

Hitachi ID Password Manager

Deployment Best Practices



Contents

1	Introduction	1
2	Project objectives	2
3	Stake-holders	4
3.1	System administrator	5
4	Design features	6
4.1	Features	6
4.2	Accessibility	8
4.3	Password policy	12
4.4	Security equivalence in authentication	13
4.5	Authentication process using challenge-response	14
4.6	Integration	16
5	Technical architecture	19
5.1	Overview	19
5.2	Server configuration	21
5.3	Locking down servers	23
5.3.1	Operating system	23
5.3.2	Web server	26
5.4	Multiple servers, load balancing and high availability	28
5.5	Network utilization and server location	29
5.6	Proxy servers	30
5.7	Backup and restore	30
6	Automatic discovery of login IDs	32
6.1	Selecting an authoritative system	32
6.2	When user IDs are consistent	32
6.3	Inconsistent login IDs	32
6.3.1	With an existing meta directory	32
6.3.2	With no pre-existing correlation	33
6.3.3	Automated correlation	33

7	User enrollment	34
8	Maximizing adoption rates	37
8.1	User education	37
8.2	Incentives for registration	37
8.3	Forced enrollment	37
8.4	Registration during assisted service	38
8.5	Incentives for utilization	38
8.6	Adjusting response time with assisted service	38
8.7	Plan for user adoption	38
9	Measuring value	39
9.1	Measuring activity	39
9.2	Trend analysis	39
9.3	User productivity	39
9.4	Support cost	40
10	Ongoing administration and support	41
10.1	Functional test	41
10.1.1	Password changes	41
10.1.2	Transparent password synchronization	41
10.1.3	Help desk logins	41
10.1.4	Directory integration	41
10.1.5	Sending e-mails	41
10.1.6	Creating call tracking system ticket	42
10.1.7	IVR integration	42
10.1.8	User registration	42
10.2	Changes to target system configuration	42
10.3	Monitoring service health	43
10.4	Monitoring the pushpass service	43
10.5	Monitoring transparent synchronization on Windows servers	43
10.6	Monitoring utilization	44
10.7	Randomizing target system credentials	44

10.8	Making backups	44
10.9	Purging old Q&A data	44
11	Summary	45

1 Introduction

This document outlines best practices for designing, installing and rolling out the Hitachi ID Password Manager password management solution in a medium to large organization.

The remainder of this document is organized as follows:

- **Project objectives**
Clearly identifying the goals of a project which will deploy password management technology.
- **Stake-holders**
Who to involve in the project and when.
- **Design features**
How to approach project design and recommended design choices.
- **Technical architecture**
Recommendations for a network architecture, for server configuration, etc.
- **Automatic discovery**
Where and how data can be automatically loaded into the password management system, to minimize ongoing administration.
- **User education and enrollment**
How to inform users about the system and whether / how to prompt users to register personal information.
- **Maximizing adoption rates**
Strategies to ensure how utilization, to maximize the value of the system.
- **Measuring value**
How to measure the value of the system.
- **Ongoing administration**
Overview of how to manage the deployed technology and how to gradually expand the system's functionality and value.
- **Summary**

2 Project objectives

A password management system is generally intended to deliver three benefits:

- **Improved service to users:**

This is due to fewer passwords to remember, a simpler password change mechanism and faster resolution of password and intruder lockout problems.

- **Reduced cost to the I.T. support organization:**

This is due to reduced help desk calls for password reset, faster resolution of remaining calls and reduced escalation of login problems.

- **Stronger authentication:**

This is due to stronger and more consistent password policy enforcement, more robust authentication of users who forgot their passwords and enforced password expiry across all systems.

At the start of a password management project, it is important to quantify (i.e., set metrics for) the existing problems with password management and set out goals for improved service, cost and security.

A project mission statement, listing current problems and how they will be solved, can be laid out in a table such as the following:

Password management project objectives

	Current problem	Planned improvement
User service	Each user has to manage 8 different passwords, on average.	With password synchronization, users will only have to manage 2 passwords.
	Only some passwords expire and they do so on individual schedules.	Users will be prompted to change every password at once.
	Different systems enforce different password policy rules.	A new, global password policy will be applied to all systems.
Help desk cost	30% of total call volume is due to login/password problems.	Password synchronization and self-service reset will reduce the problem rate by at least 80%.
	A password call takes 10 minutes to resolve (authenticate caller, create ticket, login to administration tool, reset password, close ticket).	Password problem resolution will be streamlined with a single web interface and be reduced to 2 minutes/call.
Security / quality of authentication	Users have too many passwords and write them down.	Synchronization will eliminate the main user motivation for writing down passwords.
	Each system has a different and possibly inadequate password policy engine.	Password Manager will enforce a single, global, strong password policy.
	Users who call the help desk for assistance with passwords may not be properly authenticated.	Most users will use self-service, with strong authentication built-in. Password Manager will also enforce a new authentication process that requires help desk analysts to enter user responses to profile questions before they can reset a user's password.
	Password resets are not properly logged on all systems.	Password Manager will record who made each password reset, on which system, for which user.
	Too many (front line) support staff have administrative credentials, required to make password resets.	Support staff will reset passwords through Password Manager and their administrative access will be removed.
	Support staff reset passwords on some systems to which they connect using plain-text network protocols.	All new password updates will be through Password Manager, over HTTPS. Communication between Password Manager and managed systems will be protected in all cases – in some cases physically and in other cases cryptographically.

3 Stake-holders

A password management system may affect corporate security, network operating systems, managed servers, call tracking systems and e-mail.

It is important to get buy-in from every stake-holder early in the project. Failure to get early agreement from every stake-holder will result in project delays and may put successful project completion at risk.

An empowered project sponsor is essential to get buy-in from a diverse group of stake-holders. Because of the large number of project participants, it is almost inevitable that somebody will be reluctant to cooperate, assist or approve projected-related changes. A high profile project sponsor will reduce the project risk due to such minor disagreements.

The following stake-holders should be involved in the project at the earliest possible date. Stake-holders should be made aware of the project's objectives, as documented in [Section 2](#) on [Page 2](#) as early as possible.

Stake-holder	Role in the password management project
Project sponsor	Provide mandate and budget for the project. Ensure cooperation from other stake-holders.
Project manager	Ensure that the project is managed effectively.
Software installer / administrator	Installs as many components of the password management system as possible and manages the system when in production.
I.T. security officer	Review, document and approve any changes that impact corporate security, including new login IDs, server configuration and location, password policy, non-password authentication rules, security incident response, approved access channels (web, SKA, IVR), etc.
Owner, system administrator of the help desk call tracking system	Specify integration with the help desk call tracking system, both at the business requirements and at the field/value levels of detail.
Owner, administrator of every system where passwords will be managed	Validate integration process with each managed system, create administrative credentials for use by the system and assist with software installation and testing of password management on that system.
Owner of the corporate Intranet	Provide user interface standards, possibly implement GUI localization, and validate compliance with Intranet standards.
Representative, network infrastructure	Manage production server installation, connectivity, backup services, server health monitoring, load balancing.
Representative, desktop deployment	Evaluate the impact on desktops, either of the kiosk account or (in unusual cases) of any software deployed to the desktops.
Representative, user education	Prepare and/or validate user education documents.

3.1 System administrator

Each Hitachi ID Password Manager installation should have a Password Manager software and server administrator. Following is a recommended skill-set for this person:

- Administration of Windows 2003 servers.
- Administration of web servers, preferably running the same web server software (IIS, Apache, etc.) as deployed on the Password Manager servers.
- Ability to write and troubleshoot HTML and CSS markup (i.e., not just ability to use a graphical web design program, but a good understanding of HTML and CSS coding).
- Familiarity with as many as possible of the platforms where Password Manager will manage passwords.
- Practical experience with systems that will trigger transparent password synchronization, or where Password Manager will poll for password expiration, or where a secure kiosk account will be installed. Note: these three are usually just one: Windows/AD.
- Experience with TCP/IP networking.
- Experience with directory services (LDAP, AD, NDS, etc.).
- Familiarity with any help desk call tracking system with which Password Manager will be integrated.

4 Design features

The first step in a password management system deployment is to specify what processes it will implement. All stake-holders must sign off on a design, preferably in writing.

Following is a list of features and policies that Hitachi ID recommends as best practices, along with justification for each one.

4.1 Features

- **Synchronize passwords**

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.

One of the core features of Hitachi ID Password Manager is password synchronization.

Password Manager implements both transparent and web based password synchronization.

- **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 Password Manager from Hitachi ID Systems is self-service password reset.

• **Assisted password reset**

Password Manager includes an assisted password reset console, which allows IT support staff to help callers without having direct administrative access to target systems:

- Help desk analysts sign into Password Manager with a web browser.
- Analysts can be authenticated using IDs and passwords internal to Password Manager or use pass-through authentication to an existing system.

For example, help desk analysts may sign into Password Manager using their Active Directory ID and password, with Password Manager validating the membership of each analyst in a designated AD security group and granting appropriate Password Manager privileges based on that group membership.

