WHITE PAPER

HITACHI
Inspire the Next

How to Go Passwordless at Your Organization to Reduce Cybersecurity Risk

Password Management Explained from Federation and Password Managers to Adaptive Authentication, and Legacy Solutions

Hitachi ID

The State of Password Management

Passwords pose significant problems for organizations and users alike, precisely due to their ever-growing abundance and complexity:

- Users struggle to recall strong passwords
- Users struggle to remember many passwords
- Users use password hints inappropriately that make social attacks on passwords easy

And since people need to get their jobs done, they react with common and predictable approaches that include:

- Reusing passwords across sites and services both personal and professional
- When prompted to change passwords simply add or subtract one from the number
- Use personal password managers for business accounts and secrets
- Write down passwords on sticky notes or in notebooks
- Using common words like "blue" and "car" in their passphrases. Cat-blue-car isn't a strong passphrase.

When you peel back the layers, there often are many cases where people are practicing predictable password approaches that you might not be aware of. Examples include:

- Passwords to social websites you use for business promotion
- Passwords you hold for your customers environments when you are providing services
- Passwords to encrypted spreadsheets
- Wifi and network access passwords
- Company credit cards
- Cloud hosted resources (passwords, ssh keys, etc)
- Internally hosted resources that might be officially IT sanctioned as well as unofficial systems
- Dev/test labs
- Hard drive recovery keys for encrypted devices
- 2FA recovery keys for 2FA solutions
- Authenticator tokens and backups when devices, security tokens, and YubiKey are lost
- Under the cover passwords that still exist and can be optionally used when 2FA options cannot be used

These common - and almost universal - scenarios and actions employees take to deal with the problems associated with password management that puts your organization's security at risk. Companies need strategies that work with human nature. Not in conflict with it. And the growing HitachI ID Bravura Security Fabric can provide solutions to help companies adopt realistic approaches to solve these challenges.

Ask yourself, "Am I personally doing any of the above?". Hitachi ID has found that the answer is almost universally "Yes, I'm doing some or all of the above". This is a major problem for most companies when they feel that most/all of their employees are encountering most/all of these problems. And companies are looking for strategies to get these scenarios under control.

To start, companies need to realize that there is no silver bullet here. There is a great deal of hype in the market for passwordless technologies but you need to adopt a strategy and a mentality where a baseline is established that everyone in the company can use for every application they use. Once that baseline is established you can then begin the process of optimizing points of risk by introducing a least password strategy and drive towards adopting better technologies and strategies using iterative projects prioritized by their risk to your enterprise.

With this guide from Hitachi ID, your organization can begin your least password jouney. We will provide a helpful overview of what approaches methods are available (legacy and modern) along with their use cases, strengths, and weaknesses to create a viable strategy that establishes your "level 1" baseline for all employees in your cyber security maturity model with practical strategies to grow beyond level 1.

IT Professional Password Problems

Many cybersecurity experts have long known that passwords are a weak link in the security chain. For example, one in four breaches in 2022 utilized stolen passwords, according to the latest Verizon Data Breach Investigations Report.

Most organizations have recognized password vulnerability and have adopted strong password guidelines. These can include minimum characters and a mix of letters, numbers, characters, and capitalization rules. Another common policy stipulation is forcing mandatory user password changes at set time intervals such as every six months or a year. This ever-growing list of password requirements makes them increasingly complicated and difficult to remember.

Passwords also present several problems for organizations, including complexity and quantity. With the proliferation of software and applications, the number has increased exponentially, further confusing the process for both users and IT professionals. Multiple passwords also bring different interfaces, expirations, and policies. Often, users simply have too many passwords to sign into different systems and applications, and they respond to this complexity by:

- Avoiding password changes
- Choosing simple (insecure) passwords
- Writing down passwords
- Forgetting passwords and calling the help desk or overusing forgotten password options
- Manually syncing passwords between personal and professional resources
- Using personal password managers like LastPass, Dashlane, and KeePass for both personal and professional resources

Over time, poor password management can create user and business problems such as:

- User inconvenience and frustration
- High help desk call volumes
- Weak authentication
- Compromised security
- Business continuity challenges when employees leave, are sick, or go on vacation and staff don't have access to their personal password manager.

