Reduce IBM i Help Desk Costs with Self Service Password Reset

Increased productivity, repaired relationships, reduced security & audit risks, & lower IT costs

Contents

Executive Summary

Industry studies show it takes at least 40 minutes for Help Desk personnel to manually reset an IBM i user password, and that up to 50% of Help Desk incident tickets involve manual password resets. Manual password resets enable significant but unnoticed risks to an organization's bottom line, including:

- **Decreased productivity** – 40 minute wait times for password resets stop user and production processing, slowing down business. Off-hours processing (2nd & 3rd shifts and weekend work) can incur longer work stoppages because fewer Help Desk resources are available.
- **Damaged relationships** – Customer-facing personnel cannot service customers when their passwords are locked, risking lost business and Service Level Agreement violations.
- **Increased security risks** – Manual password resets expose critical user profiles to hacker discovery and easy-to-hack passwords.
- **Audit issues** – Manual resets can be difficult to track, causing audit and regulatory violations.
- **Overconsuming IT resources** – Additional Help Desk resources are needed just to deal with password resets, money and personnel that can be better deployed for strategic purposes.

An average IT shop that performs 2,500 manual password resets a year at $50 per reset will spend $125,000 on password resets each year.

Manual password reset risks can be significantly reduced with the new and affordable IBM i automated password reset technologies detailed in this report, resulting in the following improvements:

- Average password reset wait times can be reduced from 40 minutes to below five minutes, significantly decreasing work stoppages due to locked passwords.
- The number of Help Desk incidents involving manual password resets can be reduced by 80% or more, requiring fewer IT personnel to manage user issues.
- Help Desk resource allocation for password resets can be reduced by more than 80% or $100,000+ for an average shop.

Automated IBM i password resets lead to increased productivity, better customer relationships, reduced security exposure, improved audit and compliance results, and reduced IT costs. Organizations can take a key step forward by implementing automated IBM i password resets.

Introduction

Industry studies suggest that it takes at least 40 minutes for Help Desk personnel to manually reset an IBM i user password, and that up to 50% of Help Desk incident tickets involve manual password resets. Manual password resets impact an organization in many serious ways, exposing them to the five critical risks shown in figure 1.

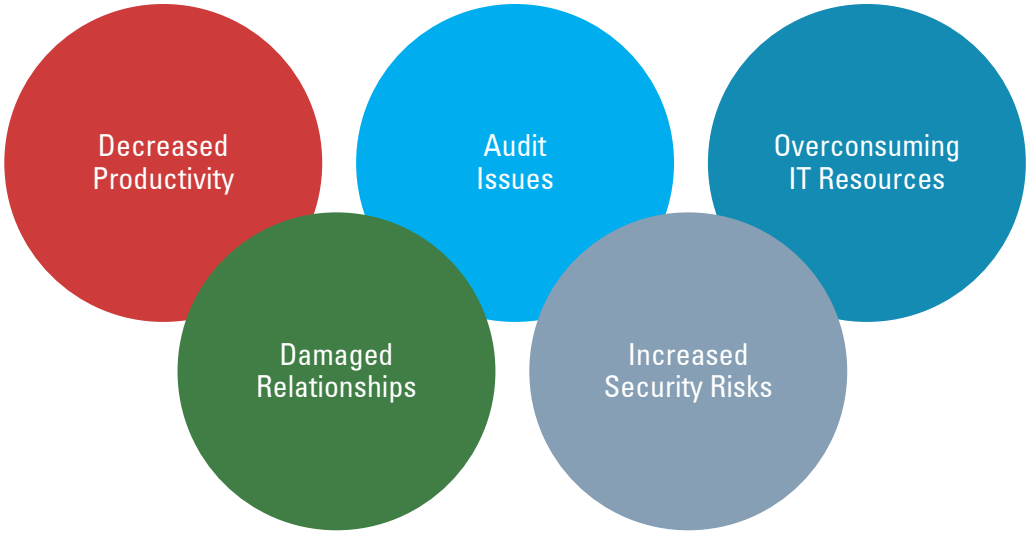


Figure 1: The five risks IBM i manual password resets expose an organization to

Until recently, nothing could be done to reduce manual password resets. Users had to contact the Help Desk when their profile was locked. Organizations had to provide extra staff for password resets, wasting time and productivity.

Today, newer technologies can automatically reset IBM i passwords or re-enable user profiles without Help Desk support.

