

Integrating

**Password Management
with Enterprise single sign-on**



Contents

- 1 Introduction** **1**

- 2 Background: One Problem, Two Solutions** **2**
 - 2.1 The Problem 2
 - 2.2 Password Synchronization and Reset 3
 - 2.2.1 Password Synchronization 3
 - 2.2.2 Self-Service Password Reset 3
 - 2.3 Enterprise single sign-on 4

- 3 Strengths and Weaknesses** **5**

- 4 Deployment** **6**
 - 4.1 Password Synchronization 6
 - 4.2 Self-Service Password Reset 6
 - 4.3 Enterprise single sign-on 7

- 5 Motivation for a Combined Solution** **8**

- 6 Interoperability Challenges and Integration Solutions** **9**
 - 6.1 Password Reset and E-SSO 9
 - 6.2 Password Synchronization and E-SSO 9

- 7 Integration Options** **10**
 - 7.1 Lightweight Integration: Self-Service Password Reset for the Primary E-SSO Password . . . 10
 - 7.2 Full Integration: Automated Enrollment of E-SSO Credentials 10

- 8 Summary** **11**

1 Introduction

This document compares and contrasts two solutions that address a single business problem: password complexity. The two solutions are:

1. password synchronization and reset, and
2. enterprise single sign-on.

It also lays out rationale for some organizations to deploy both types of technologies, and discusses integration challenges and solutions.

This document is organized as follows:

- **Background: One Problem, Two Solutions**

The business problems caused by password complexity are described, and two alternate solutions to address these problems are described.

- **Strengths and Weaknesses**

The strengths and weaknesses of three technologies designed to address password complexity are reviewed.

- **Deployment**

Identifies the major tasks that must be accomplished in order to deploy each of the three technologies.

- **Motivation for a Combined Solution**

Business drivers for deploying a combination of solutions are laid out.

- **Interoperability Challenges and Integration Solutions**

Password reset and enterprise single sign-on technologies can interfere with one another. Similarly, password synchronization and enterprise single sign-on technologies can conflict. Integrating the technologies is essential to eliminating these conflicts.

- **Integration Options**

Integration between solutions can eliminate interoperability problems, and two integration options are described.

Hitachi ID Password Manager supports both lightweight and full integration with enterprise single sign-on systems, including Citrix Password Manager, RSA Signon Manager and SAP Portal.

2 Background: One Problem, Two Solutions

2.1 The Problem

Users who must manage multiple passwords to corporate systems and applications have usability, security and cost problems.

Users have too many passwords. Each password may expire on a different schedule, be changed with a different user interface and be subject to different rules about password composition and reuse.

Some systems are able to force users to select hard-to-guess passwords, while others are not. Some systems require that users change their passwords periodically, while others cannot enforce expiration.

Users have trouble choosing and hard-to-guess passwords.

Users have trouble remembering passwords, because they have too many of them or because they chose a new password at the end of the day or week, and didn't have an opportunity to use it a few times before going home.

These problems drive users to choose trivial passwords, to avoid changing their passwords and to write down their passwords. All of these behaviors can compromise network security.

When users do comply with policy and regularly change their passwords to new, hard-to-guess values, they tend to forget their passwords and must call the help desk.

Password and login problems are the top incident type at most IT help desks, frequently accounting for 25% or more of total call volume.

In addition to the above security and support cost problems, users simply don't like memorizing and typing passwords. Password management is a nuisance that contributes to a negative perception of IT service.

Despite all these problems, passwords will continue to be needed for years to come:

1. Passwords are significantly less expensive to deploy and support than other technologies.
2. Other authentication technologies, such as biometrics, smart cards and hardware tokens, are typically used along with a password or PIN. i.e., "something you have" (smart card, token) or "something you are" (biometric) plus "something you know" (password, PIN).
3. Passwords are an important backup to other authentication technologies:
 - (a) Hardware devices can be lost or stolen or simply left at home.
 - (b) Some devices from which users need to access corporate systems, such as smart phones and home PCs, may not support more advanced authentication methods.

Since passwords are not going away and remain difficult for users to manage, solutions are needed to help users more effectively manage their passwords.

2.2 Password Synchronization and Reset

Products that offer password synchronization typically also offer self-service password reset. Similarly, products that offer self-service password reset frequently also offer password synchronization.

Hitachi ID Password Manager is a password reset and synchronization product.

2.2.1 Password Synchronization

Password synchronization is any process or technology that helps users to maintain a single password, subject to a single security policy, across multiple systems.

