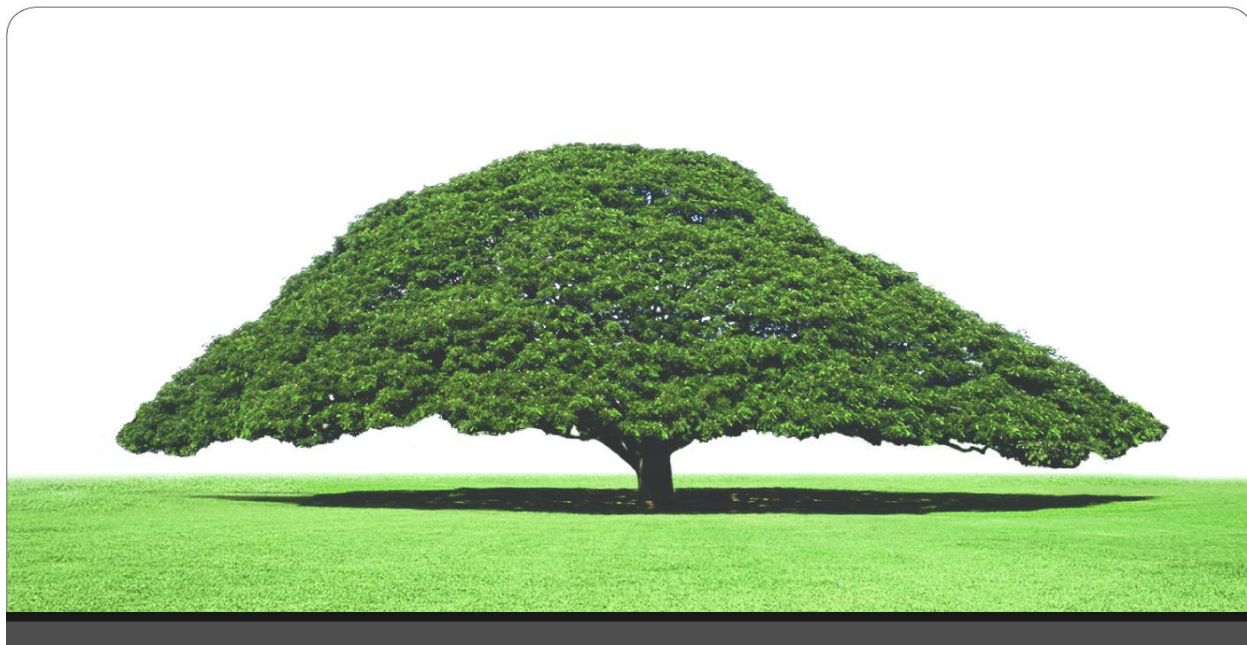


© Hitachi ID Systems, Inc.



Hitachi ID Privileged Password Manager (formerly ID-Archive) Features

Contents

- 1 Introduction** **1**

- 2 Random Passwords and Manually Set Passwords** **1**

- 3 Password Policy Enforcement** **1**

- 4 Access Disclosure** **2**

- 5 Replicated, Encrypted Storage** **2**

- 6 Access Control Infrastructure** **3**

- 7 Externalized Identification, Authentication and Authorization** **4**

- 8 Temporary Access Requests and Approval** **4**

- 9 Concurrent Access** **5**

- 10 Target System Connectors** **6**

- 11 Managing Workstation Passwords** **7**

- 12 Windows Service Accounts** **7**

- 13 Other Integrations** **8**

- 14 Auto-Discovery – Systems, Services and Logins** **9**
 - 14.1 Servers 9
 - 14.2 Workstations 10

- 15 Logging and Reporting** **10**

1 Introduction

Hitachi ID Privileged Password Manager is a system for securing privileged passwords across large numbers of devices. It works by regularly randomizing privileged passwords on workstations, servers and applications. Random passwords are encrypted and stored on at least two replicated servers. Passwords may be disclosed:

1. To administrators, after they have authenticated and their requests have been authorized.
2. To applications, replacing embedded passwords.
3. To Windows workstations and servers, which need them to start services.

Alternately to password disclosure, access may be disclosed by temporarily placing an authorized user into a privileged security group on a managed device.

Password changes and disclosure are closely controlled and audited, to satisfy policy and regulatory requirements.

2 Random Passwords and Manually Set Passwords

Normally, Hitachi ID Privileged Password Manager sets password values randomly on target systems. This may be initiated by the workstation service on user PCs or pushed out to target systems from a Privileged Password Manager server at a scheduled time and whenever a password is checked in.

