

Working 24/7 so you don't have to!

## Increase Your Security - Keep Hackers Out!

joBot, AD Robot is an innovative, time-saving application for Active Directory that provides streamlined maintenance and reporting on targeted AD objects. joBot is easy to install and use, and as a Windows service, is always on - working 24/7 - so you don't have to. joBot's client/agent platform can be installed on any number of workstations or servers within your forest. joBot helps administrators stay on top of Active Directory by automating alerts and reports on critical AD object properties. Automatic reporting allows you to spend less time tracking AD objects, and more time on demanding IT tasks.

Choose the functionality you want, when and where you need it, using the specific modules that meet your needs

- Generate customized reports and emails that report on critical information
- Flexible recurrence patterns (hourly, weekly, monthly, yearly) allow you to schedule your jobs exactly when you want them to run
- Import and export reports for web-access or import them directly into Excel

### The joBot Components:

The basic jobot components (client and agent) provide framework for performing the jobs that comprise the joBot module reports and notifications. joBot ships with the **User Count Report Module** and provides an accurate count of user objects (enabled and disabled) in all containers.

Additional joBot modules are purchased individually and currently include:

- **Password Check Module**- the perfect companion to myPassword, providing proactive password solutions to Windows users and administrators.
- **Account Check Module**- solutions that enhance security by notifying administrators of potential user account issues before they occur, such as expiring or inactive accounts. Use Account Check with rDirectory or myPassword to ensure that vital user attributes are recorded in the directory.

As new modules are added to the joBot suite, users can choose those that best suit their needs, install, and configure the jobs for immediate results.

### joBot Modules:

The **User Count Report Module** is included with joBot and provides an accurate count of user objects (enabled and disabled) in all containers.

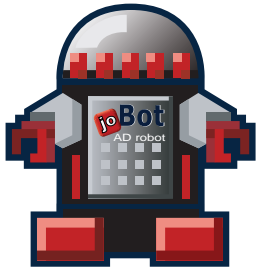
**Account Check Module** enhances security by notifying administrators of potential user account issues before they occur, such as expiring or inactive accounts. Use Account Check with rDirectory or myPassword to ensure that vital user attributes are recorded in the directory.

- **Account Expiration Notification** - The Account Expiration Notification job helps administrators save time by reporting not only on accounts that are scheduled to expire, but also on those that have already expired.
- **Account Last Logon Report** - The date and time a user last logged onto their account is typically hard to generate because the information is not replicated. joBot contacts each domain controller to verify the last time a user logged in, and reports on the latest value.
- **Accounts Without Manager Report** - This report allows administrators to view the user accounts whose Manager attribute is empty. Assigning a manager to a user assists administrators by allowing them to delegate certain tasks to managers; for example the ability to reset the password of a direct report or edit the job description for a position within the department.
- **Dial-In Status Report** - It is important to ensure that users who are permitted remote access via dial-in or VPN are current on all updates and anti-virus software. The Dial-In Status Report



*"We purchased joBot to be proactive with password resets. As a police department we are in operation 24/7 and it is critical that users have access to their accounts after working hours and on weekends. When users cannot access their email accounts this can potentially have critical implications. With joBot, I can proactively notify users via email that their password is going to expire, prompting them to change it prior to a lock-out, which enables them uninterrupted access to critical systems, and frees up IT to focus on other initiatives."*

- Gord, IT Supervisor,  
Police Department, 6 Branches



**joBot, AD Robot, working  
24/7 so you don't have to!**

- *fast and flexible*
- *plug-and-play*
- *set-and-forget*
- *what you want*
- *when you want it*
- *how you want it*

### System Requirements:

- Microsoft .NET Framework v3.5

The joBot client and agents can be installed on any 32bit/64bit machine running any of the following platforms:

- Windows Server 2003
- Windows XP
- Windows Vista
- Windows 7

For email notification, joBot supports either:

- Exchange Server 2003 and 2007
- SMTP capable mail server



For more information contact:



11811 N. Tatum Blvd., #P153  
Phoenix, Arizona 85028 USA  
Phone: 602-667-8900 Fax: 602-840-2612  
info@namescape.com | www.namescape.com

lists which users are permitted and which are denied remote access so administrators can ensure that critical security updates are in place.

- **Disabled Account Report** - User Accounts are often retained for several reasons: pending legal action, historical data, to retain the ability to reactivate an account, or the ability to log in as a particular user and access resources associated with that user. This report provides a list of all such disabled accounts.
- **Empty Attribute Notification** - This job allows administrators to view the empty attributes of a user's account properties. Using this report in conjunction with Namescape's rDirectory or myPassword, ensures administrators that vital information is recorded in the directory.
- **Inactive Account Notification** - This report ensures security by reporting an alert on accounts that have not been accessed for a specified period of time (such as accounts that were disabled improperly or created, but never used,) allowing administrators to evaluate and/or delete accounts that are no longer required.
- **Logon Script Status Report** - This report lists those users whose accounts automatically run a script (for example; load a software update) at logon.
- **Recently Created Accounts Report** - This report provides a list of all user accounts that were created within a specified time period and can be useful for administrators and Human Resources to confirm that all new employees have been correctly added to the company roster.
- **Recently Deleted Accounts Report** - The period of time that a copy of a deleted object is retained in Active Directory is referred to as the object's Tombstone date. The Recently Deleted Accounts Report lists deleted accounts whose tombstone dates have not yet expired, allowing administrators to re-animate a user account that may have been accidentally deleted or has been re-hired.
- **Recently Locked Accounts Report** - A user's account is locked due to multiple incorrect password entries, for example; repeatedly entering the password with the CAPS LOCK on. The date and time the lockout occurred is time stamped. The Recently Locked Accounts Report lists accounts where the user logged on by waiting for the time stamp to expire, which could indicate to an administrator that someone other than the user is attempting to access the account by trying different passwords. The user now has two options for logging on (1) Call an administrator and have the account unlocked (deletes the time stamp), or (2) Attempt to logon again after a specified time period, determined by IT, elapses (time stamp preserved).

**Password Check Module** is the perfect companion to myPassword, providing proactive password solutions to Windows users and administrators.

- **Cannot Change Password Report** - This job generates a report on passwords that cannot be changed. Typically, a user is required to change their password at specified intervals (e.g., once a month, every quarter, etc.), however, certain accounts may be exempt from the policy. For example; an administrator may grant access to a specific domain account to more than one user, but does not want any of those users to have rights to change the password.
- **Fine-Grained Password Policy Report** - Beginning with Windows Server 2008, administrators can apply password policies to particular sets of users rather than setting one policy for the entire domain. This report produces a list of fine-grained password policy objects for Windows Server 2008 environments only.
- **Non-Expiring Password Report** - Although administrators may allow certain accounts to have passwords that never expire, there are risks associated with this practice. This job generates a report of these non-expiring password accounts for administrators, allowing them to validate the need for such accounts, and determine possible risk factors.
- **Recently Modified Password Notification** - This report alerts the user of the date a password was last changed or reset.
- **Password Expiration Notification** - The Password Expiration notification alerts users (at the intervals IT determines) when their password is expiring. This job is particularly valuable for organizations that do not use a password reset program. Administrators can receive reports that include both passwords that have already expired, as well as those expiring in the future.
- **Must Change Password Notification** - This job reports on users who must change their password the next time they log on. Users whose passwords are expiring can be notified via email and administrators receive a report listing all accounts that fit the criteria.