

Integrating Hitachi ID Management Suite

with WebSSO Systems



Web single sign-on (WebSSO) systems are a widely deployed technology for managing user authentication and access control across multiple web applications. These systems help companies to effectively manage users on both Intranets and Extranets.

WebSSO and password management systems are sometimes perceived as redundant. In reality, they are complementary tools, with almost no overlapping functionality. Integrating WebSSO systems with password management and provisioning tools provides increased value to organizations with heterogeneous systems.

WebSSO systems are effective tools for managing authentication and access control, but are limited to on web applications. Password management and access provisioning systems extend these capabilities to legacy systems, network operating systems, e-mail systems and more.

Integrating WebSSO systems, password management and account provisioning products yields maximum value for identity management.

This document discusses how Management Suite can be deployed in conjunction with WebSSO products, how the technologies interact, and how they complement one another.

Contents

- 1 Introduction** **1**

- 2 WebSSO systems defined** **2**
 - 2.1 User directory 2
 - 2.2 Central and delegated administration 2
 - 2.3 Shared authentication infrastructure 2
 - 2.4 Access control 2
 - 2.5 WebSSO as an HTTP proxy 3
 - 2.6 Common WebSSO systems 3

- 3 Password and access management systems defined** **4**
 - 3.1 Password management systems defined 4
 - 3.2 Access management systems defined 5

- 4 Common components and processes** **6**

- 5 Differences between WebSSO and Password Manager / Identity Manager** **6**

- 6 The value of integration** **7**
 - 6.1 What WebSSO systems do well 8
 - 6.2 What WebSSO systems cannot do 8

6.3	Filling the WebSSO capability gap	8
6.4	Better self-service password reset for web applications	8
6.5	Change authorization workflow for the enterprise	9
7	Summary	10
8	References	10

1 Introduction

Integrating WebSSO systems, password management and account provisioning products yields maximum value for identity management.

This document is organized as follows:

- **WebSSO systems defined:**
A brief definition of WebSSO products.
- **Password and access management systems defined**
A brief definition of what password management and access management systems do.
- **Common components and processes:**
Some software components and processes that WebSSO systems have in common with password and account management tools such as Hitachi ID Password Manager and Hitachi ID Identity Manager.
- **Differences between WebSSO and Password Manager / Identity Manager**
Key features of WebSSO systems that are not found in password or access management systems, and key features of password and access management systems that are absent in WebSSO systems.
- **The value of integration:**
How integration between a WebSSO system and Password Manager/Identity Manager yields value to enterprise organizations.
- **Summary**
Summarizing how Password Manager and Identity Manager complement WebSSO systems.
- **References:**
Useful reference material.

2 WebSSO systems defined

WebSSO systems, also known as Web Access Management (WAM) systems, are used to manage users across multiple web applications. They separate user authentication and access control from other application infrastructure, in order to share the same security data and enforcement mechanism between multiple web servers and applications.

2.1 User directory

WebSSO systems typically maintain a database of users, their authentication (e.g., passwords, tokens and/or personal questions and answers), and their privileges. This database may exist in an LDAP directory or a relational DBMS.

2.2 Central and delegated administration

WebSSO systems normally include facilities for centralized, delegated and self-service administration of the directory and of user privileges. Centralized administration is used to configure the system, delegated administration allows designated people to manage subsets of the user population, and self-service management lets users perform routine tasks on their own profiles, such as updating personal information or resetting a forgotten password.

2.3 Shared authentication infrastructure

WebSSO systems include components that plug into most web servers, intercept attempts by users to access pages, and:

- Allow the request to be processed; or
- Block the user from accessing the page; or
- Divert the as-yet unauthenticated user to a sign-on page, where the user will log in, and be returned to the page he initially asked for.

This process provides for single sign-on across multiple web applications.

2.4 Access control

WebSSO systems typically also provide an API, where web applications can make function calls to determine whether a given user is allowed to perform a given task. Authorization decisions may incorporate policies, roles, user attributes, organization rules, etc.