- From the Password Manager web interface, analysts can search for the caller's profile by login ID or full name.
- Analysts can be required to authenticate the caller – for example by keying answers to some of the user's personal questions, which Password Manager can validate against its own back-end database or an external database, directory or web service.

Note that the same, different or overlapping security questions can be used for assisted and self-service authentication processes.

- Once both the analyst and caller have been authenticated, analysts can reset the caller's password, lock or unlock the caller's access to Password Manager or update the caller's profile. Assisted password resets may be configured to also expire the new password, requiring the user to change it on the next login.
- All transactions – analyst login, user profile lookup, successful or failed password reset and more may trigger e-mails to the user, to the analyst or to a third party, such as a security officer. The same events can also trigger automatic creation, update or closure of tickets in an incident management system.
- Since only a single, simple web interface is used, an assisted password reset is normally completed in 1–2 minutes.
- User-filter and account-filter plug-in points are available, making it possible to delegate password reset capabilities to managers, platform administration groups and regional help desks and to ensure that such groups get only appropriate password reset and user profile lookup privileges.
- At no point in the process does an analyst require administrative access to the systems where passwords are being reset. Instead, Password Manager uses its own credentials to sign into target systems and these are encrypted in an internal Password Manager database.

Assisted password reset reduces the cost of password support calls and ensures that such calls are uniformly processed in a consistent, secure fashion.

• **SecurID token management**

Organizations that have RSA SecurID tokens should allow users to clear or reset their PINs, resynchronize token clocks with the ACE server and enable/disable their own tokens. All of this should be accessible in a self-service facility, with password authentication.

There is no security impact to the above – PIN resets in particular substitute one secret (a user's password) for another (the same user's PIN).

Support analysts should be able to perform the same functions, after a reliable caller authentication process. Some organizations may also allow empower staff to issue emergency access numbers for users who misplaced their token and need access to infrastructure protected by token authentication.

Enabling self-service access to emergency pass codes reduces the security of tokens from two factor (hardware + PIN) to one factor (the password used to access self-service). This feature should only be enabled if token security can be safely reduced to password security.

4.2 Accessibility

To maximize user adoption rate, a password management system, and self-service password reset in particular, must be made available to users regardless of their location and situation:

- **Managing passwords from a web browser**

All users should be able to access routine password changes (authenticated with a current password) and self-service password reset from a web browser.

Most organizations will make this facility accessible only from inside the corporate network. Organizations with large numbers of mobile or external users may also expose this facility on their Extranet. Extranet access to Hitachi ID Password Manager is normally provided through a reverse web proxy, where users access HTTPS content on the proxy, which fetches the actual pages from a Password Manager server in a protected subnet.

- **Assisting locked out users**

Users often forget their initial network login password or inadvertently trigger an intruder lockout. These users should be able to get assistance, reset their network or local password, clear intruder lockouts and get back to work.

Since these users have a problem with their workstation login, they cannot access a conventional web browser or client/server application with which to resolve their problem. The problem these users face is how to get to a user interface, so that they can fix their login problem and subsequently access their own workstation desktop.

This problem is especially acute for mobile users, who use cached domain passwords to sign into their workstation and who may not be attached to the corporate network when they experience a forgotten password problem.

When users forget or lock out their primary password, they are in a Catch-22 situation: they cannot log into their computer and open a web browser but cannot open a web browser to fix their password and make it possible to log in.

Password Manager includes a variety of mechanisms to address the problem of locked out users. Each of these approaches has its own strengths and weaknesses, as described below:

	Option	Pros	Cons
1	Do nothing: <i>users continue to call the help desk.</i>	<ul style="list-style-type: none"> • Inexpensive, nothing to deploy. 	<ul style="list-style-type: none"> • The help desk continues to field a high password reset call volume. • No solution for local passwords or mobile users.
2	Ask a neighbor: <i>Use someone else's web browser to access self-service password reset.</i>	<ul style="list-style-type: none"> • Inexpensive, no client software to deploy. 	<ul style="list-style-type: none"> • Users may be working alone or at odd hours. • No solution for local passwords or mobile users. • Wastes time for two users, rather than one. • May violate a security policy in some organizations.
3	Secure kiosk account (SKA): <i>Sign into any PC with a generic ID such as "help" and no password. This launches a kiosk-mode web browser directed to the password reset web page.</i>	<ul style="list-style-type: none"> • Simple, inexpensive deployment, with no client software component. • Users can reset both local and network passwords. 	<ul style="list-style-type: none"> • Introduces a "generic" account on the network, which may violate policy, no matter how well it is locked down. • One user can trigger a lockout on the "help" account, denying service to other users who require a password reset. • Does not help mobile users.
4	Personalized SKA: <i>Same as the domain-wide SKA above, but the universal "help" account is replaced with one personal account per user. For example, each user's "help" account could have their employee number for a login ID and a combination of their SSN and date of birth for a password.</i>	<ul style="list-style-type: none"> • Eliminates the "guest" account on the domain, which does not have a password. 	<ul style="list-style-type: none"> • Requires creation of thousands of additional domain accounts. • Requires ongoing creation and deletion of domain accounts. • These new accounts are special – their passwords do not expire and would likely not meet strength rules.

	Option	Pros	Cons
5	<p>Local SKA: Same as the domain-wide SKA above, but the “help” account is created on each computer, rather than on the domain.</p>	<ul style="list-style-type: none"> • Eliminates the “guest” account on the domain. • Can be configured to assist mobile users who forgot their cached domain password (by automatically establishing a temporary VPN connection). 	<ul style="list-style-type: none"> • Requires a small footprint on each computer (the local “help” account.)
6	<p>Telephone password reset: Users call an automated system, identify themselves using touch-tone input of a numeric identifier, authenticate with touch-tone input of answers to security questions or with voice print biometrics and select a new password.</p>	<ul style="list-style-type: none"> • Simple deployment of centralized infrastructure. • No client software impact. • May leverage an existing IVR (interactive voice response) system. • Helpful for remote users who need assistance connecting to the corporate VPN. 	<ul style="list-style-type: none"> • New physical infrastructure is usually required. • Users generally don’t like to “talk to a machine” so adoption rates are lower than with a web portal. • Does not help mobile users who forgot their cached domain password. • Does not help unlock PINs on smart cards.
8	<p>Physical kiosks: Deploy physical Intranet kiosks at each office location.</p>	<ul style="list-style-type: none"> • Eliminates generic or guest accounts. • May be used by multiple applications that are suitable for physically-present but unauthenticated users (e.g., phone directory lookup, badge management, etc.). 	<ul style="list-style-type: none"> • Costly to deploy – hardware at many locations. • Does not help mobile users who forgot their cached domain password. • Users may prefer to call the help desk, rather than walking over to a physical kiosk.
9	<p>GINA DLL: Windows XP: Install a GINA DLL on user computers, which adds a “reset my password” button to the login screen.</p>	<ul style="list-style-type: none"> • User friendly, intuitive access to self-service. • Can be configured to assist mobile users who forgot their cached domain password (by automatically establishing a temporary VPN connection). • Works on Windows Terminal Server and Citrix Presentation Manager. 	<ul style="list-style-type: none"> • Requires intrusive software to be installed on every computer. • Broken installation or out-of-order un-installation will render the computer inoperable (i.e., “brick the PC”).

	Option	Pros	Cons
10	GINA Extension Service: <i>Similar to the GINA DLL, but uses a sophisticated service infrastructure to modify the UI of the native GINA, rather than installing a GINA DLL.</i>	<ul style="list-style-type: none"> • User friendly, intuitive access to self-service. • Can be configured to assist mobile users who forgot their cached domain password (by automatically establishing a temporary VPN connection). • More robust, fault-tolerant installation process than the GINA DLL. 	<ul style="list-style-type: none"> • Requires software to be installed on every computer. • Does not work on Citrix Presentation Server or Windows Terminal Server – only works on personal computers.
11	Credential Provider: <i>The equivalent of a GINA DLL, but for the login infrastructure on Windows 7 and Windows Vista.</i>	<ul style="list-style-type: none"> • User friendly, intuitive access to self-service. • Can be configured to assist mobile users who forgot their cached domain password (by automatically establishing a temporary VPN connection). • Works on Windows Terminal Server and Citrix Presentation Manager. • More robust infrastructure than GINA DLLs on Windows XP. 	<ul style="list-style-type: none"> • Deployment of intrusive software to every workstation.

No other product or vendor supports as many options for assisting locked out users.

The solution(s) that will be deployed to assist locked out users must be selected and appropriate change control and infrastructure must be provided for.

• **Telephone access to password reset**

Users at home, traveling, or who frequently work at locations outside the corporate network may have problems with the passwords they use to connect to the corporate network.

These users benefit from access to self-service password reset on an IVR system. Such a system allows a traveling worker to reset his RAS password from a hotel room, for example.

IVR access to self-service password reset should be enabled whenever the number of users who have problems with network-connection passwords (RAS, VPN) is significant.

