

Using Hitachi ID Password Manager

to Reduce Password Reset Calls
at an Internet Service Provider



Internet Service Providers face a significant support cost due to users who forget their network connection or e-mail password.

As ISPs scale to hundreds of thousands and millions of end customers, the cost to support repetitive problems such as password resets rises to significant levels, reaching millions of dollars annually.

Given the significant cost, it is advantageous to invest in automation to eliminate recurring user support problems. Password reset is often the most common problem, and is arguably the easiest problem to address with self-service technologies.

Contents

- 1 Introduction** **1**

- 2 Password reset as a recurrent support call** **2**
 - 2.1 The problem 2
 - 2.2 Types of passwords 2
 - 2.3 Initial vs. ongoing problems 2
 - 2.4 Cost model 3

- 3 The Password Manager password management system** **4**

- 4 Using Password Manager to reduce ISP call volume** **4**

- 5 Deployment challenges and design choices** **6**
 - 5.1 Scalability 6
 - 5.2 Connectivity 6
 - 5.3 User education 7
 - 5.4 Integration 7

- 6 Architecture, scalability and integration** **8**
 - 6.1 Scalability 8
 - 6.2 Proposed architecture 8
 - 6.3 Integration with RADIUS servers 9

- 7 Projected ROI** **11**
 - 7.1 Cost recovery model 11
 - 7.2 Rapid deployment: buy vs. build 12

1 Introduction

Internet Service Providers face a significant support cost due to users who forget their network connection or e-mail password.

As ISPs scale to hundreds of thousands and millions of end customers, the cost to support repetitive problems such as password resets rises to significant levels, reaching millions of dollars annually.

Given the significant cost, it is advantageous to invest in automation to eliminate recurring user support problems. Password reset is often the most common problem, and is arguably the easiest problem to address with self-service technologies.

The remainder of this paper is organized as follows:

- **Password reset as a recurrent support call**

Background describing why password resets are a significant cost problem for large ISPs.

- **The Hitachi ID Password Manager password management system**

A general description of the Password Manager password management system.

- **Using Password Manager to reduce ISP call volume**

A specific description of how Password Manager is relevant to customer support in a large ISP.

- **Deployment challenges and design choices**

Specific design and deployment problems raised in an ISP environment, with many users, large support volume, and little or no opportunity for user training.

- **Architecture, scalability and integration**

A network architecture to leverage Password Manager for password management in an ISP environment.

- **Projected ROI**

A cost recovery model for effective password management in an ISP environment.

- **Conclusions**

Summary of the above discussion, and a call to action: deploy password management quickly in order to recoup maximum value.

2 Password reset as a recurrent support call

2.1 The problem

Consolidation in the ISP business is producing ISPs with large user populations – ranging from hundreds of thousands to millions.

When ISP subscribers experience technical problems, they either access a subscriber service web site or call a support line. Problems that disrupt Internet access are clearly not amenable to resolution with a self-service site, and so drive support call volume.

One recurring problem that causes connectivity problems is a forgotten or mistyped password. Users who must type a current password to connect to the network may forget their password, and consequently be unable to connect. These users invariably call for service.

Even if password problems are relatively infrequent for a single user (e.g., occurring annually or even less often), as the user population scales the cost becomes significant. For example, an ISP help desk that resolves 30,000 password problem calls monthly, and where such calls only cost \$10 to resolve,¹ will incur a total annual charge of \$3,600,000 to service this problem.

2.2 Types of passwords

ISP subscribers generally have at least two types of passwords:

- Network connection passwords, used by dial-up, PPPoE and other client connectivity software to attach to the network.
- E-mail and other application passwords.

A single subscriber will often have multiple e-mail accounts attached to a single network access account.

Connection passwords are problematic because their impact is to prevent a user from connecting to the network. Users who forgot their connection passwords cannot access the ISP web site, and so cannot use a web-based self-service password reset system.

E-mail and other application passwords are easier to manage because users can access a self-service web application to address problems with them.