2.5 WebSSO as an HTTP proxy

Some WebSSO systems (e.g., Evidian) are able to act as web proxies, intercept HTTP requests, authenticate users, and insert credentials into the HTTP stream sent to web applications.

This approach has the benefits of simple deployment without impacting the configuration of existing web application servers and support for externally hosted applications and consumer-oriented web sites where it would be impossible to insert an authentication agent.

2.6 Common WebSSO systems

Some of the most common WebSSO systems are Netegrity SiteMinder, Oblix NetPoint and IBM/Tivoli Access Manager for e-business.

Please refer to [Section 8](#) on [Page 10](#) for a full list and links to each vendor's web site.

3 Password and access management systems defined

Another class of tools targeted at medium to large organizations streamline heterogeneous management of passwords, provisioning of login access, and termination of that access:

3.1 Password management systems defined

Password management systems are designed to reduce the cost of ownership of password-based authentication, and to improve the security of password authentication.

Hitachi ID Password Manager is a password management system that supports:

- Password synchronization, both automated and web-based, to reduce the password management burden on users.
- Self-service password reset, allowing users to reset their own passwords if they forget them or trigger an intruder lockout, without calling the help desk.
- Assisted password reset, which streamlines resolution of password problem calls made to the help desk.

Password Manager yields cost savings by:

- Reducing the frequency of password problems (synchronization).
- Diverting password problem calls away from the help desk (self-service reset).
- Shortening password call resolution at the help desk (assisted reset).

Password Manager improves authentication security by:

- Reducing the number of written passwords (synchronization).
- Enforcing strong, global password quality rules.
- Enforcing sound authentication prior to all password resets.
- Encrypting all network traffic and data storage related to password management.
- Making it possible to delegate the password reset privilege to support analysts without giving them other rights.

3.2 Access management systems defined

Access management systems are designed to streamline changes to user access to systems. They reduce the delay between organizational change and matching changes in user access to I.T. infrastructure, and ensure that user access is terminated once it is no longer required.

Hitachi ID Identity Manager is an access management system that supports:

- A web + mail workflow system for entering change requests, routing them to authorizers, reviewing and approving change requests, and automatically updating system access based on approved requests.
- An automated, rules-based system that monitors organizational changes on other systems (e.g., H.R. system) and makes matching updates to login systems.
- A web-based central administration system where a security officer can make global changes to user access rights, across heterogeneous systems.

Identity Manager yields cost savings by:

- Reducing the time users must wait for new or changed access.
- Reducing the number of security administrators that must be engaged to manage systems access changes.
- Streamlining system migrations.
- Cleaning up orphan accounts, which can reduce software license costs.

Identity Manager improves access security by:

- Ensuring effective and rapid access termination.
- Removing orphan accounts.
- Enforcing standards when creating new users.
- Enforcing proper authorization rules on all changes.
- Maintaining a forensic change and audit log for all changes.

4 Common components and processes

WebSSO products and Hitachi ID Password Manager / Hitachi ID Identity Manager share some common components:

- An overall objective of simplifying user authentication across multiple systems.
- The ability to delegate the right to reset passwords to designated people: either support staff or local administrators.
- The ability to delegate the right to create, update and delete accounts.
- Support for self-service password resets.

5 Differences between WebSSO and Password Manager / Identity Manager

Beyond some superficial similarities, WebSSO products and Hitachi ID Password Manager / Hitachi ID Identity Manager use different features and technology to solve similar problems in different circumstances:

- **Authentication process:**

WebSSO systems implement single sign-on to multiple (web-based) systems.

Password Manager does not change the sign-on process for support systems, but instead ensures that passwords are the same across every system a user logs into.

- **Platform support:**

WebSSO products manage users on a single platform – a directory, normally using LDAP, that contains every user of one or more web applications.

Password Manager manages passwords across an entire spectrum of systems employed by an enterprise: network operating systems, client/server applications, e-mail systems, ERP systems, mainframes and midrange systems, directories and more. Password Manager also manages other forms of authentication, including hardware tokens, biometric samples, question-and-answer profiles and smart cards.