Users who forget their passwords can dial an IVR system with any telephone and initiate a password reset. Authentication using either touch-tone entry of personal secret information or using voice print verification is supported. Existing IVR systems can be extended using a Password Manager remote API (application programming interface) or Hitachi ID Telephone Password Manager – a turn-key IVR system specifically designed for password resets.

4.3 Password policy

Hitachi ID Password Manager is normally configured to enforce a uniform password policy across all systems, to ensure that any new password will be acceptable to every integrated system. This provides the most clear and understandable experience to users. Password Manager is configured such that it will never accept or attempt to propagate a password that will not meet this global password policy.

For instance, in the case of an organization that has both Windows Active Directory (AD) and z/OS passwords, where users may enter very long passwords on AD but only 8 characters on the (older) mainframe, Password Manager can require that passwords be exactly 8 characters long. Alternately, Password Manager can support longer passwords, but truncate them when it updates the mainframe. (Users generally prefer the preset length rule, as it is easier to understand than automatic truncation).

In general, systems enforce one of two types of password rules:

- Complexity requirements ensure that users do not select easily-guessed passwords. Example rules are: disallowing any permutation of the user's login ID, password history, requiring mixed letters and digits, forbidding dictionary words, etc.
- Representational constraints limit what can be physically stored in a password field on a given system. Usually there are just two such rules: maximum length and allowable character set.

A global password policy is normally created by combining and strengthening the best-of-breed complexity requirements from each system affected by the policy. Password Manager then combines these with the most restrictive representational constraints. This forces users to select strong, secure passwords on every system.

The alternative, of defining different password policies for every target system or for groups of target systems, is considered to be user-unfriendly. To update their passwords, users must select a system, choose a password, wait for the password update to complete, possibly re-authenticate, choose another system, choose a different password, etc. Users must then remember multiple passwords and will continue to experience many password problems. It has been shown that users with many passwords have a strong tendency to write down their passwords.

The recommended global password policy depends on the system with the most restrictive representation rules. In many large organizations, this is an OS390 (zOS, MVS) mainframe, which only supports 8-character passwords, composed of letters, digits and three "special" characters (@, #, \$).

- **For organizations with a mainframe**
 - Length: 7 or 8 characters.
 - Characters: at least 2 letters, at least 1 digit, specials must be @, # or \$.
 - Special words: no dictionary word, login ID or permutation thereof.
 - Repeats: no more than 1 pair of repeating characters.

There are 39 possible characters in a password (letters, digits, 3 specials).

Note: the total search space is $39^7 + 39^8 = 5,489,240,267,160$ possible passwords.

- **For organizations without a mainframe**

- Length: 7 or more characters.
- Characters: at least 2 letters, mixed case, at least 1 digit.
- Special words: no dictionary word, login ID or permutation thereof.
- Repeats: no more than 1 pair of repeating characters.

There are 94 possible characters in a password (lowercase, uppercase, digits, 32 symbols on a US keyboard).

Note: the total search space is no less than $94^7 = 64,847,759,419,264$ possible passwords.

Password policy must be enforced on both the Password Manager server and each of the managed systems. Ideally, each managed system should enforce the largest possible subset of the policy rules enforced on the Password Manager server. In cases where a managed system initially had a rule that conflicts with the new global policy (i.e., it is impossible to compose a password that is simultaneously compatible with both the old native policy and the new global policy), the native policy should be adjusted to be compatible.

Password policy must not be disabled on any existing system, as this would allow users to bypass policy by making native password changes, without Password Manager.

Password policy must not be disabled on the Password Manager server, as this would allow users to bypass policy by making password changes using Password Manager, whose password resets are not subject to policy rules on most systems.

4.4 Security equivalence in authentication

Password synchronization makes the security of managed systems equivalent, in the sense that if an intruder can compromise one password, the intruder can infer the value of the same user's passwords on other systems.

Password reset services (both self-service and assisted) make passwords equivalent to the non-password authentication used to validate users who forgot their passwords.

If password reset services rely on users answering personal questions, and if the answers to those personal questions are collected in a registration process, then both the subsequent Q&A authentication and the passwords that can be reset with that authentication are made equivalent to the authentication used to initially register Q&A data.

To ensure that authentication is reliable, the above points lead to some basic design requirements:

- Password synchronization should be based on the use of strong, frequently-changing passwords.
- Password synchronization should not include systems with very weak security infrastructure (e.g., systems that store password in plain-text, or that have no intruder lockout mechanism triggered by repeated failed authentication attempts).

- Self-service password reset should use strong authentication, such as hardware tokens or biometrics, if possible.
- Where self-service password reset relies on a challenge-response process, users should be prompted to answer as many different questions as possible.
- It is acceptable to authenticate users to fill in challenge-response (Q&A) data using an existing password.
- It is **not** acceptable to authenticate users to fill in challenge-response with something weaker than a current password – such as a PIN, an employee number, or a date of birth.
- Help desk analysts should use a process to authenticate callers which is just as strong as a self-service system. While this may mean asking the caller the same questions that a self-service password reset system would ask its user, privacy legislation may mean that multiple, equally-strong Q&A profiles are required for each user.

4.5 Authentication process using challenge-response

As mentioned above, a password reset process makes the security of password authentication equivalent to the security of non-password authentication. This means, for example, that there is no sense in enforcing a strong password policy if users are authenticated to a password reset system with a 5 digit PIN, such as the last part of a social security number.

In most organizations, hardware tokens are not widespread enough to use as the sole means for non-password authentication. Both hardware tokens and biometric identification systems can be costly, especially in comparison to passwords. In the absence of such strong authenticators, non-password authentication normally means use of a challenge-response process to validate the identity of users.

Since password reset is provided to users who forgot their password, it makes sense to use information that users will not forget. In particular, it is not reasonable to use yet another password to authenticate users to a password reset system: if they forget the password they use daily, they are unlikely to remember a password that was assigned to them months or years in the past, which they have never used since. By the same argument, Q&A data used for non-password authentication should be static, factual and memorable. Avoid questions whose answers may change over time, such as “what is your favorite movie?”

Some additional recommendations for challenge-response authentication:

- **Combine free-form and pre-defined Q&A**

From the above, it is clear that Q&A authentication data must consist of static characteristics of the user. Questions such as SSN, mother’s maiden name, city of birth, etc. are appropriate. Since answers to such questions may be vulnerable to social engineering attacks, it makes sense to use as many questions as feasible and to combine pre-defined questions with user-entered ones.

- **Privacy**

Users are authenticated to a password reset system by answering questions that only they should know. Such questions are frequently personal and may be protected by privacy regulations in some jurisdictions.

If privacy protection legislation applies in a given jurisdiction, it may be necessary to define two sets of questions that users may be asked to answer: one set that applies to self-service authentication, to which privacy legislation does not apply, and a second set that will be used by I.T. support analysts, which does not contain sensitive personal information.

- **Sample pre-defined questions**

Some oft-used questions that users are asked to answer during registration and which may then be used to authenticate users include:

Sample security questions, which may have alpha-numeric questions and so are suitable for a text user interface, include:

- Which bank branch do you live closest too?
- What car do you wish you owned?
- What is your favorite food?
- Who is your favorite book character?
- What is your favorite game or sport?
- What is your favorite movie?
- What is your favorite pizza topping?
- What is your favorite restaurant?
- What is your favorite season of the year?
- What is your favorite sports team?
- In which department did you first work?
- What was your first position in the company?
- What was your first car?
- Who is the person you admire the most?
- What was the most memorable day in your life?
- Who was your childhood hero?
- What is the nickname of your sibling?
- Who was your first boss?
- What award are you proudest of?
- What city were you born in?
- What is the farthest from home you have traveled?
- What is the name of the first school you attended?
- What is the name of the first person you were romantically interested in?
- What is your astrological sign?
- What is your father's middle name?
- What is your mother's middle name?
- Who is your favorite actor, actress or celebrity?
- What is your favorite musical band?
- What is your favorite beverage?
- What is your favorite board game?
- Who is your favorite book character?
- What is your favorite dessert?
- What is your favorite hobby or pastime?
- What is your favorite ice cream topping?
- What is your favorite song?
- What is your favorite television show?
- What is your favorite vacation spot?
- What is your mother's maiden name?
- What is your place of birth?

- What is your school team's mascot name?
- What was the breed of your first pet?
- What was the color of your first automobile?
- What were the make and model of your first car?
- What was the name of a favorite childhood pet?
- What was the name of your first girlfriend/boyfriend?
- What was the street name of your childhood home?
- What was your favorite toy when you were a child?
- What did you do on your first job?
- What was your first phone number as a child?
- What year did you purchase your first car?
- What was the name of your first pet?
- Who is your favorite politician?
- Who is your most disliked politician?
- Who is a famous, living person you would most like to meet?
- Who was a famous, now deceased person you would have liked to meet?
- Who is your favorite artist?
- Who is your favorite author?
- With whom did you share your first romantic kiss?
- Who was your favorite elementary school teacher?

- **Authentication process**

To ensure that authentication data is of good quality, users should be required to provide answers to some standard questions, where the questions were selected to ensure that they are relatively difficult to "socially engineer."

