. These properties can be seen in Figures 2 and 3, which show the options available during the creation of a user account using Active Directory Users and Computers.

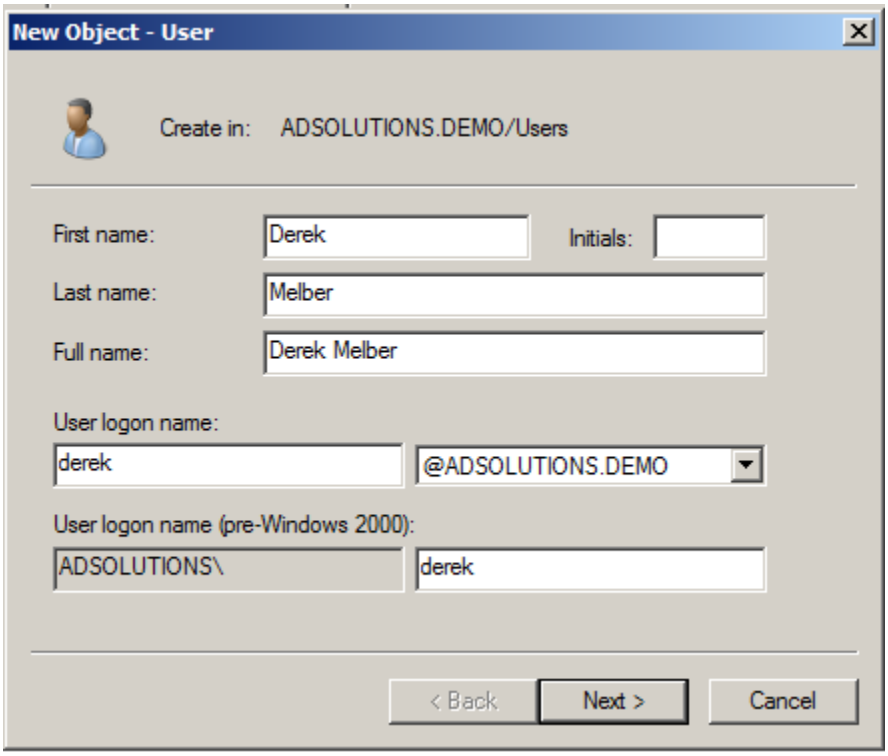

Figure 2. Basic properties that need to be established while creating a user

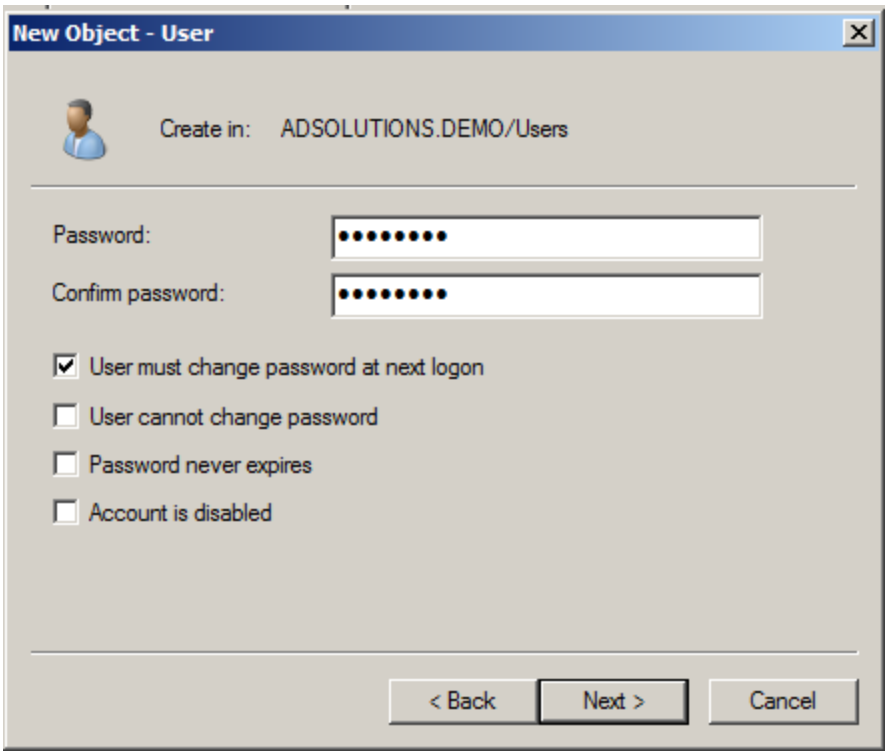

Figure 3.