Password synchronization is an effective mechanism for addressing password management problems on an enterprise network:

- Users with synchronized passwords tend to remember their passwords.
- Simpler password management means that users make significantly fewer password-related calls to the help desk.
- Users with just one or two passwords are much less likely to write down their passwords.

There are two ways to implement password synchronization:

- Transparent password synchronization, where native password changes, that already take place on a common system (example: Active Directory) are automatically propagated through the password management system to other systems and applications.
- Web-based password synchronization, where users are asked to change all of their passwords at once, using a web application, instead of continuing to use native tools to change passwords.

2.2.2 Self-Service Password Reset

Self-service password reset is defined as any process or technology that allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate method and repair their own problem, without calling the help desk.

Users who have forgotten or locked out a password may launch a self-service application using an extension to their workstation login prompt, using their own or another user's web browser or through a telephone call. Users establish their identity, without using their forgotten or disabled password, by answering a series of personal questions, using a hardware authentication token or by providing a biometric sample. Users can then either specify a new, unlocked password or ask that a randomly generated one be set.

Self-service password reset expedites problem resolution for users after a problem has already occurred and reduces help desk call volume. It can also be used to ensure that password problems are only resolved

after strong user authentication, eliminating an important weakness of many help desks: social engineering attacks.

One of the core features of Hitachi ID Password Manager from Hitachi ID Systems is self-service password reset.

2.3 Enterprise single sign-on

Enterprise single sign-on (E-SSO) systems are designed to minimize the number of times that a user must type their ID and password to sign into multiple applications.

Most enterprise single sign-on systems work as follows:

- E-SSO client software is installed on every user workstation.
- Users sign into their workstation, either as they did before or through a new user interface presented by the E-SSO client software.
- A local file, a network-attached database or a user directory stores each user's ID and password, for each system and application to which that user has access.
- When a user launches an application on their workstation, the E-SSO client software automatically populates the ID and password fields in that application's login screen with data from the aforementioned credential storage.

E-SSO software acts as a surrogate for the user: storing, retrieving and "typing in" the user ID and password on behalf of the user. The user continues to have multiple ID/password pairs, but does not have to type them manually and may not know what they are.

With an E-SSO system, users sign into their workstation with either one or two login ID / password pairs: One set of credentials if the E-SSO captures the user's password from the initial workstation login screen, or two ID/password pairs if the user must first log into the workstation (e.g., Windows login) and subsequently into the E-SSO client software.

Some E-SSO systems support use of authentication technologies other than passwords to sign into the workstation and retrieve the user's application passwords. This may include smart cards, authentication tokens or biometric samples.

Application login IDs and passwords may be stored on a smart card, rather than on the user's workstation or on the network.

Enterprise single sign-on systems include RSA Signon Manager, Citrix Password Manager and SAP Portal.

3 Strengths and Weaknesses

Each of the three technologies has its own strengths and weaknesses:

Solution	Strengths	Weaknesses
Password Synchronization	<ul style="list-style-type: none"> • Reduces both password problem frequency and help desk load. • Easily deployed – no client software, limited server-side agents. • Can be automated, requiring no user cooperation. • Can improve the quality of all passwords. • No single point of failure. • Systems with multiple access channels remain accessible from anywhere (PCs, web, phone, etc.). 	<ul style="list-style-type: none"> • Users still have to sign into each system separately. • All passwords are the same – a compromise of any one leads to a compromise of all. • Some passwords, in particular those on third party systems outside the corporate network, and those on applications with very small numbers of users, normally remain out of scope.
Self-Service Password Reset	<ul style="list-style-type: none"> • No matter what solution is deployed, users will eventually have a password problem. Self-service is a valuable solution for this eventuality. • Easily deployed – often with no client software and limited server-side agents. • Can reduce a help desk's security vulnerability to "social engineering" attacks. 	<ul style="list-style-type: none"> • Does not reduce problem incidence – only diverts resolution away from the help desk. • Requires user cooperation to be effective.
Enterprise single sign-on	<ul style="list-style-type: none"> • Eliminates repetitive sign-ons by users. • Maintains different passwords on every system. In most cases, compromise of a single user password does not lead to compromise of all. • Does not require deployment of software on target systems, and in fact can be deployed with little or no knowledge about the internal workings of integrated systems. • Can support both internal and external systems that require password authentication. • Primary authentication can be upgraded to use a hardware token, a biometric, or multiple factors. 	<ul style="list-style-type: none"> • Costly deployment of client software to every workstation. • Does not support applications with multiple user interfaces (e.g., client, web, phone) well. • Single point of failure: if the E-SSO system is down, users can't sign into anything. • Compromise of the "master" password does compromise all other passwords. • Requires enrollment of user login IDs and passwords into the credential database. • Relies on Windows "screen scraping" technology, which can be costly to deploy and manage, especially across multiple types of workstations.