The Q&A process should be protected by an "intruder lockout" security feature, so that repeated failed attempts to authenticate as a given user trigger lockout of that user's profile and possibly a security alarm.

The limitation of pre-defined questions is that there are only a finite number of possible questions. An intruder could readily discover what those questions are and research answers to every possible question ahead of time. A determined intruder would not be caught by an intruder lockout mechanism.

To overcome this difficulty, a challenge-response system should combine both pre-defined questions (where the difficulty of guessing answers can be estimated) with user-defined questions (where the questions themselves are harder to guess, but the answers may be easier for an intruder to come by). The user-defined questions should only be presented to a user attempting authentication after the standard questions have been successfully answered.

While user-defined questions are not guaranteed to be hard to guess, they are less predictable than standard questions and make social engineering attacks significantly more difficult.

4.6 Integration

A password management system obviously integrates with the systems on which it can set user passwords.

Password management systems frequently also integrate with other I.T. infrastructure. A description of different types of integrations and when they are appropriate, follows:

System	Integration process	When to activate
E-mail system	Prompt users to register.	Whenever user registration is required (see Section 7 on Page 34).
	Notify users of changes to their passwords or profiles	This is recommended in every organization where the majority of users access e-mail.
H.R. system	Access existing Q-A data for authentication.	Whenever the password management system provides password reset to users (self-service) or analysts, and the existing data is adequate (covers most users, is reliable and sufficiently hard to guess).
Call tracking system	Write tickets to reflect ongoing activity. Closed tickets are purely for utilization monitoring, open tickets are to escalate technical or security problems.	Appropriate if an organization relies on the help desk call tracking system to meter support activity.
Directory / meta directory.	Look up on what systems a user has login IDs, and what those IDs are.	Appropriate if a directory already exists and has this data.
	Access existing Q-A profile data.	As with H.R. systems above.
	Write login ID correlation data into a meta directory.	Appropriate when Password Manager deployment precedes meta directory installation, and login ID correlation is difficult with existing data in the directories being connected. Note: this leverages self-service registration of login IDs in Password Manager to populate a meta directory (subsubsection 6.3.2 on Page 33).

System	Integration process	When to activate
NOS / login scripts	Automatically prompt users to change their passwords with the Password Manager web GUI during the network login process.	Works well for primarily-NetWare environments, where transparent synchronization triggered from Novell password changes is not possible.
NOS / security policy	Secure Kiosk Account (SKA) allows users to access self-service password reset by logging into the network as “help” with no password.	Useful for any organization that deploys self-service password reset to a population of users who are primarily network-attached at the time of first login, and whose workstations are members of a login domain (Windows, NetWare, NIS, etc.).
IVR server	Self-service password reset using a telephone, with either challenge-response authentication (numeric responses keyed on a touch tone phone), or biometric voice print verification.	Appropriate when a significant fraction of password resets are due to people who have a problem with the password they type to establish a RAS connection.
Token authentication system	Authenticate to self-service password reset with a token.	This is better than Q-A – appropriate if tokens are widely deployed.
	Manage tokens	Only available for SecurID tokens – appropriate if there are many SecurID hard or soft tokens deployed.

5 Technical architecture

5.1 Overview

Hitachi ID Password Manager is designed for:

- **Security:**

Password Manager is installed on hardened servers. All sensitive data is encrypted in storage and transit. Strong authentication and access controls protect business processes.

- **Scalability:**

Multiple Password Manager servers can be installed, using a built-in data replication facility. Workload can be distributed using any load-balancing technology (IP, DNS, etc.). The end result is a multi-master, distributed architecture that is very easy to setup, as replication is handled at the application layer.

- **Performance:**

Password Manager uses a normalized, relational and indexed database back end. All access to the database is via stored procedures, which help to minimize communication overhead between the application and database. All Password Manager code is native code, which provides a 2x to 10x performance advantage as compared to Java or .NET

- **Openness:**

Open standards are used for inbound integration (SOAP) and outbound communications (SOAP, SMTP, HTTP, etc.).

- **Flexibility:**

Both the Password Manager user interface and all functionality can be customized to meet enterprise requirements.

- **Low TCO:**

Password Manager is easy to set up and requires minimal ongoing administration.

Figure 1 on Page 20 illustrates the Password Manager network architecture:

- Users normally access Password Manager using HTTPS from a web browser.
- Multiple Password Manager servers may be load balanced using either an IP-level device (e.g., Cisco Local Director, F5 Big/IP) or simply using DNS round-robin distribution.
- Users may call an IVR system with a telephone and be authenticated either using touch-tone input of personal information or using a voice print. Authenticated users may initiate a password reset.
- Password Manager connects to most target systems using their native APIs and protocols and thus requires no software to be installed locally on those systems.

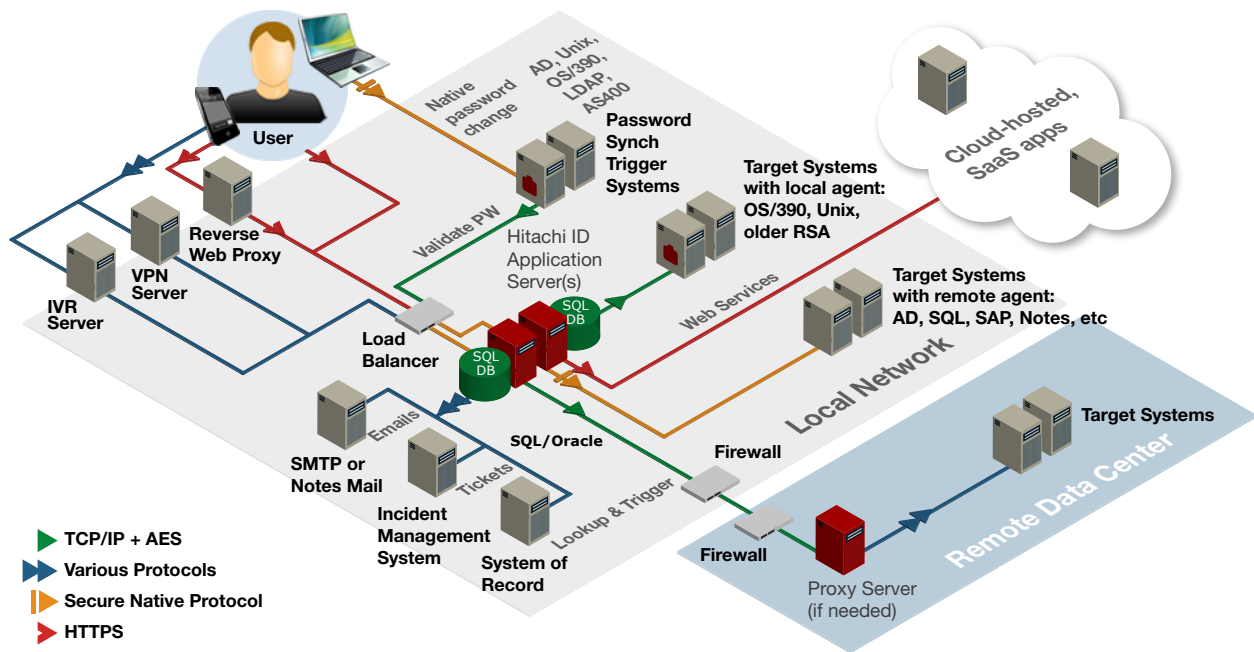


Figure 1: Network architecture diagram

- Local agents are provided and recommended for Unix servers and z/OS mainframes. Use of these agents improves transaction security, speed and concurrency.
- A local agent is mandatory on older RSA SecurID servers (version 7.x and later exposes a remote API).
- Where target systems are remote and communication with them is slow, insecure or both, a Password Manager proxy server may be co-located with the target system in the remote location. In this case, servers in the main Password Manager server cluster initiate fast, secure connections to the remote proxies, which decode these transactions and forward them to target systems locally, using native, slow and/or insecure protocols.
- Password Manager can look up and update user profile data in an existing system, including HR databases (ODBC), directories (LDAP) and meta-directories (e.g., WMI to Microsoft ILM).
- Password Manager can send e-mails to users asking them to register or to notify them of events impacting their profiles. Over 189 events can trigger e-mail notification.
- Password Manager can create tickets on most common incident management systems, either recording completed activity or requesting assistance (security events, user service follow-up, etc.). Over 189 events can trigger ticket generation. Binary integrations are available for 16 help desk applications and open integration is possible using mail, ODBC, SQL and web services.

5.2 Server configuration

A Hitachi ID Password Manager server is typically configured based on standards set out in the data center where it will be installed.

Each Password Manager server is configured as follows:

- Hardware requirements:
 - An Intel or AMD X86 CPU. Multi-core CPUs are supported and leveraged.
 - At least 4GB RAM – 8GB or more is typical for a server.
 - At least 100GB disk, preferably configured as RAID for reliability and preferably larger for retention of more historical and log data. More disk is always better, to increase log retention.
 - At least one Gigabit Ethernet NIC.

A virtual machine with similar specifications and resources allocated may also be used.