All of the other properties for the user account must be configured “after” the user is created. This might not seem like a limitation, but it is when you have to create multiple users. The iterations of creating users and only then to have to edit each user to configure the properties can be time consuming.

When it comes to creating users in bulk, using Active Directory Users and Computers is just not an option.

But let’s say an HR rep hands you a CSV file containing the latest batch of new employees. Does Microsoft provide any tools that can take this list of employees and make user accounts for them? Technically, the answer is “yes” – but with great caveats.

The longstanding tool, CSVDE, can take a CSV file containing employee names and other properties and create user accounts from it. The caveats? CSVDE offers no GUI, no confirmations of success, and no mechanism to identify failures or explain their cause. Another tool, PowerShell, can also create users in bulk. This tool has the same limitations as CSVDE.

Finally, what does Microsoft provide the administrator who wants to create users using a template? Very little. For a single user, you can select an existing user account and “copy” it to create another single user account that will have the same group memberships as the copied user account. When it comes to bulk user creation templates, Microsoft has nothing to offer.

In the end, Microsoft tools only offer a partial solution that confines you to creating single users, one at a time. Bulk user creation, using either CSV files or templates, just can’t be done efficiently using Microsoft tools.

Managing User Accounts

One of the more complex aspects of user account life cycle management is modifying user account properties to reflect changes in the user's job, role, responsibilities, and access privileges. Group membership is simple at first glance but becomes complex as soon as group nesting, local groups, and access control list inclusion are involved. Keeping a tight rein on group membership is vital to the overall security of your Active Directory enterprise and asset management.

Another key user account management issue is ensuring the correct location of each user account within the Active Directory structure. Incorrect placement of a user account in an organizational unit could lock down the user and render him or her unproductive. Incorrect placement could also loosen up security and give the user access to assets he or she should not be able to access.

Unfortunately, Microsoft provides no tools to help manage user accounts during the life of the account. When employees' roles, jobs, responsibilities, and access privileges change, Microsoft has nothing to help ensure the correct group membership or organizational unit location is correct. These corrections also include the properties related to a user account, which cannot be managed or altered based on an employee status.

While a tool like PowerShell or VBScript could be used to perform such tasks, but those tools don't come with these features by default. Someone would need to customize these tools to perform these management tasks. Even if successful, you still wouldn't have a GUI or any reporting associated with the management to inform you of any issues that might arise during the management of the user accounts.

De-provisioning of User Accounts

When an employee leaves the company, good security protocol is to immediately eliminate the user account associated with the employee. This is often accomplished by disabling the user account and moving the user account to an organizational unit where it is locked down through group policy, which is controlling all of the user accounts in the organizational unit.

For these scenarios, Microsoft tools do not provide any management of user accounts at this level. The Microsoft tools are geared towards initial creation, manual management, and manual control of the user account upon the employee's departure from the company.

What ManageEngine ADManager Plus Provides for User Life Cycle Management

For any corporation or administrator charged with managing Active Directory, ADManager Plus provides easy user account management, automated user account management, provisioning, de-provisioning, and user account recovery. Any tool that goes beyond the Microsoft tools should be extremely easy to use, perform all of the actions in an area that you are addressing, and provide an immediate return to your company. ADManager Plus meets all of those requirements and more.

Creating User Accounts

The creation of a single user or even bulk users should be a streamlined, efficient, and easy process. ADManager Plus provides a simple-to-use interface for both single user and bulk user account creation. The Microsoft solution to creating user accounts relies heavily on the Active Directory schema and the mandatory attributes of the user object. That reliance is a downfall of the Microsoft solution and one that ADManager Plus avoids.

