Hitachi ID Password Manager

hitachi-id.com

Challenges

Security

Easily guessed, never-changing and written-down passwords are traditional vulnerabilities, as are help desks that do not reliably identify callers. SaaS applications introduce new risks, especially when they rely on just a single credential.

Support Cost

Expired or forgotten passwords force users to call the help desk for assistance, accounting for 30% of call volume and costing $25 to $35 per call.

Productivity

Users waste time waiting for the help desk to resolve their problems. Work is interrupted if, while off-site, users forget their PC password and must ship their laptop back to the office to resolve the problem.

Return on Investment

Deploying Hitachi ID Password Manager and adopting best practices enables organizations to eliminate over **85%** of the IT support call volume due to login problems. Reducing peak volumes allow help desks to re-assign staff to more important work.

Managing Credentials On-premise and in the Cloud

Hitachi ID Password Manager is an integrated solution for managing credentials across multiple systems and applications. It simplifies the management of passwords, tokens, smart cards, security questions and biometrics. Password Manager lowers IT support cost and improves the security of login processes.

Password Manager includes password synchronization, self-service password and PIN reset, strong authentication, federated access, enrollment of security questions and biometrics and self-service unlock of encrypted hard drives.

Password Synchronization

Hitachi ID Password Manager can synchronize passwords across systems and applications. Users with fewer passwords experience fewer login problems and call the help desk less frequently. When users have fewer passwords to manage, organizations can increase password complexity rules and change frequency.

Password synchronization can be triggered by a password change on systems such as Active Directory (Ctrl-Alt-Del) or by inviting users to a friendly web portal that explains password composition rules.

Self-Service Password and Pin Reset

Users who forgot their password or PIN, or who triggered an intruder lockout can access self-service and resolve their own login problem. This further reduces help desk call volume.

Password reset is available for all major systems and applications, while PIN resets are available for tokens and smart cards.

Self-service Filesystem Unlock

Users who forgot their pre-boot password can interact with both the unlock process on their PC and with Password Manager, to unlock their PC and reach the OS login screen.

Always Available

The core challenge for credential management is accessibility. Users may experience login problems and need help while off-site, at the OS login screen and pre-boot. Hitachi ID Password Manager is available at the PC login screen, via a smart phone app and through a self-service phone call.

Assisted Service

Password Manager can streamline IT support calls by authenticating the help desk analyst, then the caller and finally, enabling password or PIN reset without giving the analyst administrative rights. Tickets can be automatically created or updated on most help desk applications.

Strong Authentication

Users should always sign into Password Manager with two or more authentication factors (2FA). Organizations can leverage existing technology, such as RSA SecurID, or use built-in features such as sending a PIN to the user's mobile phone via SMS or using the **Hitachi ID Mobile Access** app for Android or iOS.

Hitachi ID Systems, Inc.

HITACHI
Inspire the Next

Federated Access

Hitachi ID Password Manager can replace the login screen for applications that support SAML federation, including most SaaS services. The Password Manager login can incorporate a CAPTCHA, browser fingerprinting and 2FA to secure access to critical, Internet-facing applications.

Included Connectors

Directories

Any LDAP, AD, eDirectory, NIS/NIS+

Servers

Windows 2000--2012, Samba, SharePoint

Databases

Oracle, Sybase, SQL Server, DB2/UDB, ODBC, Informix, Progress

Unix

Linux, Solaris, AIX, HPUX, many more

Mainframes

z/OS with RAC/F, ACF/2 or TopSecret

Midrange

iSeries (OS400), OpenVMS

ERP

JDE, Oracle eBiz, PeopleSoft, SAP, Siebel, Business Objects

Collaboration

Lotus Notes, Exchange

Tokens, Smart Cards

RSA SecurID, SafeWord, Duo Security, RADIUS, ActivIdentity, Schlumberger

WebSSO

CA SiteMinder, IBM TAM, Oracle AM, RSA Access Manager

Ticket systems:

ServiceNow, Remedy, BMC SDE, HP SM, CA, Assyst, HEAT, Altiris, Clarify, Track-It!, RSA Envision, MS SCS Manager

HDD encryption

McAfee, CheckPoint, BitLocker, Symantec, Sophos

Cloud

Salesforce.com, WebEx, Google Apps, Office 365, Concur, AWS, vCloud

Miscellaneous

OLAP, Hyperion, iLearn, Cache, Success Factors, vSphere

Extensible

SPML, SCIM, SAML, SSH, Telnet, TN3270, HTTP(S), SQL, LDAP, ODBC, CSV, Python/web services

---

Hitachi ID Password Manager is part of the Hitachi ID Identity and Access Management Suite, which also includes: Identity Manager for governance and administration of identities and entitlements and Privileged Access Manager to secure elevated privileges and passwords to administrator, service and embedded passwords.

For more information, please visit: http://hitachi-id.com/
or call: 1.403.233.0740 | 1.877.386.0372

HITACHI
Inspire the Next