

Hitachi ID Privileged Access Manager

(Formerly Privileged Password Manager)

HITACHI
Inspire the Next



Securing access to privileged accounts.

Hitachi ID Privileged Access Manager secures administrator and service accounts by frequently randomizing passwords. Random passwords are encrypted and stored in a replicated vault. It controls and logs the access of users and applications to privileged accounts.

Privileged Access Management Challenges

Security

Many system administrators admit to writing down and sharing privileged passwords. Staff often retain access to sensitive systems after leaving an organization. Given time, password cracking software can guess many static passwords. Weak controls over powerful accounts pose a grave security risk.

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 Access Manager* prevents unauthorized access by current and former users and eliminates the threat of password cracking. Audit logs create accountability to monitor administrative changes.

- ✓ **PASSWORD RANDOMIZATION**
Eliminate static passwords
By frequently randomizing passwords, Privileged Access Manager blocks password cracking attacks, password sharing and privilege retention.
- ✓ **ENCRYPTED, REPLICATED VAULT**
Reliable, fault-tolerant and secure storage
Random passwords are stored in an encrypted database. Replication protects against data loss and service interruption.
- ✓ **MANY BUILT-IN CONNECTORS**
Operating systems, network devices, databases and applications
Privileged Access Manager includes connectors for over 100 types of systems and applications, more than any competing product. It can secure the entire network with minimal customization.
- ✓ **INFRASTRUCTURE AUTO-DISCOVERY**
Eliminate manual configuration of managed systems and accounts
An 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. Discovered systems are probed to find local services, accounts and groups. Rules determine which discovered systems and accounts to manage and which security policy to attach.
- ✓ **SINGLE SIGN-ON TO PRIVILEGED ACCOUNTS**
Eliminate password display
Rather than displaying passwords, Privileged Access Manager can:
 - Launch RDP, SSH and similar sessions and automate the login process.
 - Temporarily attach authorized users to privileged security groups.
 - Temporarily add authorized users to SSH authorized_keys files.Passwords are rarely displayed, so cannot be shared, retained or compromised.



✓ SESSION RECORDING

Record administrator sessions for accountability and forensic audits

Privileged Access Manager can be configured to record login sessions to privileged accounts. This includes screen capture, key logging, copy buffer capture and even webcam snapshots. This system uses ActiveX and does not require client software or a proxy server. Extensive ACLs and workflows protect access to recorded sessions, to ensure privacy.

✓ REPORTS

Accountability and transparency

Many built-in reports answer:

- What computers are on the network?
- Which system is managed by which administrator?
- Who has requested one-time access?
- Which administrators signed into this computer?
- Which computers were unresponsive during the past N days?

✓ ACCESS CONTROL POLICY ENGINE

Determine who can connect to each privileged account

Security officers set policy to link groups of IT users to groups of privileged accounts and managed systems. This links strict controls to secure single sign-on.

✓ WORKFLOW REQUESTS, APPROVALS

Fast response to emergencies and a flexible workforce access

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

✓ RANDOMIZE SERVICE ACCOUNT PASSWORDS

Seamless integration with Windows service infrastructure

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 and an IP address range eliminates static passwords embedded in applications.

✓ LAPTOP SUPPORT WITH A LOCAL SERVICE

Secure access to mobile devices

Client software for Windows and Linux laptops allows Privileged Access 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

Database:

Oracle, Sybase, SQL Server, DB2/UDB

Unix:

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

Mainframes/mini:

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

Application:

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, Salesforce.com, UltiPro HR

Network devices:

Cisco, Juniper

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 are available.

Hitachi ID Privileged Access 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

1.877.386.0372