Current Password Management Solutions

Three types of products address the same business problem of authentication and verification across enterprise organizations: federation, password managers, and privileged access management.

Your organization needs to strike a balance between the flexibility of a password manager and a vaulting solution. It sets your baseline where you can store anything in it.

Adopting federation when possible and cost-effective. You need to consider this with all SaaS-hosted applications and the perimeters to your networks regardless of if they are on-premises or cloud-hosted.

Adopting privilege when you need to guard your keys to the castle. Your special sauce. Your golden goose. Ensure you have the just in time level of access and minimized standing privileges with comprehensive auditing.

The following three password management methods are nearly universally accepted by security leaders globally because they offer many of the features needed in the current security landscape to balance security and risk, but they do have shortcomings.

1. Decentralized Password Managers, Wallets and Vaulting Solutions

Decentralized Password Managers, also known as wallets or vaulting solutions, compliment Password Synchronization strategies well. In both cases your goal is to establish **one** password that people can be expected to remember that is:

- Unique and not associated with any existing passwords in use
- Reasonably strong and easy to remember
- Not on compromised password lists or involved in known data breaches

Then to defeat the escalating arms race with brute force attacks, your **one** password for these platforms **need** to be complimented with a TOTP token or other second factor. This ensures your authentication is based on:

- What you have which is the TOTP token
- What you know which is your reasonable to remember primary password

Using this strategy, you can have confidence your password manager carries a baseline level of security that in practice is very resistant to most forms of attack.

As an enterprise, you should offer the password manager to **all** employees to use. A consistent tool sets a baseline for security that can be expected - and required of - your employees. A good tool should provide these basic capabilities:

- Ability to store any form of passwords and to set good baselines for minimum password complexity
- Ability to share one time use or onboarding passwords/files/etc securely and not in emails and IMs
- Ability to teach and alert employees to problems in the passwords they are using. Inform them when their passwords are weak, on compromised password lists, or are being manually synchronized
- Ability to share credentials within teams of people both inside your organization and externally to your organization
- Ability to automate the submission and usage of passwords in web browsers and other tools people use on a day to day basis

A decentralized password manager, wallet, or vaulting solution, like the new Hitachi ID Bravura Safe, is a baseline for establishing your enterprise cybersecurity journey that your de-risking initiatives can build upon. You can adopt an enterprise password manager like Bravura Safe as a standalone solution or add it your existing Hitachi ID solution. You can deploy Bravura Safe within a matter of hours to benefit from capabilities such as:

- Synchronization of your directory password with your master password.
  - Continue your least passwords journey to a passwordless state.
  - Ensure your one password is strong.
- Joiner/Mover/Leaver capabilities.
  - Grant people access to Bravura Safe seamlessly as they join your organization.
  - Allow people to access team credentials easily when they transfer through positions at your organization.
  - Ensure business continuity when people leave your organization.
- Promotion into Bravura Privilege.
  - Provide people with simple approaches to promote credentials into Bravura Privilege for more active management.
  - Easily access credentials in Bravura Privilege by clicking links in Bravura Safe to minimize your clicks to access.
  - Securely monitor when people use your keys to the castle to access your golden goose.

Tools like Bravura Safe should not be considered a stepping stone but instead should be considered a foundational piece of your Identity and Access Management journey. Edge and decentralized credentials are going to be around for a very long time. It will be years or decades before people stop using passwords for:

- B2B portals and service engagements between companies.
- B2C portal that your staff are signing up for to consume SaaS hosted services.
- Embedded device credentials. Hopefully not hard coded. But certainly defaulted and potentially difficult to change.
- Temporary labs, demo environments, etc that are naturally ephemeral in nature but might be accessed for days, weeks, and maybe months.

