Hitachi ID Systems, Inc.

HITACHI
Inspire the Next

Managed Administration Service (MAS):

Hitachi ID Password Manager

Contents

1 Introduction

Hitachi ID Password Manager is an integrated solution for managing credentials across 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 drives.

–

To get the most from their investment in *Password Manager*, organizations must ensure that the system is running smoothly. This means that all of the features and integrations in *Password Manager* work correctly at all times. It also means that users must be aware of the system and take maximum advantage of its features.

To ensure a smoothly running, widely adopted and effective *Password Manager* deployment, organizations must invest in the operation of the system, which includes:

- Server health monitoring.
- Generating and distributing reports about utilization of the system.
- Ongoing surveillance of user adoption and programs to increase user participation.
- Regular software upgrades, to add features and keep up with new integrations.
- Prompt and effective troubleshooting of any issues with the system.

This document describes how organizations can leverage *Managed Administration Service (MAS)*, rather than allocating their own staff to manage their *Password Manager* deployment.

2 Managed Administration Service

2.1 Hitachi ID Systems and customer resources

Customers who sign up for *Managed Administration Service (MAS)* are assigned one primary and one backup product administrator. The product administrator is responsible for the day-to-day monitoring and management of the *Hitachi ID Password Manager* software. Hitachi ID Systems will also designate a project manager during system deployment. A project manager may, at Hitachi ID Systems discretion, also be assigned on an ongoing basis post-deployment, if workload merits.

Customers must designate a primary and a backup application owner (both can be non-technical), with whom the technical Hitachi ID Systems product administrator will coordinate software configuration changes, access to target system administrators, etc.

All customer requests – be they for configuration changes or enhancements, to troubleshoot problems or general inquiries – must be communicated by the designated owner(s) to the product administrator or (if one is assigned) to the project manager. Random customer end users do not have access to the product administrator.

Conversely, all Hitachi ID Systems requests or notifications, for example to request assistance with integrations or to notify the customer of operational problems, will be routed to the designated product owner(s).

The following sections describe the responsibilities of the Hitachi ID Systems product administrator in greater detail.

2.2 System health monitoring

Hitachi ID Systems leverages a log and metric aggregation platform hosted by ElasticSearch to ship log and metric information to Hitachi ID Systems so that its administrators may review and identify issues in realtime.

This platform allows the product administrator to:

1. Carefully review all pertinent logs from recurring batch processes. This includes logs from the auto-discovery, and similar services, as well as logs from services responsible for inter-server replication and database updates.
2. Identify performance trends and anomalies which may point to issues with connected systems or with the hosting infrastructure.
3. Proactively identify and communicate any issues to the customer application owner(s).

2.3 Problem remediation

Timely problem reporting, diagnosis and remediation is essential to successful, routine operation of *Hitachi ID Password Manager*.

The Hitachi ID Systems product administrator:

1. Acts as a single point of accountability, to which customers escalate any and all *Password Manager*-related issues and configuration change requests.
2. Is responsible for troubleshooting any integration or operational issues which may arise with the production *Password Manager* system.
3. Has direct access to Hitachi ID Systems software development and QA staff and can use these resources to expedite problem resolution.

2.4 Upgrades, patches, integrations and customization

On an as-available basis, the Hitachi ID Systems product administrator:

- Applies *Hitachi ID Password Manager* patches (Z increments in version number X.Y.Z), as they become available. This includes implementation on one development instance and migration to one production instance.

  NOTE: “instance” in the foregoing may refer to multiple OS images each of which hosts *Password Manager*, but where each of these running copies of the software replicates with the others, such that there is only a single, logical instance.

On an as-needed basis, the product administrator also:

- Updates existing business logic (i.e., scripts, plug-ins or policy table rule entries) to reflect changes in customer business requirements, as these are communicated to the designated Hitachi ID Systems application administrator by the *Password Manager* business owner.

  NOTE: This is restricted to small changes in policies and rules. Significant changes to system behaviour or large numbers of rule changes may necessitate a change control and separate services engagement, at the discretion of Hitachi ID Systems.

Annually, customers may also request that Hitachi ID Systems:

- Implement at most one minor user interface customization, consisting of a CSS modification or insertion of a logo graphic.
- Add integrations to up to five non-scripted target systems or applications, for which connectors are included in the version of the *Password Manager* application or associated connector packs already deployed.
- If required, subject to Hitachi ID Systems scheduling constraints and at customer expense (i.e., pass-through of direct expenses such as airfare and hotels), visit customers offices once to meet with application owners, for up to 4.5 days.
- Provide advice regarding best practices and user adoption.

At its discretion, Hitachi ID Systems may apply major version number upgrades to the *Password Manager* deployment. In all cases, testing of the changes in a separate instance followed by production migration will be in coordination with customer staff, in accordance with existing change control procedures and will allow time for the customer team to validate functionality and integrations on the new version prior to production migration.

2.5 Reports and audits

Provide reports, via e-mail, to the application business owner. These reports, delivered monthly, will cover:

1. The number of users who have signed into the *Hitachi ID Password Manager* web UI during the month, broken down by authentication method.
2. The number of users who have completed enrollment and a list of those users.

3. The number of users who have a profile on the system and a list of those users.
4. Password change transaction volumes for the calendar month.
5. Token PIN reset transaction volumes for the calendar month, if applicable.
6. Smart card PIN reset transaction volumes for the calendar month, if applicable.
7. Encrypted drive unlock transaction volumes for the calendar month, if applicable.
8. Password/PIN reset transaction volumes for the calendar month, for remote users over application-initiated VPN, if applicable.
9. Federated logins initiated through the system for the calendar month, per Security Assertions Markup Language (SAML) service provider (SP).
10. The configuration of all user classes.
11. A detailed report of errors due to *Password Manager* attempting to connect to, enumerate accounts or groups on and managing passwords, accounts or entitlements on integrated systems.
12. A list of system faults that the Hitachi ID Systems administrator has identified and resolved.