- Operating system:
 - Windows 2003 or Windows 2008 (or R2) Server with current service packs.
 - 32-bit or 64-bit versions are both acceptable.
 - The server should not normally be a domain controller.
- Installed and tested software on the server:
 - TCP/IP networking, with a static IP address and DNS name.
 - Web server (Apache/Windows or IIS or).
 - Client software: web browser, Acrobat reader (to read the manual) native clients for the systems that Password Manager needs to interface with.
 - SQL Server client or Oracle client to connect to the Password Manager database. Please note that the SQL or Oracle client must include 32-bit client libraries.
 - If the Password Manager database is local (reduces hardware cost; not recommended on a VM), then SQL Server or Oracle Database.
 - SSL server certificate, to support HTTPS connections to the web user interface and SOAP API.

Depending on which integrations are activated, some of the following client software packages may be required:

Table 3: List of Client Software

Target Integration	Client Software Used
Oracle	Oracle database client, including sqlplus
Sybase	Sybase ASE client, including isql
MS SQL	SQL client
IBM DB2	DB2 client
Informix	Informix client
Novell GroupWise	Novell GroupWise client
Lotus Notes ID file or HTTP/Domino	Lotus Notes R5 client
SAP	SAP GUI
Remedy ARS passwords	The appropriate Remedy ARS client
PeopleSoft	PeopleSoft External API
BMC Service Desk Express ticket creation	Service Desk Express Application Server
Remedy ARS ticket creation	The appropriate Remedy ARS client
HP Service Manager ticket creation	The appropriate Service Manager client

The file-system of the servers may be segmented as follows:

Password Manager Server Configuration

Disk volume	Contents	Size	Comments
C:	Operating System (Windows 2003 or 2008 server)	20 GB	Operating system files should be isolated and should have enough space for regular updates (patches, service packs etc.) ^a
D:	Password Manager Application, client software. ^b	80 GB or more	Table 3 describes some of the client software that may be necessary to either manage passwords on a given target type or create tickets in a given incident management system.
E:	Password Manager log files	80 GB	In case Password Manager log files become large, it is good practice to have them isolated from operating system and application files to prevent essential files from becoming corrupt.

^aThis is based on a 30 GB HDD. Additionally, if other software will be installed on the Password Manager server (e.g. Backup software, remote control software) then the required hard disk size may need to be increased.

^bThe Password Manager proxy server only needs client software installed if it is proxying connections of that particular type of target system. For example, to manage a Lotus Notes password or account via a Password Manager proxy server, the Lotus Notes client software must be installed on the Password Manager Proxy (and is not required on the Password Manager primary or secondary server.)

5.3 Locking down servers

The Hitachi ID Password Manager server houses sensitive data, including administrator credentials and in some cases private user profile information.

To protect this data, the Password Manager relies on host operating system and web server security measures, as well as sound application security features built directly into the software.

Following are instructions for locking down the host operating system and web server:

5.3.1 Operating system

The host operating system on the Hitachi ID Password Manager server should be locked-down and fully patched, as defined below:

Only the following services are required on Password Manager servers:

The following services, at most, are needed on the Password Manager server:

- DNS Client - Required to resolve host names
- Event Log - Core O.S. component

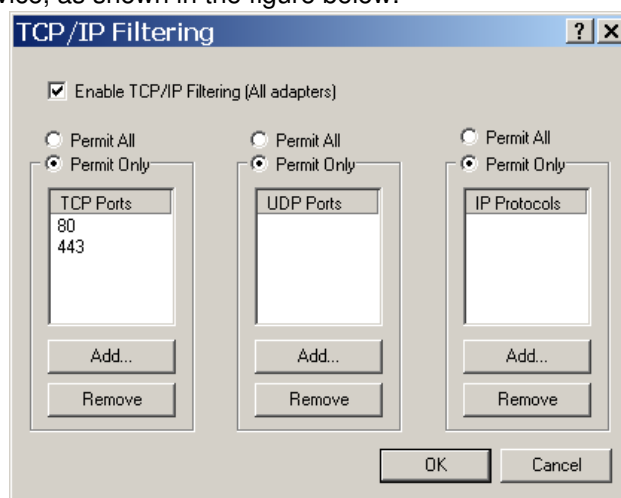
- IIS Admin Service - Only required if IIS is used
- IPSEC Policy Agent - Core O.S. component
- Logical DiskManager - Core O.S. component
- Network Connections - Required to manage network interfaces
- Plug and Play - Hardware support
- Protected Storage - Core O.S. component
- Remote Procedure Call (RPC) - Core O.S. component
- Removable Storage - Required to open CD-ROM drives
- RunAs Service - Core O.S. security component
- Security Accounts Manager - Core O.S. security component
- TCP/IP NetBIOS Helper Service - Only required if directly managing Windows 2000/2003/2008 passwords
- Workstation - Only required if directly managing Windows 2000/2003/2008 passwords
- World Wide Web Publishing Service - Only required if IIS is used

If additional services are required during implementation, then Hitachi ID Systems will notify customers.

All other services should be disabled unless there is some specific reason (not related to Password Manager) to enable them.

The Password Manager server should not be a member of any domains. This reduces the risk of a security intrusion in the domain being leveraged to gain unauthorized access to the Password Manager server.

Packet filtering should be enabled on the Password Manager server, to block all inbound connections other than those to the web service, as shown in the figure below:



A hardened Password Manager server can be port scanned to identify available services. Following is a typical port scan result, prior to Password Manager installation:

```
delli:/data/idan/vmware/win2ksrv# nmap -sT 192.168.100.8

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.100.8):
(The 1551 ports scanned but not shown below are in state: closed)
Port      State      Service
443/tcp   open      https

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
delli:/data/idan/vmware/win2ksrv# nmap -sU 192.168.100.8

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
All 1459 scanned ports on (192.168.100.8) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 91 seconds
```

The process table on the same server looks like this:

Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	99	0:29:58	16 K
System	8	00	0:00:26	208 K
smss.exe	160	00	0:00:01	344 K
csrss.exe	184	00	0:00:08	1,596 K
winlogon.exe	204	00	0:00:04	1,936 K
services.exe	232	00	0:00:03	3,696 K
lsass.exe	244	00	0:00:01	4,204 K
taskmgr.exe	312	01	0:00:00	1,664 K
svchost.exe	428	00	0:00:00	2,080 K
VMwareService.e	444	00	0:00:00	1,012 K
svchost.exe	472	00	0:00:01	3,016 K
inetinfo.exe	508	00	0:00:01	5,432 K
explorer.exe	672	00	0:00:10	2,116 K
VMwareTray.exe	744	00	0:00:00	1,204 K

Processes: 14 CPU Usage: 1% Mem Usage: 47828K / 4720

Note: VMWare entries reflect the fact that this sample was taken from a virtual machine.

This server was running with just the mandatory services described earlier.

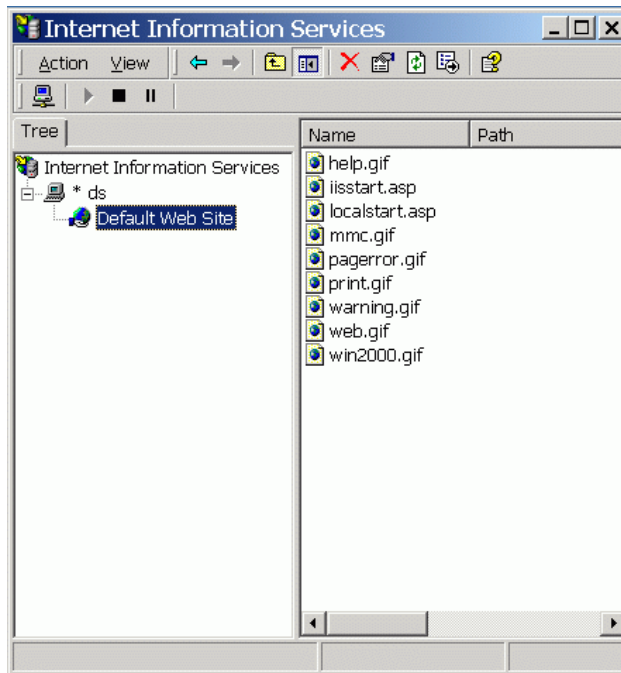
5.3.2 Web server

The web server is a required component, as it provides all user interface components. It should therefore be carefully protected.

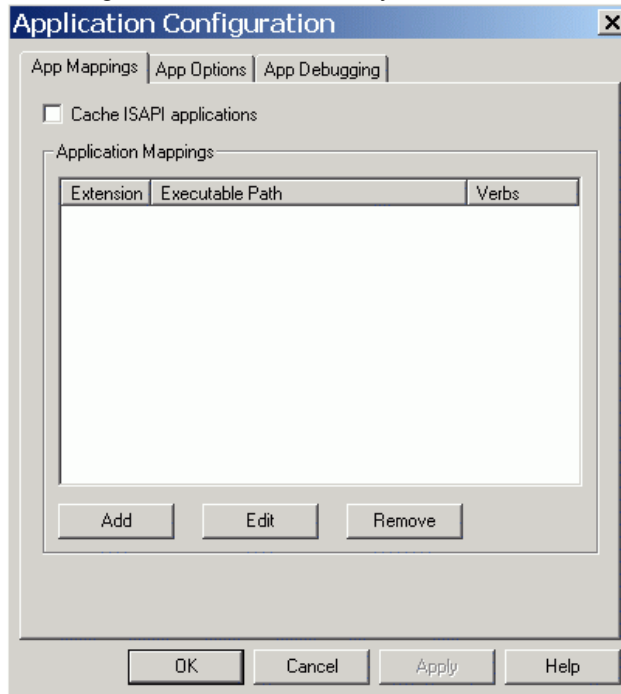
Since Hitachi ID Password Manager does not require any web server functionality beyond the ability to serve static documents (HTML, images) and to execute self-contained CGI executable programs, all non-essential web server content should be removed.