2. Federate Access to Solutions

Once you have established a baseline of access through adopting tools like Bravura Safe, you need to strongly consider federated access to solutions. Federation provides a materially stronger and easier to audit level of protection for your core services.

In a federated ecosystem, the first system is called the Identity Provider, or IDP. The application (or second system) is called the Service Provider or SP, and the message sent between systems is called an assertion. The assertion includes the user's account name and other pertinent information that the SP needs to create a user session. The assertion is cryptographically signed, so the SP can trust that it came from the correct IDP. An example of federation is when users can use their Gmail account or social media credentials to log into other applications, websites, and resources.

You'll notice the SP has nothing to do with user authentication. It relies on the IDP to do all of the heavy lifting. The only thing the SP cares about is whether the IDP authenticated the user correctly.

For federation to work at scale, IT and cybersecurity experts needed to develop standards that allow globally distributed systems, likely owned by different organizations, to work together. One of the most widely used is SAML, or Secure Assertion Markup Language. Its latest version, SAML 2, has the advantage of SP-initiated login. It provides a better user experience by allowing them to go directly to the app they want to use without navigating through a portal first.

Then within this single identity provider you can set your authentication baseline requirements such as:

- Minimum MFA factors needed. For example, your federation solution can always require 2 factors as a baseline.
- Passwordless authentication options that might be as simple as "email a link to authenticate".
- Biometric authentication option that also factors into a passwordless journey.
- Risk adjusted authentication. Ask for additional factors to prove identity if authentication attempts appear risky.
- Options for when your users forget or lose authentication factors (passwords, phones, hardware tokens, etc) and need to get them reset.

Federation is now extremely common in most enterprises. But you need to strategize about where you apply it first. It's not free and requires configuration to be done with the applications and services you need to protect. So what should you protect first? Hitachi ID would recommend you focus on them in this priority order:

1. Your SaaS applications.
    - Your first focus. Make sure Salesforce, Workday, Bamboo, Zendesk, Gitlab, Github, Jenkins, Bravura Safe, etc are secured. You must invest here.
2. Your IaaS environments.
    - IaaS platforms like Azure and AWS hold your golden gooses. Protect them. It's worth the investment.
3. Your zero trust networks.
    - As people migrate away from vpns and towards zero trust networks, start yourself off on the right foot. Invest as you transform your networks.
4. Your on-premises networks accessible over vpn.
    - Often these are guarded with 2fa options such as password and a machine key already. Invest if it makes sense. But if you are starting a zero trust network journey it might not be worth it.
5. Your on-premises applications.

- Many companies are working towards SaaS applications and removing on-premises applications. Balance the cost of configuration with other options such as directory password authentication and Bravura Safe for less sensitive applications or those with a limited lifespan.

3. Privileged Access Management

Solutions like Federation and Bravura Safe focus on authenticating your users when they have standing privileges in an environment. A standing privilege is an account that exists in your enterprise with the level of access needed to complete a task that an employee can use anytime.

It's inevitable that you have large amounts of standing access in your organization.

Examples include:

- User access to salesforce for your sales employees.
- Access to google and microsoft communication platforms.
- Instant messaging platforms.
- Support and services platforms.
- Product and project management platforms.

But some applications are too critical to allow people to have standing access rights to them. In these cases you want to provide people with just in time access to these solutions. That way you can move towards both a **least passwords** strategy as well as a **least trust** strategy.