4 Deployment

4.1 Password Synchronization

A password management system, such as Hitachi ID Password Manager, requires a profile of login IDs for every user, on every system. This must be constructed at the outset of the deployment project, and maintained over the life of the system.

In the event that login IDs are consistent across systems, constructing and maintaining these profiles is easy. If login IDs belonging to the same user are different on some systems, some work is required, either centrally or by each user, to connect different IDs back to their individual owners.

In general, no client software deployment is required.

In general, little or no target-system software deployment is required.

In general, little or no ongoing system maintenance is required.

Password synchronization systems can be quite fast to deploy, especially in organizations that have all of their pre-requisites – hardware, server OS images, target system information, administrative credentials and policy decisions – ready at the outset of deployment. For example, Password Manager has been deployed in organizations with as many as 90,000 users, to synchronize passwords over a dozen systems, in just 5 days. Password Manager has been deployed to organizations with as many as 300,000 users.

4.2 Self-Service Password Reset

In addition to the login ID profiles described above, a self-service password reset system, such as Hitachi ID Password Manager, also requires a secondary authentication factor for each user.

This typically comes in the form of a question-and-answer profile, where users must answer one or more personal questions in the event that they forget their password(s), and once authenticated can initiate a password reset.

If such Q&A data is not available or adequate prior to deployment, it must be collected from the users.

Some password reset systems rely on deployment of a GINA-wrapper DLL to address the problem of enabling users to reset forgotten or locked primary network passwords. This client software deployment can be invasive and costly. Other systems also support use of a specially constructed domain account (e.g., “help”) and/or a telephony-based solution to enable users to access password reset.

In general, little or no target-system software deployment is required.

In general, little or no ongoing system maintenance is required.

Password reset systems can be quite fast to deploy, but typically require some time after installation is complete to enroll users. For example, Password Manager has been deployed in organizations with as many as 135,000 users in just 2–3 weeks, followed by 2–3 months to run an unattended user enrollment process.

4.3 Enterprise single sign-on

An enterprise single sign-on (E-SSO) system requires not only login ID profiles for each user, but also current passwords for each user, to each target application. The enrollment process is consequently much more difficult, and in fact there are very few real-world deployments of E-SSO systems to populations of more than a few thousand users.

E-SSO systems require client software deployments by definition. Distribution and configuration of client software to large numbers of workstations can be quite costly.

E-SSO systems also require a credential database, in which to store each user's login ID and password. This may come either in the form of a dedicated network service (database or directory), or by extending the schema of an existing directory (e.g., Active Directory, LDAP, NDS).

The credential database must be fast and highly available, as a failure in this system will prevent large numbers of users from signing into any system at all. The credential database must also be secure, as a compromise might lead to the compromise of every user's password to every system.

E-SSO systems are typically harder to deploy than password synchronization and reset, due to the client software and user profile requirements outlined above.

There are very few production deployments of E-SSO with over 5,000 users. The largest publicized deployment of an E-SSO system is for 147,000 users, and that deployment is not complete as of this writing.

5 Motivation for a Combined Solution

As laid out in [Section 3](#) on [Page 5](#), both a password reset/synchronization and an enterprise single sign-on solution have their merits.

Combining E-SSO with password synchronization and reset can address some of the shortcomings of E-SSO alone:

- **Applications with both a Windows and web user interface**

If passwords are not synchronized, and users only know their E-SSO password, then they will be unable to use alternate user interfaces to their applications. For example, users might be able to access their e-mail using a proprietary client such as Outlook or Lotus Notes, but will be unable to use a web mail portal, since they do not know their own mail password.

By combining password synchronization with E-SSO, effectively making sure that the user's primary E-SSO password is the same as the user's password on other applications, and in particular on those applications that present a web user interface, it is possible to ensure that the user continues to be able to sign into these web user interfaces.

- **Users who forget their primary E-SSO password**

If users forget their primary E-SSO password, they can reset it with a self-service password reset system.

- **Automated collection of user credentials for the E-SSO repository**

Deploying a password synchronization system first, and an E-SSO system second, can significantly reduce the time and effort required to implement the E-SSO system.

