

Is your user management process getting you down?

Improving efficiency and security through automation

Relying solely on Active Directory's native tools can make the business-critical tasks of user provisioning and de-provisioning time consuming and error prone, negatively affecting productivity and security.

Even if an organisation has well defined processes for managing provisioning and de-provisioning, including authorised approvals, enforcing adherence to processes can be challenging. And if you can't demonstrate your processes are being followed or easily report on users' access privileges, compliance can be a struggle.

Organisations that want to improve the efficiency and security of user provisioning, change user and de-provisioning are increasingly considering automating these tasks. This paper looks at the key challenges that automating user provisioning can help you resolve, and outlines the user provisioning offering from leading user provisioning specialist NetIQ.

Introduction

Giving people the access they need to systems and information to do their jobs is one of the most business-critical activities of any IT department. And changing access in a timely way—when someone leaves the organisation, or changes role, or their temporary contract ends—is just as important. Maintaining a secure and productive business depends on responding quickly to user provisioning and de-provisioning requests, but accurately assigning and removing user permissions in a dynamic business environment is not a straightforward task.

If you're relying on Active Directory's native tools to manage the task, you'll know how tedious and time consuming it can be. Do you feel you lack the controls to standardise processes or securely administer Active Directory? Do you find the provisioning process is prone to human error? Maybe you struggle to grant granular permissions to users based on specific business needs? Are you confident you have the auditing and reporting capabilities to manage security and demonstrate compliance?

To drive efficiencies in user provisioning and improve the security of the Microsoft Windows environment, organisations are increasingly choosing to automate the provisioning process. By doing so, they can significantly reduce both the time and resources required to manage user provisioning, change user and de-provisioning. This can also cut down on mistakes and the need to implement and manage a more rigorous approvals process. They can also benefit from better audit trails and make achieving and demonstrating compliance easier.

Responding quickly to business requests

When people join or leave your organisation, how swiftly can you respond to requests to set up or remove user accounts? And if there's a major change—such as a reorganisation or merger—can you handle the resulting volume of provisioning and de-provisioning requests efficiently enough to meet the needs of the business?

In addition to new joiners and leavers, you'll also be dealing with employees whose roles change. If someone moves, say, from a sales role into pre-sales, how easily can you revoke their old privileges and grant new ones? Or do you tend simply to add new privileges to the old ones?

The IT staff in most organisationsare stretched to their limit with other critical projects or dealing with emergency situations. They simply don't have time to comb through the details of a user's permissions to determine if access is still relevant to their current job. Relying on people and manual process alone can result in delays, errors or neglect.

NetIQ™

Maximising the value of user management

To get the most out of automating user provisioning, you may want to consider the following questions as a first step:

* What is the trigger that instigates a provisioning request? For example, is it a ticket, a form, an email?
* How do you check that the request is coming from an authorised source? And who in your organisation is authorised to make these requests?
* What is your current process for account creation? Is there an opportunity to eliminate unnecessary steps or add critical steps before you implement automation?
* How do you currently modify an account or its attributes? Does this process need to change going forward due to new regulations or security policies?
* What would cause you to disable an account rather than delete it? Do the delete and disable processes require different approvals?

Automated user provisioning, change user and de-provisioning can save a lot of time and effort, enabling you to respond promptly and accurately to both individual and bulk requests from the business to grant, change and revoke access privileges. You can be more confident that users have the appropriate access they need to do their jobs, reducing the security risk of deliberate or inadvertent unauthorised use of systems or information—and avoiding the need to perform forensics down the line if a breach should occur.

Providing just-in-time access to systems and information

Many organisations make extensive use of temporary and contract workers who need short-term access to specific corporate resources. Equally, permanent staff who are seconded onto a special project or take over another role on a short-term basis may need access to different resources than their regular roles require.

When projects or contracts have a fixed duration, no-one can afford to wait for access. You also need to be able to assign permissions based on specific business needs. Granting granular permissions and keeping track of contract and project end dates when access needs to be revoked can be burdensome if you're doing it manually.

With an automated solution, you'll be able to grant access in time to meet contract and project start dates; and you'll have more control over the different permissions that can be assigned to temporary roles. You can also set up end dates for permissions to be revoked, cutting the risk of users retaining access rights they no longer need.

Enforcing security processes and maintaining compliance

The security of your organisation will be a key consideration of your user provisioning and de-provisioning processes. But if you're working with Active Directory's native tools alone, it can be difficult to enforce processes, which can lead to errors and non-compliance.