2.6 Exclusions

The product administrator will be responsible for maintaining and managing the *Hitachi ID Password Manager* application itself. Hitachi ID Systems will not be responsible for maintenance or support of on-premises infrastructure that supports *Password Manager*, such as connector proxy VMs or firewall configuration at or within the customers network perimeter.

As the customer will host the application on its own infrastructure, the customer will be responsible for:

1. Hardware or VM/hypervisor support.
2. Operating system support, including OS patches.
3. Network infrastructure support, including troubleshooting routing, DNS or load balancing problems directly relating to the application or where it is hosted.

If there are network problems in the customers environment, such as with users reaching the *Password Manager* UI or with *Password Manager* reaching target systems, these must be resolved by the customers IT team.

While the product administrator will be responsible for troubleshooting integration problems with systems and applications where *Password Manager* is configured to manage users, credentials or entitlements, such troubleshooting will of necessity require close collaboration with individual system and application administrators.

3 Benefits

3.1 Lower total cost of operations (TCO)

1. *Managed Administration Service (MAS)* eliminates the need for organizations to hire, train and retain internal resources to manage *Hitachi ID Password Manager*. The cost of internal resources vary from one organization to the next, but assuming a total cost of US$100,000/year for an employee, including benefits and other non-salary expenses and assuming allocation of 1.0FTE, then *MAS* can eliminate an annual US$100,000 expense.
2. *MAS* includes some services which many organizations contract professional services to perform, such as UI customizations, version upgrades and adding target systems. While the scope of such services is limited, inclusion of these services in the scope of the *MAS* agreement can replace a customers consulting expense of about US$20,000 annually.

3.2 Increased value

1. The value of a *Hitachi ID Password Manager* deployment depends on user adoption. Hitachi ID Systems product administrators have expertise with deploying *Password Manager*, managing user enrollment and maximizing user adoption.
2. Assuming a modest increase of 10% in user adoption as compared to a self-managed deployment, an organization with 10,000 users can save US$60,000/year. This is based on an average help desk call costing $30 and an average of two password-related help desk calls, per year, from each user who does not use *Password Manager*.
3. The above cost savings manifest as lower call volume at the help desk, which customers may translate to staff reduction, reassignment or deferred hiring.

3.3 Stronger security

1. *Hitachi ID Password Manager* itself is more secure, thanks to regular patches and version upgrades. Any security issues discovered by Hitachi ID Systems or its customers are be resolved and applied to running systems promptly.
2. Maximizing the user adoption of *Password Manager* ensures that password policy, history and expiry are applied effectively to all users.
3. Synchronizing passwords for all users reduces risks due to written, shared and static personal passwords.
4. Enrolling answers to security questions from all users makes it harder for attackers to impersonate a legitimate user during a call to the help desk.

4 Terms and conditions

4.1 Service pre-requisites and exclusions

1. *Managed Administration Service (MAS)* is provided per *Hitachi ID Password Manager* instance. An instance may span multiple servers (VMs) but supports a single user population, a single set of integrations and has a single configuration.

2. Customers must have a current maintenance contract or in-effect lease for *Password Manager*.

3. Customers must provide the product administrator with appropriate administrator-level credentials to each *Password Manager* server at the operating system and database levels.

4. Hitachi ID Systems staff must have independent VPN access to the on-premises network where integrated systems and applications are found, on a 24x7x365 basis. In addition, administrative credentials to the host OS where *Password Manager* is installed must be provided to the Hitachi ID Systems team.

5. Customers must designate two contacts (application owners) with whom Hitachi ID Systems will coordinate all work. Only these owners will contact Hitachi ID Systems to make inquiries or request changes (not the entire customers user population).

6. Customers must provide test or development instances of each integrated system or application, to validate integrations both initially and whenever patches or upgrades are applied.

7. The customer must provide VMs where a test instance of the *Password Manager* software will be installed, to validate new configurations and versions.

8. All production changes are subject to the customer change control process.

9. Product version upgrades (e.g., X or Y change in version X.Y.Z) may require a separate professional services engagement and are not automatically included in the periodic version upgrade process.

10. Development of custom business logic is excluded from this service.

11. Deployment or monitoring of software components on systems other than *Password Manager* servers is excluded from this service. This means both client code (ActiveX, Windows Credential Provider (CP), etc.) and server-side agents on integrated systems (Mainframe listener, Unix listener, etc.) are to be supported by Hitachi ID Systems and the customer collaboratively, outside the scope of *MAS*.

12. Hitachi ID Systems will transmit log and performance data of the system to our log and metric aggregation platform. Some information such as attribute values, account/profile names and other PII may be contained in the logs transmitted. The data is stored and transmitted in an encrypted manner, and access controlled and available only to Hitachi ID Systems product administrators. Log and performance data is retained for up to 1 year.

13. Hitachi ID Systems currently uses ElasticSearch cloud as a log and metric aggregation platform, but may from time to time use other providers for commercial or jurisdictional reasons. In general, Hitachi ID Systems will pass through any terms and conditions from these data processors including security assessments and/or certifications of the platform. Terms for ElasticSearch cloud can be found here:

    - https://www.elastic.co/agreements/bc/cloud
    - https://www.elastic.co/pdf/agreements/dpa/elastic-cloud-gdpr-data-processing-addendum.pdf

5 Find Out More

Please contact your Hitachi ID Systems account representative or e-mail sales@Hitachi-ID.com to learn more about this service and to request a price quotation.

Hitachi ID Systems, Inc.
500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 E-Mail: sales@hitachi-id.com