If Apache is used, all non-essential modules should be commented out of the configuration rules.

If IIS is used, this means removing IISAdmin, Printers, Scripts and similar folders, as shown below:



The web server's scripting, indexing and data access subsystems should likewise be removed:



As an extra precaution, remote data services are disabled by removing the following registry keys:

- HKLM
 - \System
 - \CurrentControlSet
 - \Services
 - \W3SVC
 - \Parameters
 - \ADCLaunch
 - \RDSServer.DataFactory

- HKLM
 - \System
 - \CurrentControlSet
 - \Services
 - \W3SVC
 - \Parameters
 - \ADCLaunch
 - \AdvancedDataFactory

- HKLM
 - \System
 - \CurrentControlSet
 - \Services
 - \W3SVC
 - \Parameters
 - \ADCLaunch
 - \BusObj.VbBusObjCls

ODBC drivers are also all disabled, both manually (remove data sources) and add this entry to the registry:

- HKLM
 - \Software
 - \Microsoft
 - \Jet
 - \4.0
 - \engines
 - \SandBoxMode = 3

5.4 Multiple servers, load balancing and high availability

Transparent synchronization in particular and password management in general, can produce high transaction bursts, which may necessitate a large processing capacity.

There is no advantage to building a very large single Hitachi ID Password Manager server, since the rate at which passwords can be set on a single system may depend on that system's load and capacity, as well as on client software, some of which are serialized. For example, the NetWare client only supports a single-threaded sequence of password resets.

Single threading clients that come with some managed systems, combined with high peak load and a requirement for high availability imply multiple load-balanced servers in a high-availability configuration.

Password Manager supports multiple servers, each of which is functionally identical and supports the same global user population. Load can be distributed between servers using DNS round-robin, or at the IP level with devices such as [F5 Big/IP](#) or [Cisco Local Director](#).

Password Manager includes technology to dynamically replicate data updates between multiple servers and to have one server monitor another server's health.

The number of servers in production should generally be at least 2, to provide for high availability. To determine whether more servers are needed, first find values for the following variables:

Variable	Description
<i>U</i>	The number of users who will synchronize passwords using Password Manager.
<i>A</i>	The average number of accounts per user.
<i>T</i>	The average number of seconds per password reset (assume 3 seconds if not sure.)
<i>Z</i>	The number of time zones in which users, whose passwords will expire, work. We assume that users are evenly distributed between time zones and that their passwords expire in the first hour of their workday.
<i>P</i>	The password expiry interval (e.g., 30 days).

There should be at least this many production servers to handle peak load:

$$1 + [U/P \times 7/5/Z \times A]/[60 \times 60 \times 5/T]$$

In addition to production servers, there should normally be one development server, used to stage and test upgrades and configuration changes.

To summarize: a typical organization requires three servers – two in production and one for development. Some organizations may require more servers in production, if they generate extremely high peak traffic.

A nice feature of Password Manager is that the development server can be switched into production and a production server can be switched into development. This makes upgrades fast and painless: develop on a test server until ready, then switch roles between the development and production master servers.

5.5 Network utilization and server location

As illustrated in [Figure 1](#), Hitachi ID Password Manager may be integrated with a broad range of existing network infrastructure.

User interaction with Password Manager is normally over HTTPS and is both light (requires little bandwidth) and tolerate of high latency.

Most Password Manager interaction with managed systems normally generates relatively little traffic. The sequence is normally login, reset password, logout. At night, Password Manager will generate a single larger burst of traffic to each managed system, to extract a list of user IDs from that system ([Section 6 on Page 32](#)).

Password Manager interaction with some managed systems and in particular with NOS servers and some applications may be sensitive to high latency connections.

The nightly user list and the sensitivity of some managed systems' native protocols to latency mean that Password Manager servers should be installed as close as possible to the largest possible number of managed systems.

Ideally, three servers should be rack mounted near one another: a master server, a slave server and a development server. Master and development will periodically exchange roles, after upgrades and configuration changes.

5.6 Proxy servers

In some cases, the connection to a target system may be slow, insecure or simply blocked by a firewall. This is often true when the connection is made over a wide area network or requires the use of an insecure protocol but must cross an untrusted network segment.

To address such connectivity problems, Hitachi ID Password Manager includes an application proxy server. When a proxy server is deployed, the main Password Manager server ceases to communicate with one or more (usually distant) target systems directly and instead forwards all communication to those systems through one or more proxy servers, which are co-located with the target systems in question.

Communication from the main Password Manager server to the proxy server(s) is encrypted, efficient and tolerant of high latency. It uses a single, arbitrarily-numbered TCP port number. Connections are strictly from the main Password Manager server to the proxy server (never back). A single TCP port supports an arbitrarily large number of target systems at the proxy server's location.

These characteristics of the communication between a Password Manager main server and a proxy server mean that firewall administrators will normally be willing and will always be technically able to route or forward a TCP port from the main server IP address to the proxy server IP address.

Communication between the proxy server and target systems continues to use native protocols. It is normally physically secured, in a high-bandwidth, low-latency, high-security data center network.

Deployment of the secure Password Manager proxy server is illustrated in [Figure 2](#).

5.7 Backup and restore

All Hitachi ID Password Manager software, configuration and data is normally stored on the file-system and in the registry of a single server.

The requirements for backing up Password Manager are:

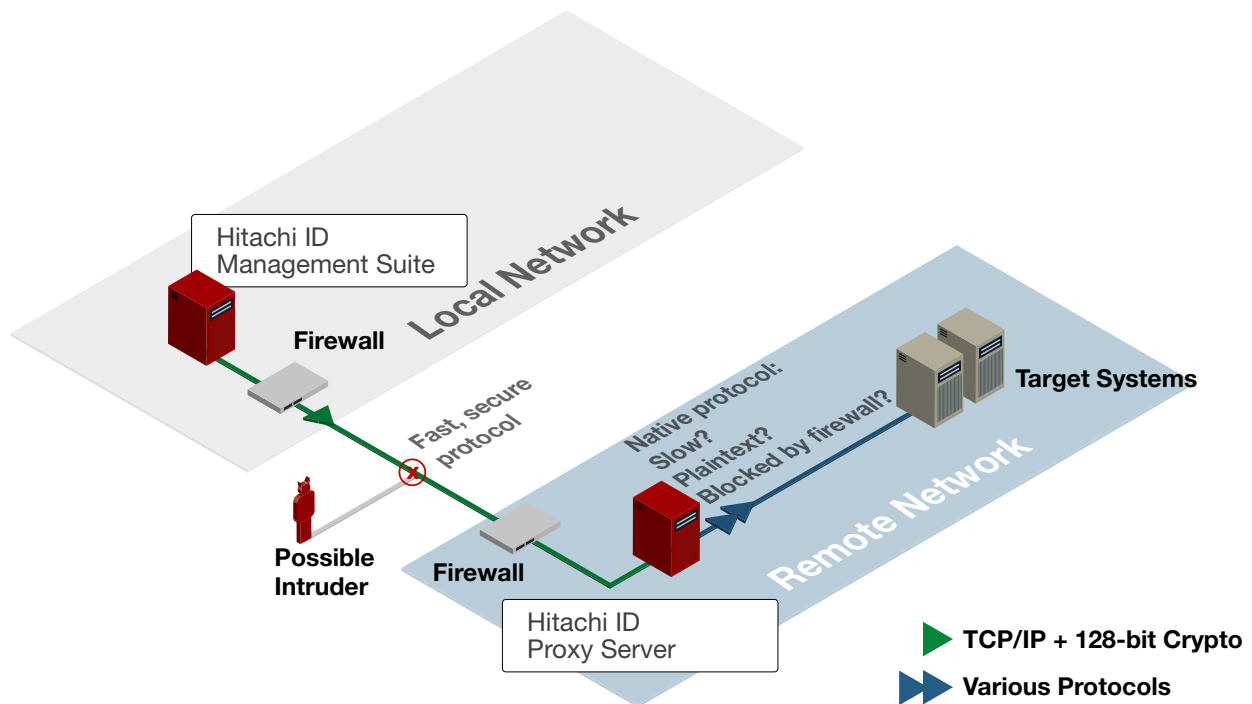


Figure 2: Target systems connected through a proxy server

- Do backup the entire file-system and registry.
- Do not place locks on the database files – which have DBF, FPT and CDX extensions, while Password Manager is running. These files are normally stored in a directory called `cgi-bin` and another directory called `treedb`.