When creating a single user or bulk users, ADManager Plus gives you the opportunity to configure all of the user attributes, eliminating the need to iterate back and forth, per user, to configure all of the user properties. Figure 4 illustrates the breadth of the user object properties that can be configured at user account creation.

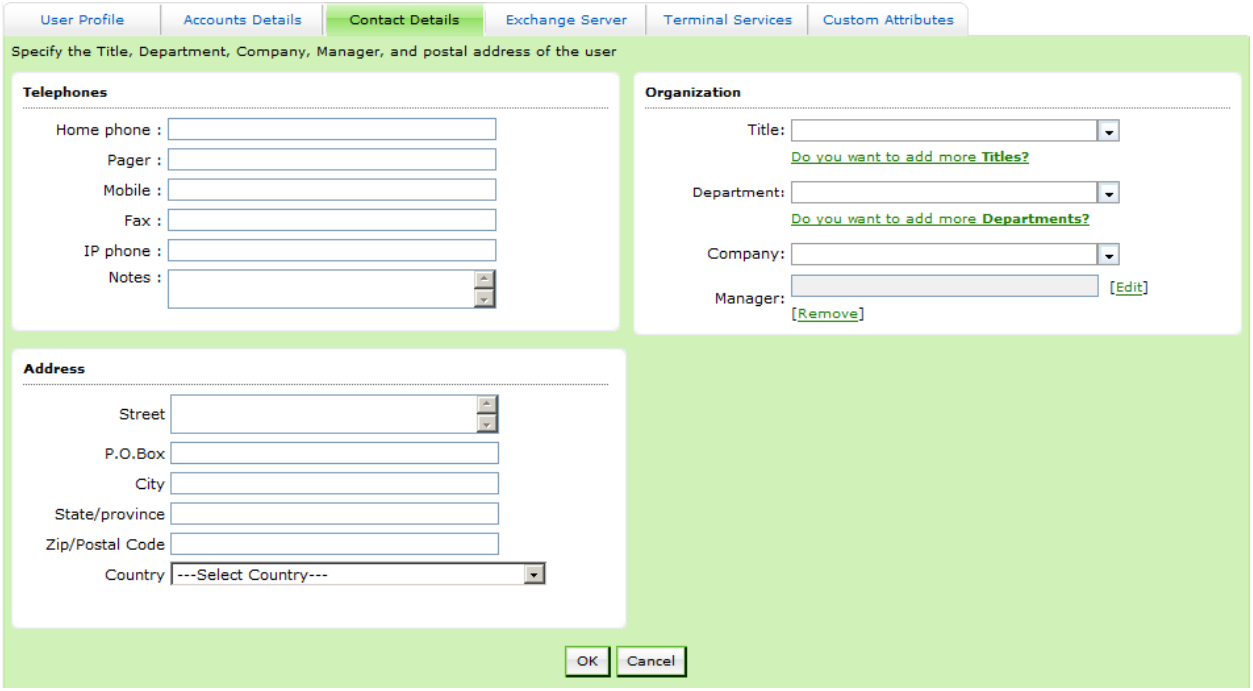

Figure 4. All user account properties can be configured during creation.

A more complete list of user profile properties that are configurable at user creation include:

- First name, last name, initials
- Logon names
- Display name
- Employee ID
- Office information
- Logon script
- User profile path
- Delegations
- Group memberships
- Account expirations
- Telephones, addresses, organization info
- Exchange server details
- Terminal server details
- Custom attributes

If multiple users need to be created, they it will often be created through a CSV file provided by HR or some other entity. ADManager Plus consumes CSV files with ease. Before generating the user accounts, ADManager Plus gives the administrator a summary of the user accounts that will be created and all of

the properties that the CSV file includes. This information enables a more efficient method of creating user accounts, as there will be fewer errors and failures during the user creation process. Simply import the CSV file into ADManager Plus, so you can review the contents before the user accounts are created as shown in Figure 5.