Privilege Access Management platforms like Bravura Privilege work on a fundamental premise. Remove employee access to long lived credentials and broker their access with temporary entitlements. But what does this all mean? Its easiest to explain with a few examples:

- Removal of people's ability to access vaulted credentials and require them to request access to them. This way they only get the vaulted credentials when they prove to an authorizer they need them.
- Periodically rotate credentials on a schedule. That way if people do store them they become invalid after a period of time.
- One time use passwords. Ensure passwords are changed **after** they have been used.
- Remove passwords entirely and broker peoples access to systems using ssh keys being added and removed from systems as needed.
- Remove needless additional accounts by giving people a **single** personal admin account which leverages one time use passwords and access brokering. This can really benefit with auditing employee access.
- Just in time add people to groups so they can use their existing directory accounts - temporarily - as administrative accounts on platforms and endpoints.

All of these are proven and industry adopted approaches to minimize the passwords employees need. Each of these materially improves people's least password journey by simply removing standing and static passwords from the equation.

A common additional level of security is access brokering both through secured client side disclosures as well as proxy approaches. The most secured systems and access result in an employee never wanting the password. Just press a button and they have access. Getting access to the password becomes an inconvenience for the user when done properly.

Credential brokering and one time use credentials requires deeper integrations with platforms due to the nature of the problem. As such, this solution is often implemented for standardized production environments and popular services.

Examples where companies are routinely succeeding with these strategies include:

- Managing built in credentials to operating systems. Administrator on Microsoft Windows. Root on Linux. SA in SQL server
- Managing credentials reserved for help desk operations that might be deployed out to a fleet of windows and linux machines
- Administrative credentials in well known SaaS platforms

Legacy Password Management Solutions

Once the current standards for password management, these methods are now outdated. In many ways, they paved the way for what followed. Federation, password managers, and adaptive authentication took some of the best elements from these legacy solutions and added new features and restrictions that provide superior experience and security. Many remain in use today, and your organization may need to find a way to integrate them into your password management mix.

Legacy solution	What it is	Why is it considered legacy?
Password Synchronization, Reset, & Unlock	Password synchronization is an approach to tackling password problems involving synchronizing different passwords, so users only have to remember one. It is a method of achieving SSO by ensuring a user's passwords are the same across multiple systems and subject to a single security policy. Reset empowers the user to reset forgotten passwords or clear a lockout on their own — all without calling the help desk. Unlock allows users to do the same for encrypted drives	Whenever you're securing more than one application with an identical credential, there's a substantial risk that one compromised resource can jeopardize multiple. Authenticating against a directory allows users to use a password they remember for a range of services within that directory, while sync can threaten multiple. Only a few significant reasons to use password synchronization exist: ● Expand the footprint ○ Connecting directory-based services to non-directory attached environments ● Create a level playing field across resources ○ Utilizing sync sets the stage for optional added features such as MFA ● Support legacy applications ○ If a resource doesn't support more modern and secure protocols ● Build convenience ○ If user experience and ease of login are more important than security

Legacy solution	What it is	Why is it considered legacy?
Enterprise SSO	Enterprise SSO (ESSO) minimizes the number of times a user must type their ID and password to sign into applications. ESSO acts as a surrogate process for the user: storing, retrieving, and “typing in” the user ID and password on their behalf, similar to how password managers work today. Traditionally ESSO is done via a centralized database that stores all your passwords and is typically not web-based (like many password managers). Instead, ESSO client software is installed on a user’s computer. ESSO uses a local or network file, database, or directory to store application login IDs and passwords for each user. This is often referred to as a password wallet, which is usually encrypted with a key derived from the user’s primary password.	It’s a single point of failure; users can’t sign into anything if the ESSO system is down. Nor does ESSO eliminate password complexity. The user continues to have multiple user ID and password pairs, so they might not know what their passwords are in some cases. When applications prompt users to change their passwords, ESSO systems often choose a new, random password and store that in the password wallet. This results in a situation where users are completely reliant on the ESSO systems to sign into applications.
Web Access Management	WAM first appeared in the late 90s as the internet began its ascent. The first WAM products delivered straightforward functionality that helped share user credentials across multiple domains without numerous logins. Now, it’s a legacy SSO designed for enterprise web applications. WAM is still present, but federation is slowly pushing it out. WAM or web-access management is historically an on-premise solution that provides centralized authentication and session management for web applications. Once it validates a user through authentication and authorization, the WAM solution typically delivers a temporary token to all the resources the user can access. WAM typically targets applications that do not support federation but are web-based. These solutions generally require support from the application vendor to expose the proper connections necessary to integrate with a WAM solution.	Technology has evolved past WAM, and many organizations have adopted new services that secure authentication and access regardless of context, network, and location. This evolution has challenged the WAM security model because it operates inside a private network and doesn’t update routinely enough to support new systems, falling short of delivering cost-effective security.

