



Hitachi ID Privileged Password Manager secures administrator and service accounts by frequently randomizing passwords. Random passwords are stored in an encrypted and replicated vault. It controls and logs the access of users and applications to privileged accounts using authorization rules, workflow approvals and single sign-on.

## The Privileged Identities Challenge

### Security

Many system administrators admit to writing down and sharing privileged passwords. Staff often retain access to sensitive systems even after leaving an organization. Given time, password cracking software can guess many static passwords.

### Coordination

There are privileged passwords on every system, including operating systems, databases, network devices and applications. Changing these passwords is hard to coordinate among every user of every password.

## Key Benefits

By frequently randomizing sensitive passwords, *Hitachi ID Privileged Password Manager* prevents inappropriate retention of elevated access by current and former staff and eliminates the threat of password cracking software. Audit logs create accountability for administrative changes.

- ✓ **PASSWORD RANDOMIZATION**  
*Eliminate static passwords*  
By periodically randomizing passwords, Password Manager blocks password cracking attacks and reduces the breadth and time interval during which legitimate users can abuse their authority.
- ✓ **ENCRYPTED, REPLICATED VAULT**  
*Reliable, fault-tolerant and secure storage*  
Random passwords must be stored in a secure place and retrieved when required. An encrypted, access-controlled and replicated database protects against data leakage, data loss and service interruption.
- ✓ **MANY BUILT-IN CONNECTORS**  
*Operating systems, network devices, databases and applications*  
Privileged Password Manager ships with built-in integrations for over 100 kinds of systems and applications, so it can secure the entire network with minimal customization.
- ✓ **AUTO-DISCOVERY**  
*Eliminate manual configuration of target systems and accounts*  
A two-tier auto-discovery system finds and classifies servers, workstations, services and privileged accounts. Machine discovery can be based on AD, LDAP, DNS or an IP port scan. Account discovery can examine services and group memberships.
- ✓ **SINGLE SIGNON TO PRIVILEGED ACCOUNTS**  
*Eliminate password display wherever possible*  
Rather than displaying passwords, Privileged Password Manager can:
  - Launch RDP, SSH and similar sessions.
  - Temporarily attach authorized users to privileged security groups.
  - Temporarily add authorized users to SSH authorized\_keys files.

## ✓ REPORTS

### ***Accountability and transparency***

Many reports are built-in, to answer:

- What computers are on the network?
- Which computers have been unresponsive during the past 30 days?
- Which administrators have signed into this computer?
- Which systems has this administrator managed?
- Who has made a large number of requests for one-off access?

## ✓ SECURITY POLICY ENGINE

### ***Control who can connect to each privileged account***

Security officers set policy to link groups of IT staff to groups of assets, combining secure single sign-on with strict controls.

## ✓ WORKFLOW REQUESTS, APPROVALS

### ***Respond to emergencies and create a flexible workforce***

A powerful workflow engine allows users to request one-time access to privileged accounts. Requests are subject to policy -- who can ask, who must approve. E-mail invites authorizers to visit a secure web form to approve or reject requests.

## ✓ RANDOMIZE WINDOWS SERVICE ACCOUNT PASSWORDS

### ***Seamless integration with Windows service infrastructure***

Privileged Password Manager automatically notifies Windows Service Control Manager, Scheduler, IIS and other components of new passwords.

## ✓ WEB SERVICES API

### ***Eliminates static, embedded passwords***

An API, authenticated with a userID, a one time password, an IP address range and more eliminates static passwords embedded in applications and configuration files.

## ✓ LAPTOP SUPPORT WITH A LOCAL SERVICE

### ***Protect mobile as well as fixed assets***

Client software for Windows and Linux laptops allows Privileged Password Manager to secure passwords on mobile devices that are often disconnected or powered down.

## INCLUDED CONNECTORS

### **Directory:**

Windows/Active Directory, LDAP, eDirectory, NDS

### **File/Print:**

Windows, NetWare, Samba, NAS appliances

### **Databases:**

Oracle, Sybase, SQL Server, DB2/UDB

### **Unix:**

Linux, Solaris, AIX, HP/UX with passwd, shadow, TCB, Kerberos, NIS or NIS+

### **Mainframes/minis:**

z/OS with RAC/F, TopSecret or ACF/2; iSeries; Scripts for VM/ESA, Unisys, Siemens, OpenVMS, Tandem

### **Applications:**

Oracle eBiz, PeopleSoft, SAP R/3, JDE and more.

### **Groupware:**

Exchange 2000 thru 2010, Notes NAB and ID files, GroupWise

### **Networking:**

Network devices and VPNs via AD, LDAP, SSH.

### **Flexible Agents:**

API, SSH, Web Service, Browser emulation, Telnet, TN3270, TN5250, HTTP(S), SQL injection, LDAP attributes and command-line

### **Cloud / SaaS:**

WebEx Connect, Google Applications, SOAP agent

## INCIDENT MANAGEMENT INTEGRATIONS

Automatically create, update and close tickets on:

- Axios Assyst
- BMC SDE
- Clarify eFrontOffice
- HP Service Manager
- Symantec/Altiris
- BMC/Remedy ARS
- CA Unicenter
- FrontRange HEAT
- Numara Track-IT!
- Tivoli Service Desk

Additional integrations via e-mail, ODBC, web services and web forms.

## Hitachi ID Privileged Password Manager

is part of the Hitachi ID Management Suite, which also includes: Password Manager for self service management of authentication factors and Identity Manager for user provisioning.

For more information, please visit

<http://hitachi-id.com/>

or call

1.403.233.0740