The frequency of random password changes is set by a policy setting, applied to each resource group. Policy also controls what days of the week and times of day are permissible times to change passwords. For example, some passwords may only be changed between 3AM and 4AM on Monday mornings.

Privileged Password Manager also supports manual override on passwords, where a requester or authorized user asks to set a given password to a given value. This takes effect immediately on push-mode target systems and at the next poll time on pull-mode target systems.

3 Password Policy Enforcement

Hitachi ID Privileged Password Manager can enforce multiple password policies. There is a global policy and local, override policies applied to resource groups. Password policies specify the complexity of both randomly chosen and manually selected passwords. In addition to mandating character types (lowercase, uppercase, digits, punctuation), the policy can specify minimum and maximum password lengths and other characteristics, especially relevant to manually-chosen passwords, such as dictionary and history checks.

4 Access Disclosure

Hitachi ID Privileged Password Manager controls access by users and agents to privileged accounts on systems and applications. By default, that means randomizing and disclosing current password values. Display of password values is not a mandatory part of the process, however:

1. IT staff can directly launch Terminal Services (RDP), SSH (PuTTY) and other connections to target systems from the Privileged Password Manager web user interface, without the ability to display a password value.
2. IT staff can use an ActiveX control embedded in the Privileged Password Manager web UI to place a copy of a sensitive password into their OS copy buffer, again without displaying any passwords.
3. Privileged Password Manager can dynamically attach a recipient's Active Directory domain login ID in a local security group on a target system, and later remove it. This eliminates the need to disclose passwords even to a software agent on the recipient's workstation.
4. Where password display is required, JavaScript in the Privileged Password Manager web UI removes it from the screen after a few seconds.

A policy defined for each group of resources in Privileged Password Manager determines which of these access disclosure mechanisms is available to each group of systems. For example, password display may be allowed for Windows workstations, since they may be inaccessible over the network, but only RDP sessions (with no possibility of disclosure) may be allowed for Windows servers.

5 Replicated, Encrypted Storage

Privileged passwords must be protected more vigorously than any other data in an organization:

1. **Sensitive data:**
Privileged passwords are arguably the most sensitive data in an organization, since they unlock all other data. Inappropriate disclosure can be catastrophic.
2. **Business interruption:**
Loss of access to privileged passwords means that the systems which the privileged passwords control cannot be managed, at least until they are powered down and "hacked into." Consider the impact on IT support of a disaster where every `root` or `Administrator` password in a company is permanently lost.
3. **Constant change / data backup:**
If privileged passwords are changed regularly, then scheduled backups will contain mostly historical data rather than current passwords and so provide little value.

Hitachi ID Privileged Password Manager includes built-in data replication.

Data replication between Privileged Password Manager servers occurs in real time – all updates to one server's database are queued up and sent to other (peer) servers as well. If a peer server is unavailable, database updates are automatically retried when the server becomes available again.

All replication is performed at the application level, over an encrypted TCP/IP socket. This makes configuration of a replicated environment straightforward and eliminates the need to license and configure a replicated RDBMS server product.

Privileged Password Manager data replication is secure. Data transmitted between servers is encrypted and each endpoint authenticates the other. Replication uses relatively low bandwidth and is tolerant of high latency, making it suitable for deployment across physically distant sites. Replication is fault tolerant, in that failed transmissions are queued and retried until they succeed.

6 Access Control Infrastructure

The most common form of access control in the Hitachi ID Privileged Password Manager is based on resource groups. Resource groups are named collections of devices where privileged passwords are managed and to which policies are applied.

Resources can either be attached to a group explicitly (e.g., “attach workstation WKSTN01234 to resource group RGWKSTNS”) or implicitly, using an expression. Expressions may be based on the operating system type, IP address, MAC address or workstation name (e.g., “attach every workstation running Windows XP in subnet 10.1.2.3/24 to resource group X”)

Policies applied to resource groups include:

1. Which accounts' passwords to randomize.
2. How to compose random passwords (e.g., length, complexity, etc.).
3. What actions to take after successful or failed attempts to disclose a password.

Resource groups may be nested, as a mechanism to more naturally represent groups of devices.

Privileged Password Manager users are likewise grouped into console user groups, either explicitly or implicitly (i.e., via membership in a user group on a target system, such as Active Directory). Groups of console users are granted specific rights to resource groups. Rights include the right to display member devices, to view passwords and to view access history.

Business policies, such as segregation of duties between different groups of IT administrators, can be enforced by assigning users to distinct user groups, each with access to different (non-overlapping) sets of passwords.