This white paper explains the risks organizations face with manual password resets and the benefits they realize when switching to automated IBM i password reset technologies. We also explain how automated password reset technology works and the most valuable features to look for in commercial password reset software.

Reversing the Risks Involved with Manual IBM i Password Resets

Manual IBM i password resets are necessary in the following situations:

1. When a user forgets their password
2. When the operating system disables a password after several invalid sign-on attempts
3. When a user password expires

In all cases, the user must call their Help Desk to manually reset their password.

Table 1 details how the password reset risks shown in figure 1 impact an average organization.

Risk	Specific Risk	Organizational effect of each risk
Decreased productivity	• Disabled passwords create work stoppages, while affected users wait for a password reset	Customer and organizational needs are unmet Off-hours resources are needed to reset passwords for 2nd and 3rd shift, weekend, and holiday work If off-hours help is unavailable, password resets can be delayed for several hours or until the next workday
Damaged relationships	• Poor customer service • Unhappy or lost customers • SLA violations • Image problems	Customer-facing personnel unable to service customers while they wait for a password reset Delayed service results in unhappy or lost customers, and failure to meet Service Level Agreements (SLAs) Manual resets project image that the organization is using outdated technology

Risk	Specific Risk	Organizational effect of each risk
Increased security risks	• Phishing risk • Compromised passwords • Compromised security standards	Phone-in password resets make it difficult to reliably identify disabled users, providing phishing opportunities for unauthorized users to access other profiles Help Desk techs can learn user passwords, undermining password security Help Desk personnel can override password security policies and assign passwords that do not meet security standards
Create audit issues	• Incomplete records on manual password resets • Possible audit points	Manual password resets may not be recorded, producing incomplete records of the number of password resets, creating audit violations & audit points May be unable to audit when a security breach has occurred
Overconsuming IT resources	• Resource allocation costs	Additional Help Desk personnel needed just to reset passwords Inflates IT budget, redirecting money from other projects

Quantifying Manual Password Reset Risk

An average company can quantify resource allocation risk (i.e., how much Help Desk cost is devoted exclusively to password resets) by using this formula.

Resource allocation risk = Average cost per Help Desk incident * number of manual password reset incidents

To calculate an average resource allocation risk, assume that the average Help Desk incident cost is $50 and that an average Help Desk handles 2,500 manual password reset incidents per year. Using these numbers, we get an average resource risk equal to:

Average resource allocation risk = $50/incident * 2500 incidents = $125,000

This number approximates an organization's annual spending on manually resetting IBM i passwords. It can be used to cost justify an automated password reset system.

Most companies can calculate their resource allocation risk by plugging their own numbers into this equation.

How Automatic IBM i Password Resets Reverse Risk

Because they eliminate Help Desk intervention, automated IBM i password resets reverse the risks involved with manual resets.

Enabling automated password reset techniques mitigate the five critical password reset risks in these significant ways.

Increasing productivity

- User reset their passwords without contacting the Help Desk, minimizing lost work time
- 2nd and 3rd shift, weekend, and holiday work is no longer threatened. Automated resets are available 24x7x365.

Protecting relationships

- Minimal time needed for customer-facing personnel to reset passwords; enabling locked password users to quickly get back to servicing customers
- Eliminates password-related customer service delays; helping keep customers happy and protecting required SLAs
- Organization offers automated password reset service in line with industry standards for Web & mobile sites; eliminating perception of using outdated technology

Reducing security risks

- Two-factor authentication significantly reduces chances of phishing
- Majority of password resets become automatic, without manual intervention
- Avoids the risk of the Help Desk learning user passwords
- Forces all password changes to be enforced by organizational security standards

Eliminating audit issues

- All automated password changes are recorded and can be reported to auditors or other personnel
- Audit violations and audit points eliminated

Reducing IT resource consumption

- Help Desk personnel who perform low-level manual password resets can be retrained and reassigned to higher level work or other jobs

Changing password reset metrics

With automated password resets, organizations can expect the following changes.

- Average password reset wait time will drop from 40 minutes to under 5 minutes. Password changes quickly occur with automated password resets. The average password reset wait time for off-hours work (2nd & 3rd shifts and weekends) will significantly improve, and organizations may be able to redeploy off-hours resources that are dedicated to password resets.

- Percentage of password reset Help Desk incidents will drop from up to 50% of all incidents to less than 10% of all incidents (an 80+% reduction). With automated password resets, there will be less demand on the Help Desk to change passwords.