2.3 Initial vs. ongoing problems

Subscribers may have password problems when their initial network connection is configured, or thereafter.

If the problem is when making the initial network connection, no assumptions can be made about the configuration of the subscriber's workstation or about any agents installed on that computer.

¹Gartner and Metagroup figures estimate \$25 to \$35 per call for this type of problem in internal corporate help desks

If the problem occurs subsequent to initial, successful configuration, then client software may have been made available on the subscriber's computer, and may be used to assist in an automated problem resolution process.

2.4 Cost model

The cost of password problems can be calculated using the following variables:

Variable	Units	Description
$P_{initial}$	Number/month	Number of password problems per month that take place during subscriber activation.
$P_{ongoing}$	Number/month	Number of password problems per month that affect already-configured subscribers.
$C_{initial}$	\$/problem	Cost of password problems at activation time.
$C_{ongoing}$	\$/problem	Cost of password problems affecting configured subscribers.
C_{annual}	\$/year	Total cost of password problems per year.

$$C_{annual} = 12 \times (P_{initial} \times C_{initial} + P_{ongoing} \times C_{ongoing}) \quad (1)$$

For instance, consider an example ISP where:

Variable	Value
$P_{initial}$	20000/month
$P_{ongoing}$	10000/month
$C_{initial}$	\$20
$C_{ongoing}$	\$10

$$C_{annual} = 12 \times (20000 \times 20 + 10000 \times 10) = \$6,000,000/\text{year} \quad (2)$$

3 The Password Manager password management system

Hitachi ID Password Manager is an enterprise solution for managing passwords and other authentication factors. It improves the security of passwords and related IT support processes, reduces the cost of user support and improves user productivity. This is done with features such as password synchronization, self-service password reset, enterprise single sign-on, PIN resets for tokens and smart cards, enrollment of security questions and biometrics and emergency recovery of full disk encryption keys.

Password Manager reduces the cost of password management using:

- Password synchronization, which reduces the incidence of password problems for users
- Self-service password reset, which empowers users to resolve their own problems rather than calling the help desk
- Streamlined help desk password reset, to expedite resolution of password problem calls

Password Manager strengthens security by providing:

- A powerful password policy engine.
- Effective user authentication, especially prior to password resets.
- Password synchronization, to help eliminate written-down passwords.
- Delegated password reset privileges for help desk staff.
- Accountability for all password changes.
- Encryption of all transmitted passwords.

To find out more about Password Manager, visit <http://Password-Manager.Hitachi-ID.com>.

4 Using Password Manager to reduce ISP call volume

Hitachi ID Password Manager can be used to reduce the volume of password problem calls that reach an ISP's support desk as follows:

- Initial problems:

- **Self-service password reset with a telephone**

- When users dial the ISP's help desk line, the automated call director (ACD) system can drive their calls to a self-service password reset system.

- This system can prompt users to key in personal information, such as their account number, telephone number and any other personal identification that they provided when they first signed up for their account.

Callers key in answers to these questions using a touch-tone telephone. Once authenticated, users are asked to confirm that they want a new password, and when they confirm, a random password is generated and read out to them. Users confirm that they have heard and either entered or written down their new password. Once confirmed, the new password is applied to the user's account (and in particular to the connection authentication system).

- Ongoing problems:

- **Password synchronization**

Users can be periodically prompted, by e-mail, to change their passwords. Users who get this e-mail can click on a URL embedded in their e-mail to do so. Password Manager presents users with a web GUI, where they authenticate with their current ID and password, and select a new password.

New passwords can be applied to multiple IDs attached to the same subscriber's profile. Typically, the main subscriber would change both the connection and his/her own e-mail password, while subsidiary subscribers would only be able to change their own e-mail password.

The ability to set multiple passwords to a single value is synchronization. Users who manage their multiple passwords in a routine, managed fashion tend to have fewer problems, and generate fewer calls.

- **Self-service password reset with a telephone**

The same process described above can be used to help configured users who forgot their connection password to reset it from any telephone.

