helpsystems

GUIDE *(Cybersecurity)*

IBM i User Provisioning

User provisioning is one of the most fundamental tasks performed by IBM i administrators, and perhaps the most influential if one acknowledges the breadth of its implications.

Yet within many companies, this core responsibility is not approached with the proper care and consideration. Not only do managers have to carefully design initial account configurations, they must also continuously review and correct those plans as time goes on.

Although managers might want to initially provision the same set of broad responsibilities to all users for simplicity's sake, history suggests that this approach could be problematic.

From large government organizations to small startup ventures, entities of all sizes have been burned by a scourge of data breaches and network disruptions in recent years. As a result, regulatory bodies, business executives, and consumers have taken a much keener interest in the state of IT security and compliance protocols. Clearly, one-size-fits-all strategies no longer suffice.

The good news for IBM i shops is that they are well positioned to turn this chaos into an opportunity to drive lasting, positive change. IBM i includes security controls that can be configured to minimize the risk of external attacks. Remaining vulnerabilities reside within the user community in the form of costly administrator mistakes and possibly intentional privilege escalations. While this realization may be a bit sobering, the fact that pressing threats have shifted to an area completely under managerial control should be encouraging.

By adopting a centralized, role-based IBM i user provisioning model, companies can feel more confident that they are setting themselves up for success. But responsibility does not stop at initial account creation. Managers must also have complementary tools and policies in place to continuously monitor and review the integrity of controls and the compliance of administrator behavior. This evolving system of checks and balances may take time and talent to construct, but it is perhaps the only true way to satisfy the obligations and expectations of all stakeholders in an efficient and effective manner.

Provisioning Challenges and Best Practices

1. Profile Management Drains Time

As any business professional can attest, time constraints often prevent them from following the best course of action. While cutting corners on certain tasks is acceptable and understandable, the key is understanding when "good enough" isn't really good enough. Such is the case when provisioning and reviewing the privileges afforded to IT administrators. Considering the root-level access they have to an organization's technological underpinnings, responsibilities must be carefully distributed.

Tech directors now have to take a more granular view of profile provisioning. However, even for the smallest shops, creating accounts from scratch and reviewing them on an individual basis is rarely feasible—or effective. Between these two ends of the spectrum, companies can find an intelligent solution in template-based profile management.

By dividing users into distinct, role-based groups from the start, a number of important opportunities arise:

- Separation of duties becomes crystalized
- Managers establish consistency for future on-boarding
- Updates can be made and pushed out to users en masse

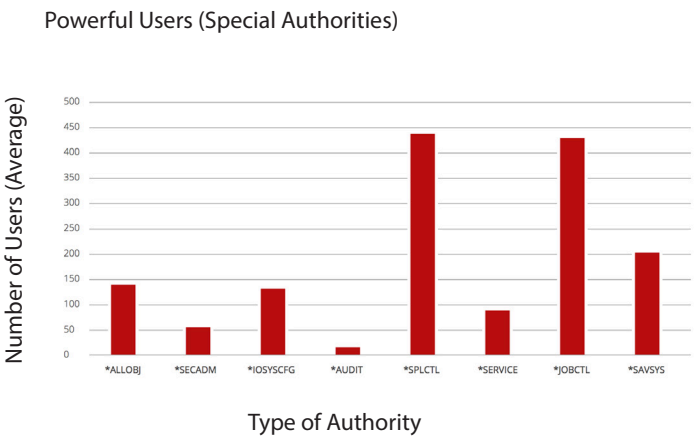
2. Users Hold Too Much Power

Even with template-based provisioning, managers cannot realistically expect to get everything right the first time. Indeed, simply assuming that initial configurations will automatically align with future objectives is both dangerous and prone to failure.

One of the most common occurrences that appear on the risk management radar is the case of users gaining or maintaining more authority than they truly need. This circumstance is often the consequence of overly permissive initial provisioning.

To conserve both time and sanity, overtaxed IT managers effectively give their colleagues the entire key chain as opposed to the select few that match the locks of their assigned duties.

According to the latest State of IBM i Security Study, the average participating organization had over 400 active profiles with job management capabilities (*JOBCTL). More concerning is that the average firm had more than 400 profiles with complete control of spooled files (*SPLCTL) and nearly 150 with the ability to access, modify, or delete any object on the system (*ALLOBJ).



By giving open and distributed access to such serious controls, managers make it harder on themselves and invite future problems. Ideally, there should also be little to no variance in the number of accounts assigned to each privilege classification. Although some overlap is unavoidable, no one individual should be afforded unrestricted access to everything. Ultimately, security should be highly correlated with the overall interdependence of team members.

This division of duties and role-based approach to privilege allocation are decisive steps on the road to faultless internal security and compliance. But this harmonious state rarely seems to last. As new people and components are welcomed into the IT ecosystem, managers must routinely review their state of affairs. Auditing profile settings against previously established templates will help identify dangerous discrepancies quickly, providing network administrators with plenty of time to intervene and correct course before irreversible oversights are made and security and compliance records are compromised.

3. Privileges are Still Being Abused

Establishing a firm foundation with templates and auditing visibility puts you ahead of the curve when it comes to satisfying internal and external risk management objectives. But the job does not stop there.

Although managers have set up smart, safe perimeters for colleagues to operate in, there is always the chance that someone will push the envelope when no one is looking.