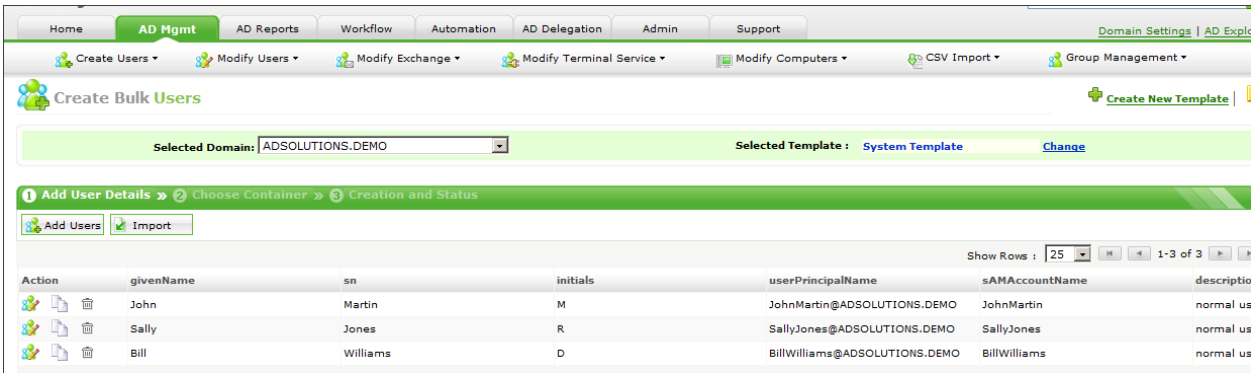

Figure 5. Importing CSV files is easy and provides for quick review for errors.

Each row contains approximately 20 properties in this example, which can all be seen by scrolling across the table output. This allows for verification before the next step, which is to define which container the user accounts will be created in. This is a key aspect of the user account creation (single or bulk) as moving objects after creation can be difficult and can cause incorrect configurations if the objects are not located properly. The selection of the container is easy to make as a view of the Active Directory structure is presented, allowing you to choose the container as you can see in Figure 6.