- **Self-service password reset with a web browser**

Users who only forgot an e-mail password, and are already connected, can authenticate to the service either with their current password or with some non-password data, and can reset their own e-mail password.

Users who have connected to the Internet, either directly or using a different computer (work, neighbor, etc.) can reset both connection and e-mail passwords after providing suitable non-password authentication.

The Password Manager service can enforce password policies over new passwords. It supports rules for length, composition, history, dictionary words, etc.

Users who forget their password, and wish to perform a self-service password reset, must provide some non-password authentication. This normally means that they must answer a sequence of personal or secret questions.

Data for non-password user authentication may be collected by Password Manager itself, or accessed on existing systems (e.g., subscriber billing system, subscriber account database, etc.). Where Password Manager is configured to collect new or supplementary authentication data, it generally prompts users to register by e-mail, and users respond by clicking on a URL embedded in their e-mail; entering their login ID and current password; and filling in blank answers on a Q&A form.

5 Deployment challenges and design choices

Providing password management in general, and self-service password reset in particular, is challenging in an ISP environment:

5.1 Scalability

A population of hundreds of thousands of users will generate tens of thousands of password resets per month. These problems normally occur during “prime time” for residential subscribers – a 4 hour/day block in the evenings.

Consider an ISP that generates 30,000 password problems/month. Assume that half of these problems happen during a four hour peak period, on week-days:

$$RATE_{peak} = (30000 \times \frac{1}{2}) / (4 \times 5 \times 4) = 187/hour. \quad (3)$$

From this analysis, it is clear that a password management system must be able to handle at least hundreds, and perhaps thousands of subscriber login sessions per hour.

A password management system deployed by an ISP must also support at least hundreds of thousands of users, each of which may have multiple login IDs on multiple managed systems (connection, e-mail, etc.).

5.2 Connectivity

Users who experience a password problem while not connected must either get service on a telephone or must use client software that automatically connects to the network with some special access, resolves the user’s problem, and disconnects.

The diversity of subscriber workstation types (Windows 9x, Windows NT, Windows 2000, Windows XP, MacOS, Linux, etc.) , combined with the many types of dial-up software (built-in RAS, PPPoE dialers, etc.) make the implementation of a dial-fix-and-hangup client program very difficult.

A client-side dialer may be difficult to deploy, but client-side and possibly personalized instructions are appropriate. It is not unreasonable for software installed on the client software to include instructions about:

- How to identify a password problem, as opposed to a different connectivity problem. (e.g., symptoms, screen shots, explanations, etc.)
- How to resolve e-mail password problems on-line (including a URL to the system, ideally with the client ID already embedded).
- How to resolve dial-up or broadband connection/authentication password problems using a telephone (including phone number to dial, digits the user must press to navigate through the system, digits the user must press to identify himself, etc.).

These instructions may be personalized at installation time to refer to the subscriber's local support dial-up number, the subscriber's personal account number, etc.

5.3 User education

Any self-service problem resolution system targeted at a consumer population must be tolerant of subscribers who are not very computer literate. Consumer-oriented systems do not have the luxury of roll-out with a user education program.

As a result, a password management system for consumers should be extremely easy to use, intuitive, and require little or no explanation.

5.4 Integration

A password management system deployed at an ISP must obviously manage passwords on the ISP's authentication infrastructure. This typically means LDAP directories and RADIUS services from various vendors.

6 Architecture, scalability and integration

6.1 Scalability

Hitachi ID Password Manager has been deployed in very large organizations, including:

- One password reset system supporting 750,000 users and another supporting more than 2,000,000 users (both Extranet-facing).
- Internal corporate deployments with up to 300,000 users.
- Users distributed over six continents (nobody in Antarctica).
- A single Password Manager instance, running on a single server, managing passwords on over 3,200 stand-alone Unix systems.

This level of scalability is a result of many features:

- Built-in data replication.
- Explicit support for load-balanced configurations with cooperation between replica servers.
- Multi-threading operation of the UI components, service components and connectors.
- A local, high-performance database that contains easily accessed data about users, including their security questions and various login IDs.