Instead of using password synchronization, the best (and most flexible) solution is to utilize SSO strategies such as SAML and OAuth that don't use passwords. You will not only avoid the problem of identical passwords (since you're not using them), but gain some security benefits in the process.

Organizations can address these legacy limitations by replacing them with integrated identity access management (IAM) solutions like Hitachi ID Bravura Identity, allowing you to link users to any resource, regardless of architecture or location.

Legacy Solutions and Interoperability Challenges

Federation is the go-to method for password management when you have a solution to support it. Your solution also needs to be flexible and adaptable to previous standards and compatible with a wide range of resources and maintains capabilities in scenarios such as:

- Legacy applications that cannot federate running on a "thick client"or a computer that provides rich functionality independent of the central server, providing critical functions to your network and systems
  - Pair with password synchronization
- Web applications that cannot federate because they are too old or do not support federation web-based protocols such as SAML 2.0 or newer ones such as OpenID Connect, OAuth2
  - Password vaulting and injection may be necessary
- Self-service password reset on your "master vendor" is unsupported
  - Most vendors have this but it is a key component of any SSO solution as the master password basically holds the keys to all of your downstream applications
  - Making sure this is both (a) strong and (b) easy to recover if forgotten is important

Integration for the Win

With login and password problems continuing to represent 30% of the call volume to a typical help desk, organizations need a way to help themselves.

Hitachi ID Bravura Safe and Pass, components of the Hitachi ID Bravura Security Fabric, helps users to better manage their own credentials with an integrated solution for maintaining credentials across systems and applications.

Bravura Pass is the answer to many of the challenges your organization (and users) have with password quantity and complexity, including:

- Strong authentication (MFA) and federated access SAML 2 identity provider (IdP)
- Self-service password and PIN reset
- Self-service unlock of encrypted drives
- Managed enrollment of security questions, mobile phone numbers, email addresses, and biometrics

The Hitachi ID Bravura Security Fabric, which includes Hitachi ID Bravura Pass, provides a single access point for all of your enterprise applications whether you're accessing through federation, password synchronization, adaptive authentication, or legacy solutions.

Next Steps

The Hitachi ID Bravura Security Fabric has the technological building blocks with decades of proven reliability to manage and protect your entire digital identity and access infrastructure from malicious attackers. It encompasses all of the Hitachi ID Bravura Security Fabric including Identity, Privilege, Pass, and Group with the Hitachi ID Bravura Discover threat detection and response (TDR) layer all together in a singular, powerful platform.

Simplify password management, easily control credentials on-premises and in the cloud while reducing IT support costs and improving login security with Hitachi ID Bravura Safe.

REQUEST A DEMO of Bravura Safe to get started.

We Are Hitachi ID

As a recognized market leader, we deliver access governance and identity administration solutions to organizations globally, including many Fortune 500 companies. By leveraging decades of experience, we provide the industry's only single platform identity and privileged access solution to simplify implementation as your IAM and PAM roadmaps evolve.

Hitachi ID Systems, Inc.

Corporate Headquarters
1401 - 1st Street S.E., Suite 500
Calgary, Alberta, Canada T2G 2J3
hitachi-id.com

Contact Information
1.403.233.0740
Sales Toll Free: 1.877.386.0372 / 1.877.495.0459
sales@Hitachi-ID.com