Hitachi ID Password Manager

hitachi-id.com

Managing Credentials On-premises 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, certificates 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 drives.

Challenges

Security

Easily guessed, never-changing and written passwords are traditional vulnerabilities, as are help desks that do not reliably identify callers. SaaS applications introduce new risks, especially when they authenticate users with just a password.

Support Cost

Login problems continue to represent 30% of the call volume to a typical help desk. Legacy password reset systems are breaking down because of drive encryption with pre-boot passwords, a mobile workforce with locally cached passwords on their laptops and poor user enrollment rates.

User 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.

Convenience

Users have too many passwords to remember, manage and type. They continue to request a better experience.

Return on Investment

Deploying Hitachi ID Password Manager and adopting best practices enables organizations to eliminate over 85% of login-related support calls. Reducing peak volumes allow help desks to re-assign staff.

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 often. 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.

Federated Single Sign-on

Hitachi ID Password Manager can replace the login screen for applications that support SAML federation, including most SaaS services. It includes an application launch-pad, so that users can sign into Password Manager in the morning and launch logins to Office 365, Google Apps, Salesforce and more by clicking application icons.

Built-in Strong Authentication

Users always sign into Password Manager with two or more credentials. Password Manager includes its own two-factor smart phone app and can integrate with existing systems, such as Duo Security or RSA SecurID. Using these mechanisms, both federated SSO and self-service credential updates are protected by strong authentication.

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.

PIN resets are available for tokens and smart cards.

Encrypted Drive Unlock

Users who forgot their pre-boot password can mediate between the unlock process on their PC and Password Manager, using either a smart phone app or call to an IVR system. They can unlock their PC without calling the help desk.

Hitachi ID Systems, Inc.

HITACHI
Inspire the Next

Available Everywhere

The core challenge for credential management is accessibility. Users 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. It can unlock encrypted drives and update locally cached passwords.

Assisted Service

Password Manager can streamline IT support calls by authenticating both the help desk analyst and the caller before enabling password or PIN reset. The support technician does not require administrative rights and tickets can be automatically created, updated or closed.

Included Connectors

Directories

Active Directory and Azure AD; any LDAP; NIS/NIS+

Databases

Oracle; SAP ASE and HANA; SQL Server; DB2/UDB; Hyperion; Caché; MySQL; OLAP and ODBC.

Server OS: X86/IA64

Windows: NT thru 2016; Linux and *BSD.

Server OS: Unix

Solaris, AIX, HP-UX and many others.

Server OS: Mainframes

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

Server OS: Midrange

iSeries (OS400); OpenVMS and HPE/Tandem NonStop.

ERP, CRM and other apps

Oracle EBS; SAP ECC and R/3; JD Edwards; PeopleSoft; Salesforce.com; Concur; Business Objects and Epic.

Messaging and collaboration

Office 365; Lotus Notes/Domino; Google Apps; Cisco WebEx, Call Manager and Unity.

Tokens, smart cards and 2FA apps

Any RADIUS service or SAML IdP; Duo Security; RSA SecurID; SafeWord; Vasco; ActivIdentity and Schlumberger.

Web access management and SSO:

CA SiteMinder; IBM Security Access Manager; Oracle AM; RSA Access Manager and Imprivata OneSign.

Help desk incident management (ITSM):

ServiceNow; BMC Remedy, RemedyForce and Footprints; JIRA; HPE Service Manager; CA Service Desk; Axios Assyst; Ivanti HEAT; Symantec Altiris; Track-It!; MS SCS Manager and Cherwell.

PC drive encryption:

McAfee; CheckPoint; Microsoft BitLocker; Symantec Endpoint Encryption and PGP and Sophos SafeGuard.

HR / HCM

WorkDay; PeopleSoft HR; SAP HCM and SuccessFactors.

Extensible / scriptable:

CSV files; Google Sheets; SCIM; SSH; Telnet/TN3270/TN5250; HTTP(S); SQL; LDAP; PowerShell and Python.

Mobile device management:

BlackBerry Enterprise Server and MobileIron.

Security Incident / Event Management:

Splunk; ArcSight; RSA Envision and QRadar. Any SIEM supporting SYSLOG or Windows events.

Hitachi ID Password Manager is part of the Hitachi ID Identity and Access Management Suite, which also includes: Identity Manager to manage users and groups and Privileged Access Manager to secure administrator, service and embedded accounts and membership in high-risk groups. For more information, please visit: https://hitachi-id.com/ or call: 1.403.233.0740 | 1.877.386.0372