In addition, Password Manager incorporates many features that, while not directly performance-related, are needed to operate in large, complex networks:

- Compatibility with reverse web proxies, which can expose some or all of the Password Manager UI to less-trusted network segments (e.g., DMZ).
- A proxy server, which allows Password Manager to operate across firewalls.
- Support for multiple languages (including Unicode) per running instance.
- Auto-discovery of users and groups on integrated systems.

6.2 Proposed architecture

Following is a network architecture diagram for deployment of Hitachi ID Password Manager in an ISP environment:

In the diagram:

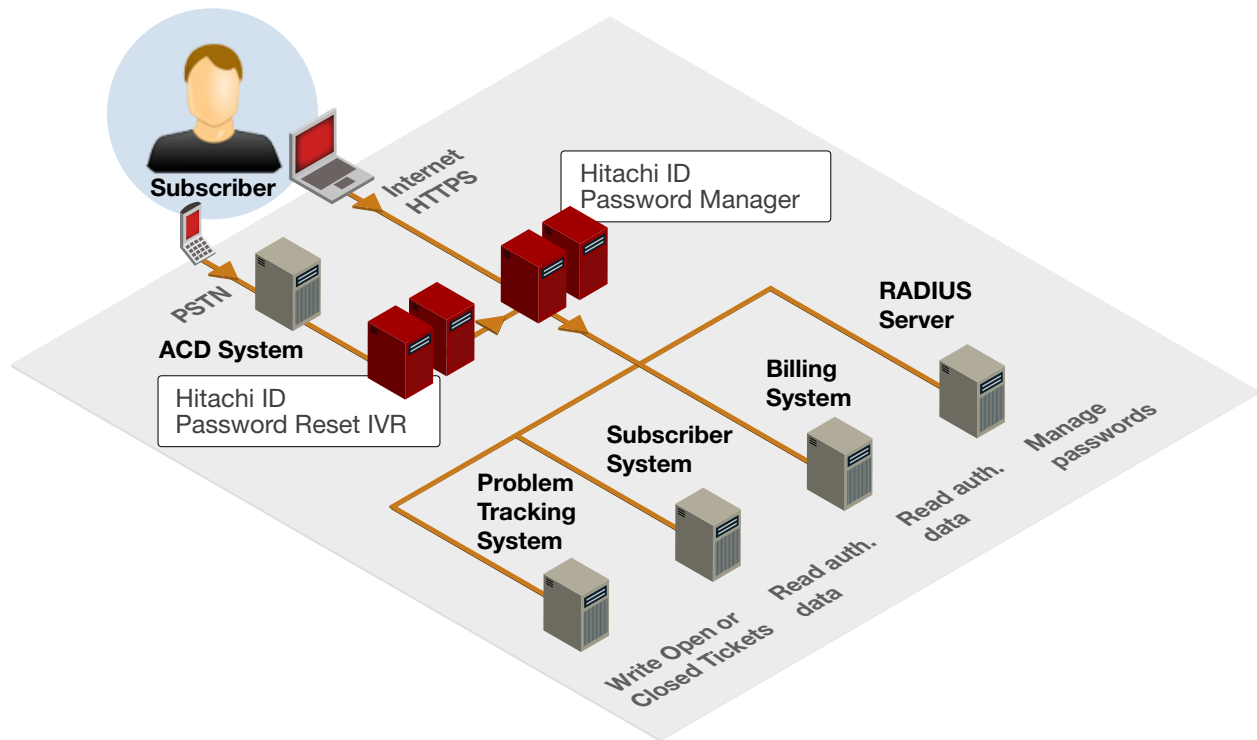


Figure 1: Password Manager Service Provider Architecture Diagram

- There are multiple, redundant, replicating and load-balancing Password Manager servers.
- An ACD directs incoming calls to one or more IVR servers which service password reset problems. The IVR servers present a voice interface, but otherwise access user authentication and password reset functions through Password Manager.
- Password Manager manages passwords on one or more target systems, which are most likely running vendor RADIUS implementations.
- Password Manager accesses authentication data about users on existing billing and subscriber information databases or directories.
- Password Manager can write open or closed tickets to a problem management system, as appropriate.