This is because the password synchronization system will already have a login ID profile for every user, and can capture and store each user's password to every system with which it is integrated. As a result, E-SSO user profiles can be pre-populated by the password synchronization system, eliminating a costly and time consuming user enrollment process.

6 Interoperability Challenges and Integration Solutions

6.1 Password Reset and E-SSO

As mentioned in [Subsection 2.3](#) on Page 4, an E-SSO system stores a user's login ID and password to every system and application in an encrypted database.

Typically the user's credentials are encrypted with a key derived from the primary E-SSO password. This might be the user's Windows, Active Directory or NDS password, or it might be a separate password altogether.

If the user forgets his primary E-SSO password, then the user's credentials to every other system will be lost. Even after the E-SSO password is reset, the encrypted credentials will continue to be inaccessible, since they are encrypted with a key derived from the user's old, forgotten password.

In other words, resetting a user's E-SSO primary password means that the user's profile will be lost, and the user must get a new password for all other systems, and must re-enroll with the E-SSO system.

To address this problem, an E-SSO system must provide a "back door," so that the credential database for a user can be recovered after a password reset. The simplest way to do this is to store the user's current password, or current key, in a safe location, and use it to decode the user's credentials in the event that the user forgets his current password.

A password reset system must integrate with this back door system, or provide its own back door. In other words, after resetting the user's primary E-SSO password, a password reset system must recover the user's previous password or key from safe storage, decrypt the user's old credentials, and re-encrypt them using the new password and key, so that the E-SSO client software will be able to access them again.

6.2 Password Synchronization and E-SSO

If a password synchronization system changes a user's password on a system or application where the user signs in using an E-SSO client, then the credentials in the E-SSO's database will become obsolete. The E-SSO will not be able to sign the user into that system, and will either fail entirely or force the user to re-enroll his password on that system.

At worst, this interference will either prevent the user from using the system or application in question. At best, this interference is a nuisance for users, who must re-enroll passwords in the E-SSO after every password change.

If the password synchronization system is able to update the E-SSO's credential database after each successful password update, the problem can be eliminated.

7 Integration Options

Hitachi ID Password Manager supports both lightweight and full integration with enterprise single sign-on systems, including Citrix Password Manager and SAP Portal.

7.1 Lightweight Integration: Self-Service Password Reset for the Primary E-SSO Password

A lightweight integration between a password reset system, such as Hitachi ID Password Manager, and an E-SSO, provides self-service password reset for the primary E-SSO password only.

After each successful password reset, the user's credentials are decrypted using the old password or key, and re-encrypted using the new password or a key derived from the new password.

This integration may be characterized as follows:

Strengths	Weaknesses
<ul style="list-style-type: none"> Seamless password reset, which does not invalidate E-SSO credentials. Easy for E-SSO software installers to implement, because it does not require new skills for direct integration with target systems. 	<ul style="list-style-type: none"> E-SSO deployment continues to be challenging. Users cannot access dual-interface applications from a web browser, because they do not know their own passwords.

7.2 Full Integration: Automated Enrollment of E-SSO Credentials

A more comprehensive integration involves deploying both password synchronization and E-SSO, and updating individual passwords in the E-SSO's credential database after each successful password change / synchronization.

This integration may be characterized as follows:

Strengths	Weaknesses
<ul style="list-style-type: none"> Significantly reduces the work required to deploy the E-SSO system, because the credential database can be automatically pre-built. Users can access dual-interface applications from a web browser, because they do know their own synchronized password. 	<ul style="list-style-type: none"> Requires more platform-specific skills from software installers, who must understand how to integrate the password synchronization system directly with target systems.

8 Summary

Password synchronization and single sign-on address the same business problem: password complexity leading to cost, productivity and security issues.

Both approaches to this problem have their strengths and weaknesses:

- Password synchronization is relatively easy to deploy, because it is architecturally unintrusive, and requires relatively little new user profile data. With password synchronization, users must still sign into each application separately.
- Enterprise single sign-on is more costly to configure because it requires client software and a credential database. With E-SSO, the number of times that users must sign into password-protected systems is significantly reduced.

Independent password reset and enterprise single sign-on products conflict, because user credentials in the E-SSO are encrypted with a key derived from the user's current password. That password is lost in a password reset process, so the credentials are invalidated.

Independent password synchronization and enterprise single sign-on products conflict, because new passwords are not reflected in the user's credential database after a password change.

Integration between a password reset and synchronization system and an enterprise single sign-on system eliminates these conflicts, and allows enterprises to combine the benefits of rapid deployment, reduced sign-on and self-service problem resolution.