7 Externalized Identification, Authentication and Authorization

Hitachi ID Privileged Password Manager can be configured to take advantage of an existing directory of users for authentication and authorization:

1. Users may sign into Privileged Password Manager with their Active Directory or LDAP login ID and password.
2. Users may be required to authenticate with a two-factor technology, such as an RSA SecurID token.
3. User membership in Privileged Password Manager security groups and consequently user privileges, may be based on user membership in AD or LDAP groups.

Externalizing user identification, authentication and authorization can significantly reduce the administrative overhead of managing a Privileged Password Manager deployment.

8 Temporary Access Requests and Approval

Hitachi ID Privileged Password Manager includes the same authorization workflow engine as is used in other Hitachi ID products – Hitachi ID Identity Manager (formerly ID-Synch™), Hitachi ID Access Certifier (formerly ID-Certify) and Hitachi ID Group Manager (formerly ID-Access). Workflow enables one user to request release of a given password. When this happens, one or more other users are invited (via e-mail) to review and approve the request. Approved requests trigger an e-mail to the password recipient, including a URL to Privileged Password Manager where he or she can re-authenticate to display the requested password or launch a login session to the device in question.

The workflow process is illustrated by the following series of steps:

1. User UA signs in and requests that the then-current password to login account LA on system S be made available to user UB at some later time T. UA may or may not be the same person as UB.
2. Privileged Password Manager looks up authorizers associated with LA on S.
3. Privileged Password Manager may run business logic to supplement this authorizer list, for example with someone in the management chain for UA or UB. The final list of authorizers is LA. There are N authorizers but approval by just M ($M \leq N$) is sufficient to disclose the password to AZ.
4. Privileged Password Manager sends e-mail invitations to authorizers LA.
5. If authorizers fail to respond, they get automatic reminder e-mails.
6. If authorizers continue to fail to respond, Privileged Password Manager runs business logic to find replacements for them, effectively escalating the request and invites the replacement authorizers as well.
7. Authorizers receive invitation e-mails, click on a URL embedded in the e-mail invitation, authenticate themselves to the Privileged Password Manager web login page, review the request and approve or reject it.
8. If any authorizers reject the request, e-mails are sent to all participants (UA, UB and AZ) and the request is terminated.
9. If M authorizers approve the request, thank-you e-mails are sent to all participants. A special e-mail is sent to the recipient – UB with a URL to a password disclosure page.

10. UB clicks on the e-mail URL and authenticates to Privileged Password Manager and displays the password.
11. UB clicks on a button to “check-out privileged access.”
12. UB then may click on a button to do one of the following (the options available will vary based on policy):
 - (a) Display the password.
 - (b) Place a copy of the password in the operating system copy buffer.
 - (c) Launch an RDP, SSH or similar remote control session to the server in question.

In other words, display of a sensitive password is not a mandatory part of the solution.

9 Concurrent Access

Hitachi ID Privileged Password Manager can be configured to track and control the number of people to whom a given password is disclosed at any given time. This is done using the concept of password checkout and checkin.

1. Rather than simply disclosing a managed password, a user may be required to check it out. Checkout is subject to policy control:
 - (a) A counter is incremented whenever a password is checked out, indicating that one more person is in possession of the password.
 - (b) The number of users who may concurrently check out a password is limited – for example, up to two at a time.
 - (c) The time interval for which a user may hold a password is limited – for example, no more than two hours.
2. Users are asked to check-in passwords when they are done using them:
 - (a) The password’s checkout counter is decremented.
3. If the maximum allowed password checkout time has elapsed, Privileged Password Manager may automatically check the password back in, which causes it to be randomized again.
4. Checkin and checkout supports coordination among IT workers:
 - (a) Privileged Password Manager can notify users who already possess a password of new check-outs, for example to let them know that someone else will now be working on the same system on which they are already working.
 - (b) Privileged Password Manager can show requesters who already has a given password.
5. Password checkout is time limited and passwords may be automatically checked back in after the allowed time has elapsed.
6. Passwords can be automatically randomized whenever the checkout counter returns to zero, meaning that no users will know the new password after a given amount of time has elapsed.

Checkin/checkout supports easier coordination between IT workers who need to collaborate.