6.3 Integration with RADIUS servers

Hitachi ID Password Manager can manage passwords on many types of systems, including:

- Unix passwords, in `passwd`, `shadow`, `NIS`, `NIS+` or `Kerberos` formats.
- Passwords on any standards-compliant LDAP directory (Sun/iPlanet, Novell/eDirectory, IBM/Tivoli, OpenLDAP, Critical Path, etc.).

- Passwords on Windows NT or Windows 2000 AD domains.
- Connect passwords to databases such as Oracle.
- Passwords maintained in an application table on a DBMS such as Oracle.

7 Projected ROI

7.1 Cost recovery model

The return on investment (ROI) for an ISP deploying Hitachi ID Password Manager is entirely due to call redirection and avoidance. In turn, these figures depend heavily on user adoption rates.

Extending the cost model in [Subsection 2.4](#) on Page 3, we define two new variables to model user adoption rates:

Variable	Units	Description
$A_{initial}$	fraction	User adoption rate for self-service problem resolution at network activation time.
$A_{ongoing}$	fraction	User adoption rate for self-service problem resolution for configured subscribers.
S_{annual}	\$/year	Projected annual cost savings.

$$S_{annual} = 12 \times (A_{initial} \times P_{initial} \times C_{initial} + A_{ongoing} \times P_{ongoing} \times C_{ongoing}) \quad (4)$$

Extending the example from [Subsection 2.4](#) on Page 3, using very conservative user adoption rates:

Variable	Value
$A_{initial}$	25%
$A_{ongoing}$	35%

$$C_{annual} = 12 \times (0.25 \times 20000 \times 20 + 0.35 \times 10000 \times 10) = \$1,620,000/\text{year} \quad (5)$$

Clearly, this is a significant cost savings.

As user adoption rates escalate, cost savings increase. Continuing with the same examples, if user adoption rates can be increased:

Variable	Value
$A_{initial}$	40%
$A_{ongoing}$	75%

$$C_{annual} = 12 \times (0.40 \times 20000 \times 20 + 0.75 \times 10000 \times 10) = \$2,820,000/\text{year} \quad (6)$$

7.2 Rapid deployment: buy vs. build

As illustrated in both [Subsection 2.4 on Page 3](#) and [Section 7 on Page 11](#), the problem of password resets is a costly one for ISPs.

Cost savings from a password reset system are substantial – in our example of an ISP that fields 30,000 password problems per month, cost savings range from \$1.6M/year to \$2.8M/year, based on user adoption rates.

Given the rate of cost recovery, it makes sense to deploy a solution very quickly. In particular, once the decision to automate password problem resolution is made, every month of waiting time until the solution is deployed costs from \$130k to \$230k.

This rapid ROI is a strong motivation to purchase a pre-built solution, which can be deployed quickly (2-3 months), rather than developing a custom solution, which may take 6-18 months. The ROI lost during development of a program to compete with a commercial solution would more than offset the cost of the commercial product.

8 Conclusions

Password reset problems are a costly, recurring problem at most I.T. help desks, including customer support lines in an ISP.

Password reset problems are relatively simple to resolve using automation, where a user either dials into an IVR server with a telephone or accesses a self-service web site; identifies himself; authenticates himself; and resets his own passwords.

Hitachi ID Password Manager is a mature password management system, which can scale to address the challenging technical and usability requirements of a large ISP.

Deployment of Password Manager in a large ISP with several hundreds of thousands of subscribers can yield cost savings on the order of \$1M to \$3M/year.

The bottom line is that effective password management technology can be deployed very quickly (2-3 months), and yield significant cost savings to an ISP, with time-to-ROI measured in months.