IT managers are often reminded that personal trust and digital trust are very different concepts. From Fortune 500 companies to family-owned small businesses, hundreds of executives have stories about model employees secretly siphoning away intellectual property, spying on co-worker salary information, or selling credentials to eager cybercriminals.

At the same time, honest mistakes are made and no intrusion detection system can guarantee true 100 percent effectiveness. Whatever the case, the embittered feelings upon discovery pale in comparison to the security and compliance fallout. As a result, managers must employ a healthy sense of skepticism and keep contingency measures in place to guard against and mitigate threats.

"Comprehensive monitoring solutions allow administrators to confirm that baseline activity levels are aligned with established templates and quickly flag anomalous behavior."

In the IBM i environment, this amounts to comprehensive monitoring solutions that allow administrators to confirm that baseline activity levels are aligned with established templates and quickly flag anomalous behavior. Whether an employee improperly leverages a user profile or credentials are corrupted by an outside attacker, managers need to localize the issue before it can be properly resolved.

Power Admin Promotes Safe, Sane User Profile Management

HelpSystems is acutely aware of the challenges facing IBM i security teams and uniquely positioned to offer the appropriate solutions. As an IBM Advanced Business Partner, we are accustomed to operating in-step with IBM and working with our colleagues to identify and address issues in this rapidly evolving age of IT.

Our thought leadership is further exemplified by our privileged post as publisher of the annual State of IBM i Security Study and our seat on the Payment Card Industry Security Standards Council. More importantly, this all translates into a comprehensive user profile management tool designed to target the following areas:

Centralized User Profile Management

With the knowledge that time restrictions often lead to cut corners, Powertech Power Admin was designed to eliminate administrative roadblocks wherever possible and allow tasks to be accomplished more efficiently.

The centralized management platform eliminates the need to sign on to each individual system to create or toggle user privileges. In addition, product license information for all managed systems is stored and accessed at a single touch point.

Profile Templates

Instead of mapping out a new set of privileges with every new hire or promotion, managers can work off a pre-configured framework and make refinements as needed with Power Admin.

For example, when a new developer is onboarded, it takes seconds to ensure they are only granted access to the necessary systems and processes to complete their assigned tasks. If the employee later becomes part of the security team, that template could be swapped for one that includes the necessary system oversight privileges without dragging in the clutter of their previous profile.

> ***"Taking the time to construct templates in proper alignment with user groups is an investment that pays long-term dividends."***

Taking the time to construct templates in proper alignment with user groups is an investment that pays long-term dividends. Instead of merely saving profile managers time upfront, this enlightened approach also ensures that updates are delivered in the most efficient way possible. Change is inevitable in the IT ecosystem, whether as a result of human or technical factors.

Compliance statutes and security risk realities demand that managers stay on top of these developments. Centralizing updates not only saves managers time, it ensures any potential loopholes and liabilities are closed as quickly as possible.

Role-based Security

Profile creation, audit value modification, and data deletion are all privileged tasks and must be regarded as such. By applying security controls with direct respect to the specific roles of a certain user group, managers achieve several crucial objectives:

- Less administrative overlap
- Increased understanding over which credentials allow each task
- Streamlined process for authority swaps, updates, and changes

With fewer moving parts in the equation, monitoring controls are suddenly more powerful and anomalous behavior has less chance to slip under the radar. When a user attempts to escalate privilege rights incidentally or intentionally, the issue can be resolved in an objective manner. She either has approved access or she does not; and if the user ultimately believes those policies need to be amended, then Power Admin's event detection helps prompt productive conversations that inform managerial decisions.

Finally, these well-defined boundaries also allow administrators to demonstrate their diligence to outside observers. In today's regulatory climate, simply paying lip service to security and compliance best practices is not good enough. Instead, IT managers need to ensure that their profile management protocols are defensible in the eyes of external auditors and internal executives.

Trusted Reporting and Audit Preparation

Establishing digital paper trails is not only a business best practice; it is a legal obligation for many companies. HIPAA, SOX, PCI, GLBA and FISMA are just a few of the acronyms climbing to the top of both corporate and IT-specific agendas lately, and PowerAdmin has been designed with those standards in mind.

With a role-based security protocol in place, companies can limit access to legally covered assets such as protected health information, customer transaction data, and government contracts. PowerAdmin's reporting features confirm this due diligence with clear documentation of user profile design, settings, and historical adjustments. Management can confirm that only a handful of employees had access to administrator privileges or others were restricted to read-only access.

The software's intuitive design and centralized management view makes internal auditing a painless process, and the more frequently those exercises are conducted, the simpler it will be when outside auditors, such as QSAs, pay a visit.

Instead of approaching these sessions with trepidation, IBM i users can logically and confidently review their current risk management strategies and make note of any areas that may be open to improvements.

Concluding Thoughts

The fundamental challenge facing today's IBM i administrators tasked with user provisioning is one of complexity. One-size-fits-all approaches simply don't address emerging security realities and compliance expectations, but addressing each account on a case-by-case basis is time-consuming and error-prone.

The solution begins with a template-based approach that simplifies and centralizes managerial oversight and ensures policies and updates are globally applied in line with a role-based strategy.

In the end, IT teams benefit from the clear boundaries drawn by department directors as a culture of transparency and accountability takes hold. Management across all levels of the organization will appreciate this update as well, since it keeps the company's security and compliance reputation standing on solid, well-defended ground.

Let's Get Started

To find out how Power Admin can help you provision IBM i users, request a demo at www.helpsystems.com/demo-power-admin.

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.