10 Target System Connectors

Hitachi ID Privileged Password Manager includes built-in integrations for a broad variety of target system types:

Directories:	Servers:	Databases:
Any LDAP, AD, WinNT, NDS, eDirectory, NIS/NIS+.	Windows NT, 2000, 2003, 2008, Samba, Novell, SharePoint.	Oracle, Sybase, SQL Server, DB2/UDB, ODBC.
Unix:	Mainframes:	Midrange:
Linux, Solaris, AIX, HPUX, 24 more.	z/OS with RAC/F, ACF/2 or TopSecret.	iSeries (OS400), OpenVMS.
ERP:	Collaboration:	Tokens, Smart Cards:
JDE, Oracle eBiz, PeopleSoft, SAP R/3, Siebel, Business Objects.	Lotus Notes, Exchange, GroupWise, BlackBerry ES.	RSA SecurID, SafeWord, RADIUS, ActivIdentity, Schlumberger.
WebSSO:	Help Desk:	HDD Encryption:
CA Siteminder, IBM TAM, Oracle AM, RSA Access Manager.	BMC Remedy, BMC SDE, HP Service Manager, CA Unicenter, Assyst, HEAT, Altiris, etc.	McAfee, CheckPoint.

Privileged Password Manager includes a number of flexible connectors, each of which is used to script integration with a common protocol or mechanism. These connectors allow organizations to quickly and inexpensively integrate Privileged Password Manager with custom and vertical market applications. The ability to quickly and inexpensively add integrations increases the value of the Privileged Password Manager system as a whole.

There are flexible connectors to script interaction with:

API binding:	Terminal emulation:	Web services:	Back end integration:	Command-line:
<ul style="list-style-type: none"> • C, C++ • Java, J2EE • .NET • COM, ActiveX • MQ Series 	<ul style="list-style-type: none"> • SSH • Telnet • TN3270, TN5250 • Simulated browser 	<ul style="list-style-type: none"> • SOAP • WebRPC • Pure HTTP(S) 	<ul style="list-style-type: none"> • SQL Injection • LDAP attributes 	<ul style="list-style-type: none"> • Win32 • PowerShell • Unix/Linux

Organizations that wish to write a completely new connector to integrate with a custom or vertical market application may do so using whatever development environment they prefer (J2EE, .NET, Perl, etc.) and invoke it as either a command-line program or web service.

If customer develops their own integrations, an effort of between four hours and four days is typical. Alternately, Hitachi ID offers fixed-cost custom integrations for a nominal fee.

11 Managing Workstation Passwords

To manage privileged passwords on workstations, Hitachi ID Privileged Password Manager includes a service, which installs on each workstation and which contacts a central server to coordinate local password changes.

This architecture has several important advantages:

- The workstation service uses only HTTPS to communicate with the central server and works even when the workstation is connected behind NAT devices, firewalls or application proxies.
- The workstation service does not randomize passwords unless it has established connectivity with the central privileged password management server. This avoids a situation where the central server does not know the new password value for a workstation.
- Dynamic IP addresses have no impact on this architecture.
- Physical relocation and long periods of detached network connectivity may delay updates to local passwords, but do not introduce a failure whereby the local administrator passwords on a workstation are unknown.

12 Windows Service Accounts

On the Windows operating system, service programs are run either using the SYSTEM login ID, which possesses almost every privilege on the system (and consequently can do the maximum harm) and which has no password or using a real user's login ID and password, in order to execute with reduced privileges. This means that on each Windows workstation and server there are a number of service accounts, each with its own password, which are used to run service programs such as web servers, backup agents, anti-virus software, etc.

Service account passwords differ from administrator passwords in that they are stored in at least two places:

1. Hashed, in the security database – e.g., the local SAM database or Active Directory, just like all users.
2. Reversibly encrypted, in the registry or elsewhere, where the program that starts the service (e.g., Service Control Manager or similar) can retrieve it when it needs to start the service.

Other Windows components besides the Service Control Manager also store passwords twice:

1. Virtual directories used to access web content from the IIS web server.
2. Programs scheduled to be run by the Windows Scheduler.

Third party programs may also require passwords to be stored outside the Security Accounts Manager (SAM) database.

Of the above passwords, all but those used in IIS are static and may represent a security vulnerability.

Hitachi ID Privileged Password Manager can be configured to secure service account passwords. This means two things, depending on the mode of operation:

1. In pull mode, the Privileged Password Manager workstation service periodically scrambles service account passwords locally, in coordination with the central Privileged Password Manager server cluster.
2. In push mode, Privileged Password Manager servers periodically connect to Windows servers in order to change the passwords of service accounts.

In both cases, Privileged Password Manager notifies the program that launches service accounts of the new password value, so that it can successfully launch the service at the time of the next system restart or when an administrator manually stops and restarts the service in question.

In push mode, Privileged Password Manager runs an exit program which remotely connects to the server in question and updates the secondary storage of the service password. Exit programs are provided to remotely update:

1. The Windows Service Control manager.
2. The Windows Scheduler.
3. The IIS web server.

Privileged Password Manager implementers can write additional exit programs to update service passwords used by other programs, stored in other locations. These are typically command-line programs (Win32 executable or script) that run on the Privileged Password Manager server.