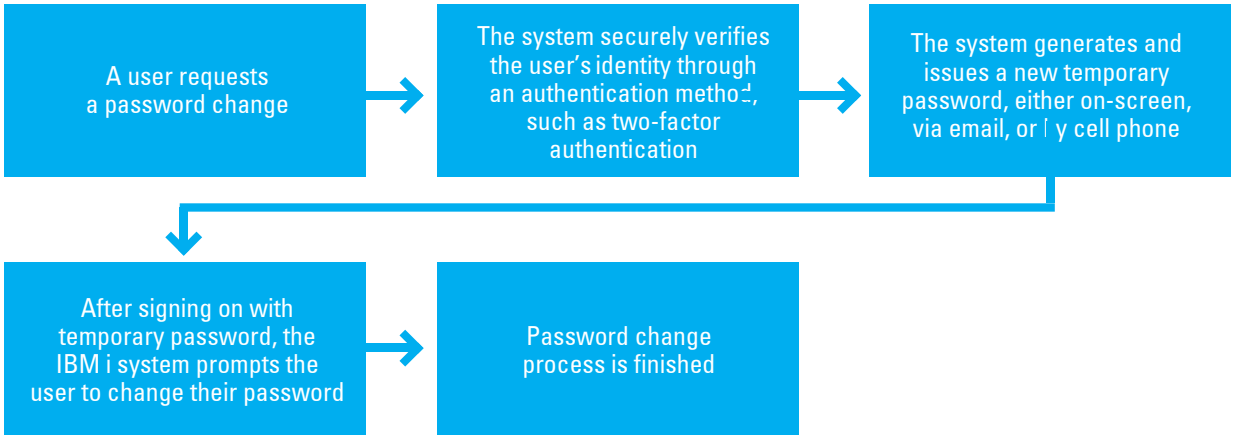
- The average resource allocation cost for password resets can be reduced by more than 80% or $100,000+ for an average company. For an average help desk, this can be calculated by taking the $125,000 average resource allocation risk (calculated above) multiplied by an 80% reduction in Help Desk tickets involving manual password resets.

Note: the percentage of password reset Help Desk incidents will not usually drop to zero (0%). A small percentage of users will always need help resetting their IBM i passwords.

How Automated Password Reset Programs Work

Automated IBM i password resets use a common framework for changing passwords. With some variations, most automated reset packages use the password change process shown in figure 2.

Figure 2: The automated password change framework



When properly set up, this framework provides for securely setting and resetting passwords.

What to Look For in IBM i Automated Password Reset Programs

There are several important features to look for in an automated password reset package. In our experience, we found these features deliver the most benefits and the best return on an automated password reset installation.

- Two-Factor Authentication (2FA) – Robustly identifies the user requesting a password reset.
- Automated deployment – Quickly deploys automated password resets without requiring the user to set up a reset profile.
- Agentless Password Changes on Computing Devices – Enables automated password reset without loading client software, agents, or apps to a device, decreasing roll-out & support costs.
- Group User Verification Policies – Enables organizations to use different authentication parameters for different user groups, providing stricter controls for sensitive users than for casual users.
- Logging and reporting capabilities – Records and reports on all automated password activity for auditors, and legal & regulatory compliance.
- Multi-system and multi-lingual deployment – Allows password reset technology to be used for all IBM i partitions and for all languages the organization does business in.

Here's how each of these technologies benefit an average IBM i shop.

Two-factor authentication

To prevent fraud or phishing, automated password reset software relies on robustly identifying users requesting password changes. Many packages employ two-factor authentication (2FA) to uniquely identify users by using any two of the following components.

- Something the user knows (the answer to a qualifying question)
- Something the user possesses (a cell phone or access to their email account)
- Something that is inseparable from the user (ex.,a fingerprint or a voiceprint) – Not usually used in IBM i password reset software

2FA systems usually verify user identify by asking the user one or more questions (something they know). After receiving a correct response, the system sends a verification code to their cell phone or email account (something they possess). The user retrieves the verification code, re-enters it into the password change program, and verification is complete. The probability of a hacker knowing the qualifying answers AND having access to the user's cell phone or email account is low, making this method a secure, reliable way of verifying user identify.

Automated deployment

Automated password reset programs succeed by how many users register and provide qualifying questions that prove their identity. But it's difficult to obtain 100% participation in an automated reset environment when relying on user self-registration. Many users will not participate.

