

Hitachi ID Password Manager Features at a Glance

FEATURE: Password Synchronization

Description

Password Manager makes it easy for users to maintain just one or two passwords across all of their login accounts. This can be achieved either by inviting users to change all of their passwords with a web form or by intercepting and extending the native password change process on a system such as Windows.

Benefit

Users with fewer passwords to remember have fewer login problems and are less likely to write down their passwords. Synchronizing passwords can eliminate 80% of password-related login problems and help desk calls.

FEATURE: Enterprise single sign-on

Description

Password Manager can automatically populate login prompts on applications whose ID and/or password is the same as Windows. This process works without having to build and populate password wallets or scripts.

Benefit

Reduced sign-on streamlines user login processes and increases user satisfaction with IT.

FEATURE: Self-Service Password and PIN Reset

Description

Users can access Password Manager from a full-screen or smart phone web browser, from their PC login screen or via a telephone call. They identify themselves and authenticate with any combination of security questions, a random PIN sent via SMS to their mobile phone, their voice print, a one time password token or a smart card. Once authenticated, users can reset their forgotten password, clear an intruder lockout or reset a PIN on their smart card or token.

Benefit

Users can resolve their own login problems, 24x7 without calling the help desk. Password-related calls to the help desk typically decline by about 65%.

FEATURE: Key Recovery for Full Disk Encryption

Description

Users who forgot the password that activates their encrypted PC can call Password Manager on the telephone, authenticate themselves and step through a key recovery process, acting as the intermediary between a challenge/response process at their PC login screen and a key recovery system on the telephone.

Benefit

When a user forgets his HDD encryption password, his PC is effectively a brick. Key recovery lets users recover use of their computer 24x7 without a help desk call.

FEATURE: Self-Service, Anywhere

Description

Access to self-service password reset, intruder unlock, smart card PIN reset, token PIN reset and disk encryption key recovery is available from anywhere. It can be accessed both at and away from the office, over a wired or wireless network, including over WiFi, a VPN and the Internet.

Benefit

Mobile users and users with encrypted PCs need advanced technology to take advantage of self-service. This technology is built into Password Manager.

FEATURE: Assisted Password Reset

Description

IT help desk staff can use Password Manager to authenticate themselves, authenticate a caller, reset passwords and automatically generate an incident / ticket.

Benefit

Efficient call processing accelerates service and lowers costs.

FEATURE: Password Policy Engine

Description

Password Manager enforces a robust password policy, including 50 rules regarding the composition of new passwords, open-ended password history and regular password changes (expiry).

Benefit

Complex yet memorable passwords strengthen security.

FEATURE: Auto-discovery and ID mapping

Description

Password Manager automatically lists login IDs on every integrated system and application, nightly. It supports both automatic, data-driven ID mapping between systems and self-service, so users can attach non-standard IDs to their profile.

Benefit

Automation lowers both the deployment and ongoing support cost of the system.

FEATURE: Managed enrollment

Description

In a typical deployment, users are required to fill-in their profile with answers to security questions, login IDs, their mobile phone number and possibly a biometric voice print sample. The processes for inviting users to do this and the web forms for registration are built-in.

Benefit

A managed enrollment system controls the pace and method of user invitations, both to ensure high adoption and to reduce the nuisance impact of too many e-mails.

FEATURE: Many included integrations

Description

Password Manager includes connectors for over 100 systems and applications, plus flexible agents designed to integrate new ones.

Benefit

Including connectors in the base price and providing a rich set of connectors lowers both the initial and ongoing cost of the system.

FEATURE: Multi-master, replicated architecture

Description

Password Manager includes a data replication layer and can be deployed to multiple servers, at multiple locations, at no extra cost.

Benefit

Built-in support for high-availability and fault-tolerance make Password Manager suitable for enterprise deployments.

FEATURE: Multi-lingual user interface

Description

Password Manager ships with multiple user interface languages and additional ones can be added easily, both by Hitachi ID Systems and customers.

Benefit

A multi-lingual user interface makes Password Manager suitable for international organizations.