

© Hitachi ID Systems, Inc.



Service Offering:
Outsourced IdM Administrator Service

Contents

- 1 Introduction 1**

- 2 The Outsourced IdM Administrator Service 1**
 - 2.1 Hitachi ID and Customer Resources 1
 - 2.2 Server Health Monitoring 1
 - 2.3 Problem Remediation 2
 - 2.4 Upgrades, Patches, Integrations and Customization 2
 - 2.5 Reports and Audits 2
 - 2.6 Exclusions 3

- 3 Service Benefits 3**
 - 3.1 Lower Total Operating Cost (TCO) 3
 - 3.2 Increased Value 3
 - 3.3 Stronger Security 4

- 4 Terms and Conditions 4**
 - 4.1 Service Limitations and Exclusions 4
 - 4.2 Legal Liability 5

- 5 Find Out More 5**

1 Introduction

Hitachi ID Password Manager (formerly P-Synch™) enables customers to more effectively manage passwords and other authentication factors. This helps organizations lower IT support cost, increase user productivity and strengthen network security.

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

To ensure a smoothly running, widely adopted and effective Password Manager deployment, organizations must provide for:

- Server health monitoring.
- Ongoing surveillance of user adoption and programs to increase user participation.
- Periodic software upgrades, to add features and keep up with new integrations.
- Prompt and effective troubleshooting of any issues that may come up.

This document describes how organizations can leverage the Outsourced IdM Administrator Service, in lieu of internal resources, to address these requirements and deliver maximum benefit from their investment in Password Manager.

2 The Outsourced IdM Administrator Service

2.1 Hitachi ID and Customer Resources

Customers who sign up for the Outsourced IdM Administrator Service will be assigned one primary and one backup Hitachi ID Password Manager administrator. The Hitachi ID Password Manager administrator will take on the day-to-day monitoring and management of the Password Manager software on the customer's network.

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

The following sections describe the responsibilities of the Hitachi ID Password Manager administrator in greater detail.

2.2 Server Health Monitoring

1. Receive and carefully review a daily e-mail from the Hitachi ID Password Manager servers, including all pertinent logs from the nightly auto-discovery process.

2. Communicate any issues to the customer's application owner.

2.3 Problem Remediation

1. Act as a single point of accountability, to which the customer should escalate any and all Hitachi ID Password Manager-related issues and configuration change requests.
2. Be responsible for troubleshooting any integration or operational issues which may arise with the Password Manager application.
3. Have direct access to Hitachi ID software development and QA resources and will take advantage of this to expedite problem resolution.

2.4 Upgrades, Patches, Integrations and Customization

On an as-available basis:

1. Apply Hitachi ID Password Manager patches (Z increments in version number X.Y.Z), as they become available. This includes implementation on a development system and production migration, if applicable to the customer's change control process.
2. Apply security or performance patches to Password Manager.

Annually:

1. Implement at most one minor user interface customization, consisting of a CSS modification or insertion of a logo graphic.
2. Add integrations to up to five non-scripted target systems or applications, for which connectors are included in the base Password Manager software or any connector packs released by Hitachi ID.
3. On the customer's invitation, subject to Hitachi ID scheduling constraints and at the customer's expense (charge through of travel expenses), visit the customer's offices once to meet with the customer staff, for up to 4.5 days.
4. Provide advice to the customer regarding best practices for use of Password Manager and guidance regarding how to maximize user adoption.

2.5 Reports and Audits

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

1. The number of users who have completed enrollment and a list of those users.
2. The number of users who have a profile on the system and a list of those users.

3. Transaction volumes for the calendar month.
4. A list of all error messages produced by the system during the month.
5. A list of system faults that the Hitachi ID administrator has identified and resolved.

2.6 Exclusions

The Hitachi ID Hitachi ID Password Manager administrator will be responsible for maintaining and managing the Password Manager application itself and not the underlying infrastructure that supports it. For clarity, following are items for which the Hitachi ID Password Manager administrator will not be responsible:

1. Hardware support.
2. Operating system support, including OS patches.
3. Network infrastructure support, including troubleshooting routing, DNS or load balancing problems on the customer's network.

3 Service Benefits

3.1 Lower Total Operating Cost (TCO)

1. The Outsourced IdM Administrator Service eliminates the need for the customer 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 \$100,000/year for an employee, including all benefits and other non-salary expenses and assuming allocation of 0.5FTE, then the Outsourced IdM Administrator Service can eliminate an annual \$50,000 expense.
2. The Outsourced IdM Administrator Service includes services which many Hitachi ID customers contract professional services to perform, such as UI customizations, version upgrades and adding target systems. Inclusion of these services in the Outsourced IdM Administrator Service can replace a services expense of about \$20,000 annually.
3. By outsourcing server management, the customer can eliminate the need to train its own administrators – typically one primary and two backup administrators would have to attend training.

3.2 Increased Value

1. The value of a Hitachi ID Password Manager deployment depends on user adoption. Hitachi ID's administrators have expertise with deploying Password Manager, with managing user enrollment and with 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 \$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 will manifest as lower call volume at the help desk, which customers may translate to staff reduction, staff reassignment or deferred hiring at the help desk.

3.3 Stronger Security

1. Hitachi ID Password Manager itself will be more secure, thanks to regular patches and version upgrades. Any security issues discovered by Hitachi ID or by other Hitachi ID customers will be resolved and applied to the customer's systems promptly.
2. Increasing the user adoption of Password Manager will ensure that password policy, history and expiry are applied effectively to all users.
3. Synchronizing passwords for all users addresses the risks due to written passwords.
4. Enrolling challenge/response data from all users will eliminate social engineering attacks against user profiles, through the help desk support process.

4 Terms and Conditions

4.1 Service Limitations and Exclusions

1. The Outsourced IdM Administrator Service offering is provided per Hitachi ID Password Manager instance. An instance may span multiple servers but supports a single user population, a single set of integrations and has a single configuration.
2. Customers must have a current maintenance contract for Password Manager.
3. Customers must provide the Password Manager administrator with appropriate administrator-level credentials to each Password Manager server.
4. VPN software must be installed and running on each Password Manager server with 24x7x365 availability.
5. Customers must designate two contacts (application owners) responsible for communication of issues.
6. Customers must have a staging environment to allow testing of enhancements and patches before migration to production.
7. All production changes are subject to the customer change control process.
8. Major product version upgrades (e.g., X changes in X.Y.Z) may require a separate professional services engagement and are not included in annual version upgrades.
9. Development of custom business logic is excluded from this service.
10. Deployment or monitoring of desktop software is excluded from this service.

4.2 Legal Liability

This document is for informational purposes only. Hitachi ID Systems, Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. The terms and conditions of this service are governed by the Administrative Service SLA. This is separate from the Support SLA.

5 Find Out More

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