Several vendors offer quick-start features that pre-register users with information from the customer's back office HR systems. These programs import HR information into the automated reset system and convert it into user accounts with basic qualification questions for two factor authentication. This information can also be imported from Excel files created from the HR system.

HR Information that can be imported and used for authentication data and starter questions include:

- Employee #
- Social security number
- First name
- Birthday
- Family name
- Email address
- ID number
- Cellphone # (if available)

After a password reset system is populated with HR information, it can be personalized for specific individuals and groups.

Agentless Password Changes on Computing Devices

Many companies use agentless software to speed deployment and avoid desktop or mobile configurations for password resets. Instead of providing client software or apps, these packages allow users to change passwords through two agentless techniques.

- From the IBM i sign-on green screen –The user signs-on to an IBM i using a special password reset user profile and password. This sign-on triggers a password change program that initiates two-factor authentication and changes their password.

- A Web-enabled program – Some packages offer Web services that provide 2FA authentication and run the password change process, without being signed on to an IBM I partition. The administrator creates a special URL for the Web program and users can change their IBM i password from any location that can access the password change URL.

Group User Verification Policies

This technology recognizes that different users have different verification requirements (ex., a CFO with access to financial information needs stricter verification than a warehouse worker). Some packages provide password reset classes that create different password verification procedures for different organizational groups Password reset classes override the global user verification policy with a different policy for group members, including these items.

- Number of times the users must verify a new password
- The number of private personnel questions to be asked (0-10 questions), in addition to standard questions
- How users should receive new temporary passwords
- How long a temporary password is valid for, usually in number of minutes

Logging and Reporting Password Reset Attempts

Increasingly stringent audit requirements combined with regulatory and legal requirements are requiring tighter controls on password modification. Answering these needs, many automated reset programs log all password change attempts into a history log for full audit traceability. History files can be accessed to provide the following information.

- All password reset attempts
- Reset requests by date and time ranges
- All password reset errors and exits (indications of possible hacker activity)
- SQL or SQL-like query filters, for auditing requests and suspicious activity investigation

Multi-system and multi-language deployment

Many automated reset packages allow users to reset their passwords for all systems and platforms they are authorized to access, using a single authentication screen.

Some software also allows users to set up and define 2FA qualifying questions and other text in several different languages. This lets customers use one IBM i package in multiple local and global locations, insuring that foreign nationals and overseas users can use automated password reset.

Summary: The Benefits of IBM i Automated Password Resets

Manual IBM i password resets create a multitude of risks for every organization. They drain productivity, damage customer relationships and SLA commitments, increase security exposure to financial systems, cause auditing and compliance issues, and waste IT resources.

Implementing an automated IBM i password reset system mitigates these risks and provides benefits beyond risk reduction, especially in the following areas:

- Increased productivity – Password resets will stop affecting production processing. Users can reset their password themselves. Off-hours password resets will no longer be delayed until the next working day.
- Protecting relationships – Password lockout delays will no longer endanger customer relationships or SLA commitments. Self-service password resets allow an organization to continue servicing clients in a timely way.
- Reducing security risks – A locked out user's identity will always be securely established before they reset their password. Bad actors will not be able to reset passwords for critical users, the Help Desk will no longer know other people's passwords, and password security standards will always be enforced.
- Eliminating audit and compliance issues – Auditing and compliance reporting will be almost instantaneous. IT will always have password reset information at its fingertips.
- Reducing or redirecting IT consumption – IT can realize cost savings by reducing Help Desk resources or retraining excess Help Desk resources to support key initiatives.

IBM i-based organizations can take a key step forward by implementing automated IBM i password resets.

Learn More About iSecurity Password Reset

iSecurity Password Reset is SEA's IBM i automated password reset solution, providing most of the capabilities described in this white paper. Password Reset is integrated into the IBM iSecurity software suite and can be used as part of that suite or as a stand-alone solution.

To learn more about IBM i automated password resets and iSecurity Password Reset, contact SEA for a live demonstration or a 30-day free trial or visit the iSecurity Password Reset page.

About Software Engineering of America (SEA)

Established in 1982, Software Engineering of America has built a global reputation as a leader in datacenter software solutions. SEA is one of the most successful companies in the data center software industry, with products used at thousands of installations worldwide. Over 10,000 data centers of all sizes and configurations are utilizing one or more of SEA's products, including 9 of the Fortune 10 as well as 85% of the Fortune 500 Companies.

Learn more at seasoft.com