This is normally done by scheduling a backup to run after the Password Manager nightly automation has completed, as that automation creates fresh copies of the same files in the `psupdate` directory and those files are not used thereafter. The backup then skips the same files in the `cgi-bin` directory.

If/when a restore is needed, just recover the file-system and registry onto a server with the same web service pre-installed. Re-run the nightly automation before bringing a restored server back into production.

6 Automatic discovery of login IDs

In most installations, Hitachi ID Password Manager fetches a full list of user IDs from every managed system, every night. This is intended to reduce or ongoing manual administration of Password Manager and in particular to eliminate any need to manually enroll, update or remove users from Password Manager.

6.1 Selecting an authoritative system

In most installations, Hitachi ID Password Manager is configured to “trust” one or more systems to be an authoritative source of Password Manager profile IDs. Any user who is added to an authoritative system will, during the auto-discovery process, be automatically added to Password Manager. Conversely, users removed from all authoritative systems will be automatically removed from Password Manager.

This process ensures that users do not have to be explicitly or manually enrolled in or removed from Password Manager.

Users sign into Password Manager with their login ID on the authoritative system.

Where there is no obvious authoritative system, e-mail addresses or employee IDs can be extracted from an existing system and used as the authoritative ID.

6.2 When user IDs are consistent

On systems that use login IDs consistent with the authoritative system, Hitachi ID Password Manager is configured to automatically correlate IDs. Users automatically see these login IDs in their profile.

6.3 Inconsistent login IDs

When users have inconsistent login IDs on different systems, their non-standard login IDs have to be associated with their authoritative login ID.

If the correlating data exists in any format before Hitachi ID Password Manager is deployed, then it should be used. Otherwise, correlating data must be acquired – and this is typically done by prompting users to register their own alternate login IDs with a web GUI.

6.3.1 With an existing meta directory

If a meta directory already exists, then Hitachi ID Password Manager can use it to retrieve login ID correlating data, either in real-time or in batch form.

In this case, no user registration of alternate login IDs is required.

6.3.2 With no pre-existing correlation

In environments where users have different login IDs on different systems and where there is no reliable method or data set to correlate different IDs back to individual users, Hitachi ID Password Manager can automatically prompt users to register and correlate their own login IDs.

Self-service login ID reconciliation is fast, inexpensive, secure and reliable. It significantly expedites system deployment in organizations where login IDs are different and cannot be automatically reconciled.

Self-service login ID reconciliation works as follows:

- Users are automatically prompted to fill in their profiles – for example by receiving an e-mail with an embedded URL.
- Users sign into the registration system, using a primary login ID and password or other types of credentials.
- Users are prompted to type their additional ID/password pairs. Each provided ID/password pair is compared against an automatically maintained inventory of login IDs drawn from target systems, to find instances where the user-entered login ID appears on a system and does not yet belong to a known user profile. Password Manager then attempts to sign into that system with the user-entered password. If the login attempt succeeded, the user's profile is updated with the system ID and the user-entered login ID.

Self-service login ID reconciliation has major advantages over data cleansing projects and over approximate matching on attributes such as full names:

- The process is inexpensive to implement, as it only requires a few minutes from each of thousands of users. This distributed effort is effectively free.
In contrast, data cleansing projects require months of effort from multiple full time staff.
- The process can be made as fast as desired. Thousands of users can be asked to enroll per week. An entire organization can be deployed in one or two months.
- Connected login IDs are guaranteed to belong to the indicated user, since their owner “proved possession” by providing a validated password to each login account.
In contrast, both a data cleansing project and approximate matches on full name will yield erroneous matches, which will later constitute security breaches, including allowing one user to reset another's password.

6.3.3 Automated correlation

If user IDs are different, but each system where a user has a login ID has some common attribute in the user record (e.g., SSN or employee number), then correlating data can be automatically generated.

Before pursuing this approach, validate that the common attribute is truly unique and widely populated. In particular, full names are not appropriate key attributes, as they are frequently mistyped, and many people share an identical full name (e.g., Michael Smith).

7 User enrollment

In many organizations, deployment of a password management system requires a user enrollment process. Users may have to provide personal data such as answers to authentication questions (which can subsequently be used to authenticate users who forget or lock out their passwords). Users may be asked to attach their non-standard IDs to their profiles. Users may have to provide biometric samples, likewise used for non-password authentication in the event of a future password problem. Finally, users may simply be asked to review and agree to some corporate policy, for example regarding password sharing or writing down their password.

If enrollment is required, it is helpful for the password management system to automate the process by identifying users who must be enrolled, inviting and reminding them to enroll, provide a strongly authenticated enrollment user interface, etc.

Hitachi ID Password Manager includes built-in infrastructure to securely and automatically manage the user enrollment process:

- By monitoring one or more systems of record, Password Manager automatically creates new and removes old profile IDs.
- New users and existing users with incomplete profiles are automatically prompted to complete their profiles (e.g., by answering security questions).
- Invitations to enroll may be e-mailed to users.
- Users may be more forcefully reminded to enroll by having a web browser automatically open to the enrollment page when they log into the network.
- Users may be forced to enroll, by opening a kiosk-mode web browser to the enrollment page when they sign into the network, and blocking access to the Windows desktop until users complete their profile. This process is typically controlled by placing users into a “mandatory enrollment” AD group and attaching a suitable GPO to that group.
- To enroll, users must first authenticate. This is normally done by leveraging an existing strong authenticator – such as a network password or a token.
- A single, integrated enrollment system supports collecting answers to security questions, mapping different login IDs, on different systems back to their owners and collecting biometric voice print samples.

Following is a sample registration request e-mail:

To all users:

Acme, Inc. is activating a password management system on our network.
This system will help you to manage your own passwords:

- * It will help you to synchronize passwords for all of your systems.
- * If you forget your password, you will be able to reset it yourself,

without calling the help desk.

Please take a few moments to register with the password management system now:

- * Click on the URL below.
- * In your web browser, log in with your Windows ID and password.
- * Select the ``Personal information`` screen and fill in the blanks. Your answers on this form will be used to verify your identity should you forget your password in the future.
- * Select the ``Add login accounts`` screen and type every login ID / password pair that you currently use. This lets our system verify what systems you log into.

To register now click here ---> <http://password.acme.com/>

After you have registered, you will still have to change your Windows password every 60 days. When you do that, all your other passwords will be automatically set to the same new value.

One password is easy to remember: please find and destroy any notes you may have that contain your system passwords.

You can also change your passwords or registration information any time, using the same URL (above).

After registering, if you forget or disable your Windows password, you can just log into your workstation with the ID "help" and no password, and follow the on-screen instructions to fix your problem. Please *do* put a sticky note on your monitor to remind yourself of this feature.

From now on, passwords will be subjected to a more secure password policy, to make them harder for intruders to guess. Please make sure that your new passwords:

- * Have at least 7 and at most 8 characters.
- * Have at least one digit and at least two letters.
- * Have both lowercase and uppercase letters.
- * Are not derived in any way from a dictionary word or name.

Do change your passwords at least every 60 days and do not reuse old passwords (ever).

If you have any questions, please contact password_support@acme.com.

Thank you!

-- The I.T. department.

8 Maximizing adoption rates

Hitachi ID Password Manager is intended to deliver value to an organization, by reducing support costs, improving user service and strengthening security.

The following sections describe some strategies to increase user adoption of Password Manager, which maximizes its value:

8.1 User education

Provide users education about password management generally, and Hitachi ID Password Manager in particular. Education may be wholly electronic (e.g., how-to and frequently-asked-questions web pages) and in some organizations may be incorporated into a broader training schedule, where users receive live instruction.

If providing purely electronic education, get the users' attention. For example, one Password Manager customer admonishes users: *Passwords are like underwear – change them often and don't share them with your friends.*

8.2 Incentives for registration

Some organizations that deployed Hitachi ID Password Manager have had great success with incenting users to register early. A moderate number of inexpensive prizes (such as restaurant gift certificates), available on a random draw to early registrants or a small number of expensive gifts (such as PDAs, smart phones or holiday airfare) have been used successfully to motivate users to enroll.

8.3 Forced enrollment

Some organizations have opted to force users to enroll with Hitachi ID Password Manager – which typically means completing their personal Q&A profile. This is done by associating users who will be forced to enroll with an Active Directory GPO that replaces their normal login shell (explorer.exe) with a kiosk mode web browser directed at the enrollment page. Users are removed from the AD group that activates this GPO on successful enrollment.

This strategy is very effective, but should be preceded with a user education program advising users to enroll voluntarily. Organizations pursuing mandatory enrollment should have strong and vocal executive support prior to activating this feature.

Enrollment in general and forced enrollment in particular should be paced – not all users should be invited to or required to enroll at the same time. A user enrollment / invitation pace of 500 to 1000 users per day is reasonable in most organizations.

8.4 Registration during assisted service

Some organizations choose not to automatically prompt users to register, but instead register users when they first call the help desk with a password problem, after Hitachi ID Password Manager deployment.