In pull mode, the Privileged Password Manager workstation service can use a DLL to update local passwords. DLLs are provided for the same Windows components as the exits above and implementers can write new DLLs to update other passwords.

13 Other Integrations

Hitachi ID Privileged Password Manager is integrated with a broad variety of IT infrastructure components that, while not ID management or password management targets, are critical to the success of the project:

- Meta directories (read, update user object data):
 - Microsoft / ILM.
 - Open API (application programming interface) for others.
- E-Mail systems (send e-mail, manage mail folders and ACLs):
 - Microsoft Exchange.
 - Novell GroupWise.

- Lotus Notes.
- HP/Samsung OpenMail.
- Open API for others.
- Incident management systems (create/update/close tickets):
 - Axios Assyst
 - Altiris.
 - BMC Service Desk Express (7.0, 7.5, 9.x)
 - CA Unicenter Help Desk
 - Clarify eFrontOffice (8, 12)
 - FrontRange HEAT (5, 6, 7, 8)
 - HP Service Desk
 - HP Service Manager (any version)
 - BMC/Remedy ARS (4, 5, 6, 7)
 - ... and more
- Authentication systems (manage tokens, authenticate passcodes):
 - RSA / SecurID.
 - Vasco.
 - Secure Computing SafeWord.
 - Others using either native APIs and RADIUS.
- Biometric voice print verification:
 - Nuance.
 - Votent.
 - VoiceVantage.
- Hard disk encryption (reset local password):
 - PointSec.

14 Auto-Discovery – Systems, Services and Logins

14.1 Servers

In organizations with large numbers of servers, clearly it is desirable to auto-discover and auto-maintain a list of servers, rather than manually adding and maintaining thousands of separate target systems.

The manner in which servers should be discovered will vary from organization to organization. For example, server records can be extracted from Active Directory, a DNS zone transfer, extracted from an IT inventory management system or acquired through a periodic port scan of key network segments.

An important part of any large-scale Hitachi ID Privileged Password Manager deployment is designing and implementing this auto-discovery system to suit the specific needs of the target network. To support this effort, Privileged Password Manager includes a batch-load capability, to import large numbers of target system records and an Active Directory-specific auto-discovery program, which pulls server records from AD.

Once target systems are identified, loaded into the Privileged Password Manager database and attached to resource groups (for example, based on characteristics such as their IP address, operating system, computer object directory OU, etc.), target login accounts must also be discovered and configured. This is done in a second auto-discovery phase, which periodically connects to discovered systems, lists their local user IDs and automatically determines which ones either (a) have administrative rights or (b) are used to start services, run batch jobs or publish web directories.

Privileged Password Manager also includes an automated mechanism to inform programs that store a copy of passwords of new password values. A plug-in program is provided to connect to Windows servers after each local password change and to automatically update Service Control Manager, Windows Scheduler and IIS with the new password value.

14.2 Workstations

In organizations that deploy the Hitachi ID Privileged Password Manager workstation service, there is no need to manually configure client devices in the Privileged Password Manager database. Instead, the workstation service is installed on devices through one of several means:

1. By being made a part of the standard workstation software image.
2. By being distributed through a system such as SMS.
3. By being distributed using an Active Directory Group Policy Object (AD GPO).

Once installed, the Privileged Password Manager workstation service automatically starts and registers itself, along with all local user accounts with the central Privileged Password Manager server cluster.

The software installation MSI package is constructed on the Privileged Password Manager server and includes information about the Privileged Password Manager server URL, what resource groups workstations should be attached to, etc. This means that software installation can be fully automated and does not present a user interface.

A similar approach is used to deliver .tar format installation packages to Unix and Linux workstations.

15 Logging and Reporting

Hitachi ID Privileged Password Manager logs all attempted and completed password updates. This data can be used to track not only current administrator passwords for workstations and servers, but also device IP addresses and network status. Privileged Password Manager also logs all attempts by users to look up devices and to display passwords. This creates a chain of accountability, making it clear who accessed what device and when and also who attempted to access a device and was blocked by policy or failure to get approval.

Privileged Password Manager includes event reports, which make it possible to see, among other things:

- Who disclosed passwords to given resources.

Privileged Password Manager Features

- How often any given password was disclosed.
- When and how often passwords were changed on target systems.
- How often users attempted to sign into Privileged Password Manager.
- What the results of those authentication attempts were.

Reports are also included to examine the set of discovered / managed systems and accounts.

The Privileged Password Manager schema is well documented and the database is a standard, relational SQL back-end. This makes it possible for Hitachi ID customers to write custom reports using off-the-shelf programs such as Crystal Reports.