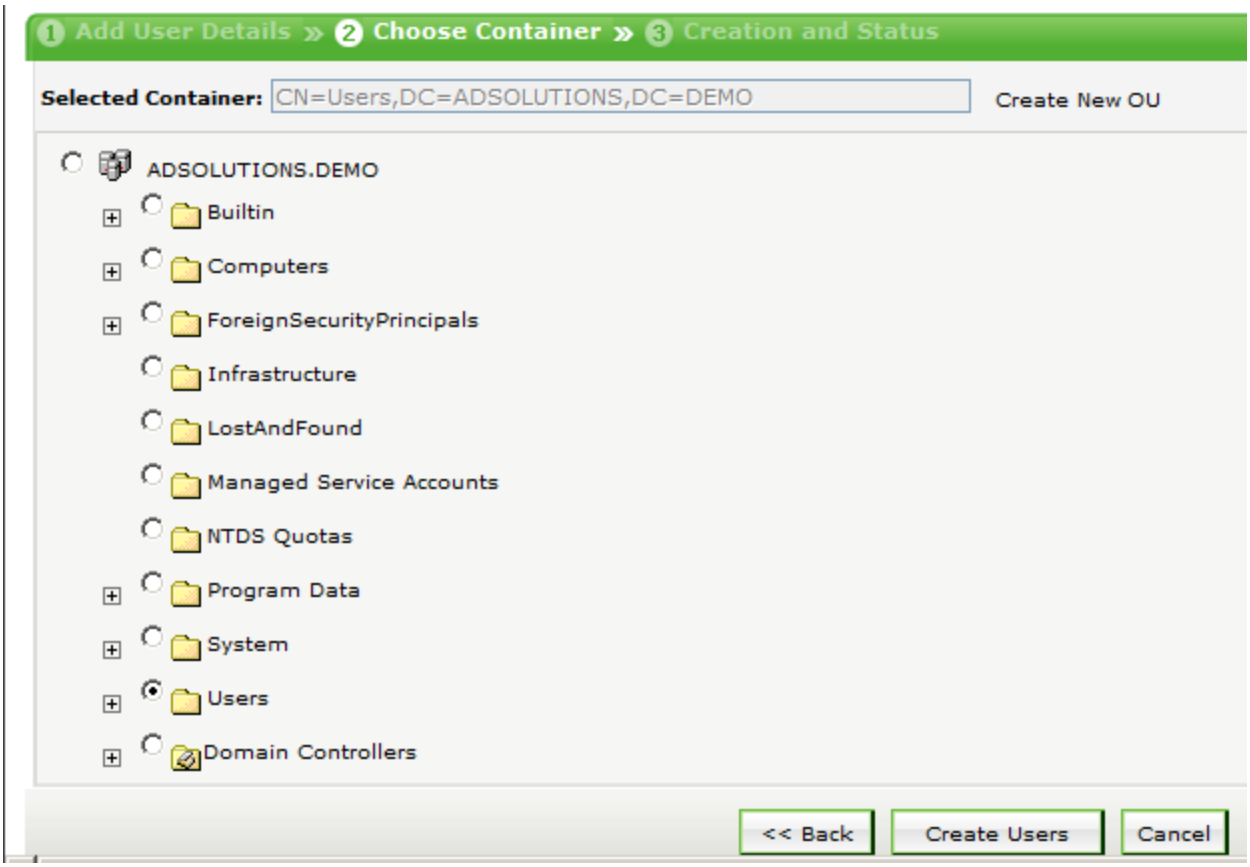

Figure 6. During user account creation, user accounts are located in the correct AD container.

As you can see above, the creation of bulk user accounts using ADManager Plus is easy and efficient. And if you were to use the user template option, you could use wildcards and variables to generate the majority of the user properties, eliminating the need to have those fields in the CSV file or to fill out in the user creation GUI as seen in Figure 7.

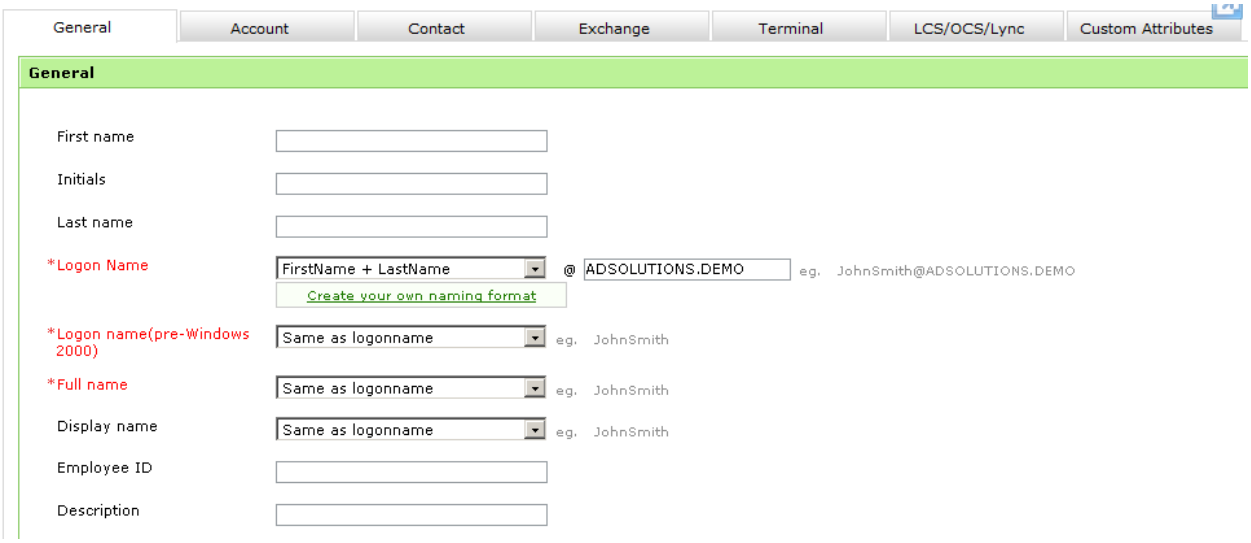

Figure 7. Templates allow for variables and wildcards for quick and efficient user account creation.