This approach to user registration technically works, but tends to lengthen service desk problem resolution time, because the analyst is registering and educating the user, not just resolving a simple problem. Avoid this approach if possible, and if it is taken, plan on increased password problem incident support cost for 12–18 months.

8.5 Incentives for utilization

Some organizations have increased user adoption rates for self-service password reset (rather than assisted reset) by offering prizes, similar to those for enrollment, to users of the self-service system.

This approach should be used with care, as users with no password problem at all may use the system to qualify.

8.6 Adjusting response time with assisted service

Some organizations intentionally reduce the level of service for assisted password problem resolution. For example, users may have to wait through a recording on the automatic call director (ACD) system that explains self-service password reset before they can talk to a human analyst to resolve their problem.

Conversely, organizations where assisted resolution of password problems is very fast and friendly may get poor user adoption of self-service, since assisted service is so convenient.

8.7 Plan for user adoption

The strategy for user enrollment, education and service adoption depends heavily on corporate culture.

The common thread with every approach is that planning is required, and budget should be set aside for user education and user incentive programs.

High adoption rates do not happen with technology alone.

9 Measuring value

In many organizations, the help desk pays for Hitachi ID Password Manager and expects to measure a direct economic value from it. The following sections discuss how Password Manager utilization and value can be measured.

9.1 Measuring activity

Hitachi ID Password Manager records all activity in a session log table. This includes full sessions, with login time/date, operations, the identify of users and support analysts, results on managed systems and more.

Use the SESSREP program provided with Password Manager to extract a summary of this activity from a given time period.

Once Password Manager is deployed, require support analysts to carry out all password resets with Password Manager, rather than with native tools. If possible, disable their access to native password resets. This will ensure that all password resets are recorded in Password Manager and yield usable metrics.

9.2 Trend analysis

Over time (e.g., monthly), run SESSREP to record both user access to Hitachi ID Password Manager (registration, synchronization, self-service reset) and analyst access (assisted reset incidents and duration).

Plot registration against total user population, to illustrate how many users have registered, how many remain and what the estimated completion date will be.

Plot password synchronization over time, to measure basic utilization of the system.

Plot the sum of self-service password reset and assisted reset over time, to show how effective password management reduces the frequency of password problems.

Plot the fraction of password resets that are self-service over time, to show how users transition from assisted service to self-service.

9.3 User productivity

User productivity benefits are primarily due to reduced frequency of password problems. Refer to the trend analysis in the previous section for an analysis of reduced password problems over time.

9.4 Support cost

Password-related support cost is due entirely to assisted password resets. Refer to the trend analysis in the previous section for an analysis of reduced volume of help desk password resets over time.

10 Ongoing administration and support

The following sections describe the routine ongoing administration of Hitachi ID Password Manager:

10.1 Functional test

Periodically test the functionality of the Hitachi ID Password Manager server. If any component should fail, it is better to discover it pro-actively than wait for users to notice and complain.

10.1.1 Password changes

Create a test user that has at least one login ID on every system where Hitachi ID Password Manager manages passwords. Regularly use both the administrator (nph-psa) and self-service (nph-pss) web GUIs to change every password for this user.

10.1.2 Transparent password synchronization

If you deployed transparent password synchronization (highly recommended), periodically verify that a native password change does, indeed, trigger automatic password updates for the same user on other systems.

10.1.3 Help desk logins

Verify that help desk analysts can log into the application. Create a test analyst ID for this, either internally on Hitachi ID Password Manager or on another system if you use pass-thru authentication.

10.1.4 Directory integration

If you integrated with a corporate or meta directory, and Hitachi ID Password Manager accesses user and login ID information on that system, verify that you can still log in with the ID of a user who does not exist locally on the Password Manager server. Test with both nph-psa, nph-pss, nph-pss and pushpass.

10.1.5 Sending e-mails

If you implemented e-mail notifications for registration, clear a test user's profile and verify that the user does receive an invitation to register.

If you implemented e-mail notification of events (e.g., password change, intruder lockout, etc.), trigger every relevant event and verify that e-mails were sent out appropriately.

10.1.6 Creating call tracking system ticket

If you implemented call tracking system integration, trigger every relevant event and verify that tickets were opened appropriately. Open the tickets in the call tracking system to verify that they are constructed correctly.

10.1.7 IVR integration

If you implemented an IVR user interface, verify that it is able to authenticate a test user and reset that user's passwords.

10.1.8 User registration

If you implemented web-based registration, verify that a test user can update his own Q&A profile or login aliases, as appropriate.

If this feature is enabled, also verify that help desk analysts can register Q&A data on behalf of callers in nph-psa.

10.2 Changes to target system configuration

Changes made to the configuration on some targets can have an impact on Hitachi ID Password Manager. Arrange with your change control manager (or your system and/or application owners) to notify you of changes to individual system configuration.

For example:

- Changes to targets that use Telnet agents may require modifications to Telnet scripts.
- Changes in the LDAP schema may require changes to the Password Manager target definition.
- Upgrades to Novell and Oracle clients/servers may require reconfiguration of the client software on the Password Manager server.
- Upgrades to SAP or PeopleSoft ERP applications will typically require configuration changes or upgrades to the relevant agents on the Password Manager servers.

Use a test server to validate configuration changes such as installation of updated client software or modified scripts before you enable those changes in production.

10.3 Monitoring service health

You can check service health by monitoring the contents of the service log files in the temporary logging directory, or by using the Hitachi ID Password Manager administration module (nph-psa.exe). The log files should give few or no warnings, and no errors.

To check service health using the Password Manager administration module (nph-psa.exe):

1. Log into the Password Manager administration module (nph-psa.exe).
2. Click **Server monitor** -> **Service** to see the *Monitor Password Manager server* page.
3. Check the status of the services.
4. Click **Manage** next to the service you want to check to see the *Password Manager server manager* page for that service.
5. Read the contents of the log in the temp directory in the field at the bottom of the page.
6. Check the Windows Event Viewer for warnings or errors.
7. Use the Windows Task Manager to monitor system CPU, memory and I/O load.

10.4 Monitoring the pushpass service

The `psppmon` program monitors the `pushpass` service and sends out an e-mail when `pushpass` starts up or goes down. The message will state at what time `pushpass` went down, and whether it was restarted. If `pushpass` has stopped, the service appends the last 200 lines of the specified log file to the email.

`psppmon` can execute a program, such as a batch file to restart the service, if `pushpass` is down for too long. By default, `psppmon` will try to execute the program once. You can specify a number of times that it will retry while `pushpass` is down.

The service will monitor the Hitachi ID Password Manager databases every 24 hours from the time it is started. If any of the databases double in size or drop by half, `psppmon` will send a warning e-mail.

10.5 Monitoring transparent synchronization on Windows servers

Monitor the health of the transparent synchronization DLL (`psintcpt.dll`) on Windows NT PDCs and Windows 2000 DCs. Run `netstat -an` to see whether there are many (more than 20 or 30) TCP connections pending between the PDC/DC and the Hitachi ID Password Manager server. If so, there may be a problem with the Password Manager server.

10.6 Monitoring utilization

Monitor Hitachi ID Password Manager utilization to determine the progress of your deployment and to ensure the success of Password Manager operation. You can do this using the Password Manager administration module (`nph-psa.exe`), or with the `sessrep` program.

Password Manager includes a facility to allow help-desk users, with the specified right, to run reports on Password Manager targets, users, usage, and events.

Use the `sessrep` program to provide a quick statistical report, in ASCII text format, on the usage of all Password Manager modules.

10.7 Randomizing target system credentials

Use the `admchgpw` program to change the administrator passwords used by Hitachi ID Password Manager to log into various systems. Run `admchgpw` periodically to ensure that Password Manager target system credentials are random and secure.

After each password change, the new value is verified, and if the change was successful, it is stored in the Password Manager database host table.

Verify that password verify and reset operations continue to work on every target system after running `admchgpw`.

10.8 Making backups

Please refer to [Subsection 5.7](#) on [Page 30](#) for details about making backups of production Hitachi ID Password Manager servers.

10.9 Purging old Q&A data

If entire question sets or individual questions are removed from Hitachi ID Password Manager, related answers that were already defined by the end user will remain in the response database. This data is left in the database table in case the questions are returned later.

As a result, `deploychk` and possibly `sessrep` produces invalid data and reports.

Also, when a question is created and then deleted, and then re-created (for example, if it was deleted in error), it will be given a new QID and the previously defined answers would no longer match, and may be considered invalid.

To purge this data, pack and re-index the response database with the `dbop` program.

11 Summary

Hitachi ID Password Manager deployment is straightforward and can be completed in a matter of weeks, typically requiring only a few days of professional services.

Because Password Manager impacts so many groups in an I.T. organization, it is important to have powerful and visible project sponsorship and to involve all stake-holders as early as possible.

This document outlines numerous best practices regarding technical architecture, security policies, user enrollment, maximizing user adoption and ongoing administration. These should be taken as guidelines and combined with specific requirements of each organization to produce an implementation design and project plan.