For example, how many users end up with more access rights than they need to perform their current job role, or administrative access that they shouldn't have? Do paper or email trails make it difficult to demonstrate that your processes are being followed; or show who requested, approved or revoked a user's access, and to which resources?

By automating user change management, you'll gain greater visibility and so minimise the number of users who have elevated or unnecessary privileges, which should in turn reduce the security risk. You'll cut down on provisioning errors and find it much easier to ensure privileges are granted and revoked in line with standards like ISO 27001 and other applicable regulations.

Demonstrating compliance becomes much more straightforward with onscreen workflows that show you have a process and that it is being followed, with controls to help prevent mistakes. You'll be able to capture and securely store an audit trail of the privileges assigned to each user that records when changes have been made and who authorised them. This makes it much simpler to produce reports for your auditors in response to questions like, "Show me what this temporary contractor did not have access to over the last 60 days".

Streamlining the provisioning process through automation

Even if you have established robust, well documented provisioning and de-provisioning processes, executing them and maintaining an audit trail are likely pain points if you rely purely on Active Directory's native tools—especially if you're administering 1,000 or more users.

An automated solution like NetIQ® Directory and Resource Administrator™ can speed up response times to requests, enable accurate granting and revoking of user permissions, improve your ability to keep to processes and demonstrate that you do and significantly reduce resources needed to handle the user maintenance workload, freeing up IT staff for other activities. At the same time you're likely to minimise the potential for errors and make it easier to avoid high numbers of users with elevated privileges.

NetIQ Directory and Resource Administrator provides an intuitive graphical interface that makes processes easy to enforce and errors and omissions less likely. An integrated solution that goes beyond traditional identity management solutions, NetIQ Directory and Resource Administrator covers processes like email account setup in addition to Active Directory administration. Its policy-based administration capabilities can help improve the security and efficiency of your Microsoft Windows environment.

With NetIQ, provisioning and de-provisioning requests can be automatically triggered by updates in your HR application or helpdesk ticketing system, and you can build in an approval phase that can't be worked around. You'll also have a comprehensive, easily accessible audit trail of permissions granted and revoked that will help you stay compliant. NetIQ Directory and Resource Administrator can also carry out automated clean-up maintenance of Active Directory, such as removing empty groups or users with expired passwords. This helps ensure that Active Directory runs smoothly and remains a secure foundation for your identity and access management programmes, at the same time as reducing the administrative workload.

If you don't have the skills in house or can't spare the time, you can engage NetIQ Professional Services to install and configure NetIQ user provisioning solutions for you. They'll align it with your processes and handle the integration of your HR application or helpdesk ticketing system with Active Directory. your distributed environment, providing detailed insight into files, directories, file shares, registry keys (on Windows), system processes, database activity (on Oracle, Microsoft, Sybase and other databases) and more. It delivers enhanced audit information to provide greater fidelity and clarity of information than native log events can provide, and recording pre- and post-change information for improved incident analysis.

Conclusion

Automating your user management will dramatically reduce the time and resources you need to dedicate to the task and cut down the volume of errors. Even an organisation with just a few hundred users will find the investment worthwhile if, for example, compliance is a major burden or the organisation handles particularly sensitive data.

NetIQ Directory and Resource Administrator will help you automate access requests and incorporate stakeholder approval in your provisioning, change management and de-provisioning processes, streamlining the lifecycle of an employee's access needs.

You'll be able to respond promptly to business requests to grant, change and revoke users' privileges, and manage short-term access requirements for contractors and project staff more easily. NetIQ Directory and Resource Administrator will also give you the control and visibility you need to enforce security; and the comprehensive audit trail and reporting capabilities that will let you both maintain and demonstrate compliance.

Austria:	+43 1 595 43 35 0	**Middle East:**	+20 2 2291 2218	NetIQ Europe Limited
Benelux:	+31 (0) 172 50 5555	**Nordics:**	+46 8 630 1700	Building 2,
Europe:	+44 (0) 1784 454 500	**South Africa:**	+27 11 700 4250	2nd Floor
France:	+33 1 46 04 10 10	**Spain:**	+34 (0) 91 151 71 11	Parkmore East Business Park
Germany:	+49 (0) 89 99351 0	**Switzerland:**	+41 (0) 43 399 2090	Galway,
Italy:	+39 02 9906 0201	**UK:**	+44 (0) 1784 454 500	Ireland