Managing User Accounts

Often, a user will move from one stage to another in his or her career. For instance, an intern becomes a full-time employee, a full-time employee becomes a contractor, a student advances from 1st grade to 2nd grade, or many other scenarios. In such situations, the user account must be modified to meet the new employee responsibilities, access demands, and other environment requirements. Without some reminder or existing workflow process, the administrator will need to remember to perform these actions on the date of the change to the employee. This work often will fall through the cracks, and the administrator will either forget to perform the action, or if many user accounts are affected, one or more user accounts will not be configured correctly.

Instead of having a human responsible for such configurations, it is better to have a computer perform the action on the required day. Building in an automated schedule for how user accounts will be managed is extremely easy to do with ADManager Plus. As Figure 8 shows, you can create one or more actions that will be performed on the user account as the user account ages and as milestones are hit.

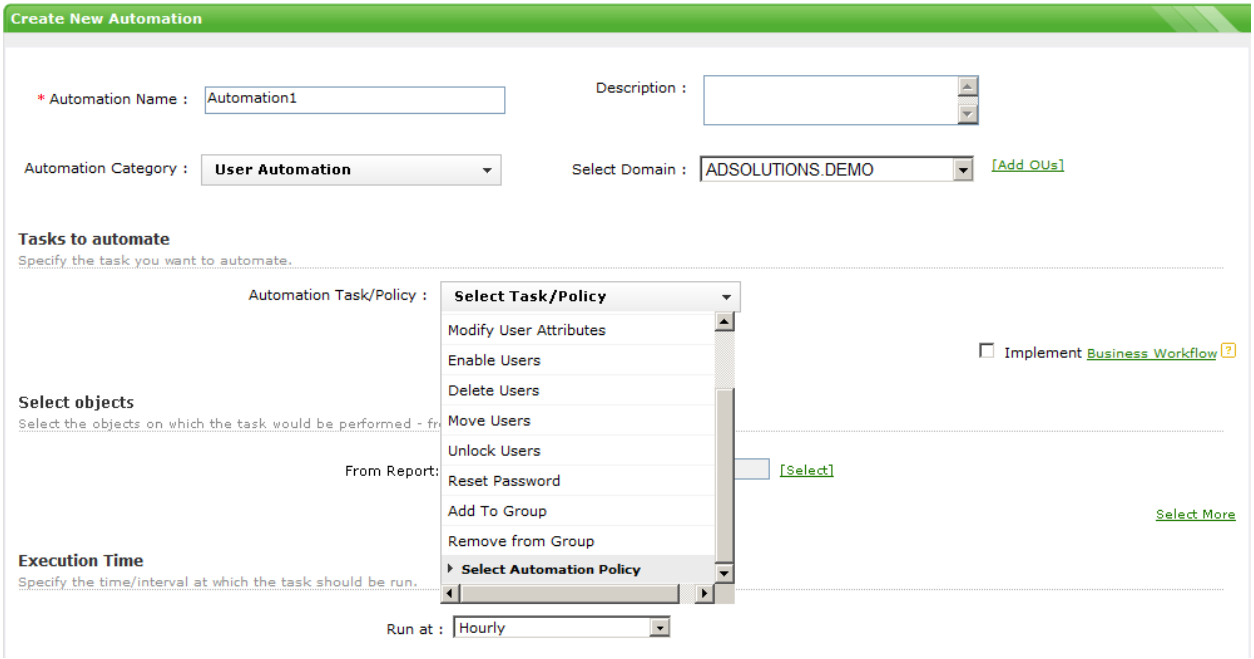

Figure 8. Automation policies automatically perform actions to user accounts.

Now, you are able to create an elaborate or simple set of rules that will apply to specific user accounts. The rules will have a schedule associated with them, which automatically performs the actions, so you don't need to remember to perform the action. This will create a stable, secure, and compliant environment for all user accounts.

De-Provisioning User Accounts

In a similar fashion to managing a user account when the employee changes roles and responsibilities, user accounts need to be de-provisioned upon certain milestones. There are at least two scenarios in which user de-provisioning is viable. The first is when you know that a user account needs to be disabled, based on the employee contract or other factors related to the user. This could be the last step in the automated management of the user account in the section above.

Another scenario is when an employee is separated from the organization and his or her account is disabled. Upon disabling the user account, the automated rule could place the user account into a different organizational unit. This would help keep the user account secured and locked down. Then, another rule in the automation policy could delete the user account after a certain period of time, per the corporate policy. That automation policy would look like Figure 9 in ADManager Plus.

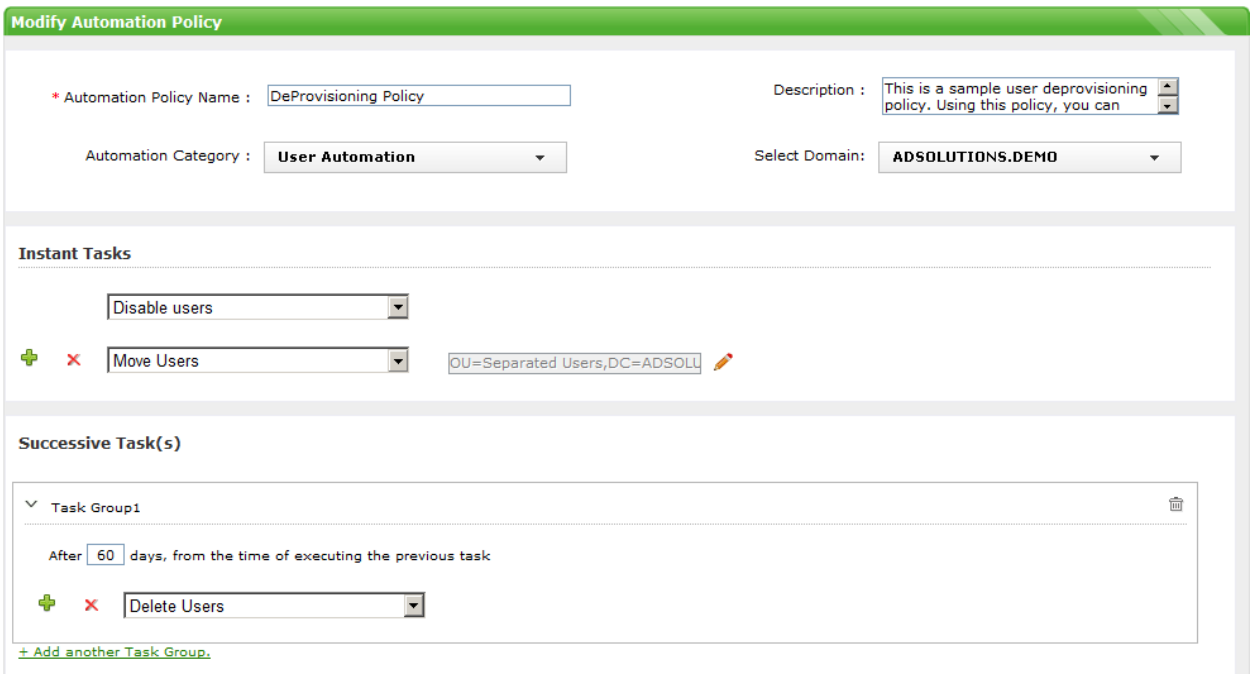

Figure 9. De-provisioning of user accounts is automatic to ensure security of the enterprise.

With ADManager Plus, user accounts will no longer be orphaned, left enabled after separation, or retained in the Active Directory after the corporate policy's purge time frame.

Summary

User account life cycle management is simple upon first glance, but the details and requirements for the creation, management, and de-provisioning of user accounts can be complex. The Microsoft tools are far from complete when it comes to user account life cycle management. In turn, administrators must perform more actions to complete mundane tasks or develop scripts to manage users as they move through their life cycle.

ADManager Plus from ManageEngine solves those issues quickly, efficiently, and cost effectively. The tool is designed for every aspect of life cycle management for user accounts, as well as for other Active Directory objects. With its easy-to-use GUI configurations and its reporting and error information, ADManager Plus will make your user account management simple in the future.