Identity Manager manages access to the same systems where Password Manager manages passwords. It can create accounts, update them, and deactivate or delete them. Identity Manager can also provision hardware (such as authentication tokens, computers or telephones) and access to systems that do not necessarily use passwords, such as building access.

WebSSO systems do not support this range of systems: they are targeted specifically at managing access to *web* applications. In practice, other systems are just not supported.

- **User interface access channels:**

As their name implies, WebSSO systems authenticate users and perform delegated and self-service user administration from just one user interface: a web browser.

Password Manager supports other user interface channels, especially for self-service password reset, which may be needed by users who forgot their initial workstation password, or require a new password before they can connect to a RAS or VPN service.

Password Manager can be accessed from workstation login prompts, Unix and mainframe login prompts and IVR systems, as well as a web browser.

- **Number of user directories:**

WebSSO systems normally maintain data in a single user directory. This directory may be implemented using LDAP or a DBMS like Oracle, and may in rare cases form a virtual directory, aggregating users from more than one source.

WebSSO systems cannot manage users or passwords outside of this single directory. For example, if a user forgets his mainframe password, a WebSSO system can't help. If a user has a mixture of passwords – one for the web infrastructure and several others for non-web applications and systems, the WebSSO cannot synchronize them, or simplify login to those systems.

- **Password policy engine:**

Most WebSSO systems incorporate a simple password policy engine, to ensure that a user's single password to the web infrastructure is sound. Typically these engines enforce just a few rules, such as minimum length, finite history, etc.

Password Manager incorporates the most powerful password policy engine available, including open-ended history, over 50 built-in rules, a random password generator, a regular expression engine and a plugin system. This engine is needed when constructing a password policy intended to secure heterogeneous systems, whose native capabilities are diverse.

- **Robust non-password authentication:**

Many WebSSO systems allow users to register one or two question-and-answer pairs, so that in the event that a user forgets his password, he can be prompted to answer one or two personal questions, and then be allowed to select a new password.

This type of authentication is very weak, and may not be appropriate for an organization's web Intranet, let alone critical business systems.

Password Manager includes a much more powerful self-service Q&A model, including a mix of pre-defined and user-defined questions, automatic prompting asking users to register data, separate Q&A for self-service password reset and help desk password reset, and much more.

A complex non-password authentication system is essential when managing user authentication to every system, rather than just web content.

- **Workflow for authorizing access changes:**

Most WebSSO systems incorporate delegated user administration, including creating, modifying and deactivating users. They do not, however, support an authorization workflow, where one user requests a change, others approve or reject it, and it is then implemented.

Identity Manager incorporates this functionality in the base package.

Many WebSSO vendors are introducing this capability, but in a separate "identity management" package.

6 The value of integration

6.1 What WebSSO systems do well

As described above, WebSSO systems are an effective infrastructure for:

- Managing a single, global user directory.
- Simplifying user authentication across multiple web applications.
- Enforcing policy over what web content and web-enabled functions users can access.

WebSSO systems are a mature technology, and useful in most Intranet and Extranet environments.

6.2 What WebSSO systems cannot do

WebSSO systems do not address all the authentication and access management requirements of an enterprise, however. They cannot manage sign-on to or access control in systems such as network operating systems, midrange servers, mainframes, e-mail systems or client/server applications.

In effect, WebSSO systems are limited to managing authentication in a single enterprise directory (typically LDAP), and interacting with users over a single channel (a web browser).

6.3 Filling the WebSSO capability gap

Enterprise password and authentication management, as implemented by Hitachi ID Password Manager, allows organizations to simplify sign-on and administration of authentication data on every system, rather than just web applications.

Password Manager password synchronization, in conjunction with WebSSO, reduces the number of credentials that a user must manage across every system, web-based or not.

Password Manager self-service password reset means that users can maintain a single, secure Q&A profile, and use it to securely reset forgotten or disabled passwords on both web and legacy systems.

It is important to note that while most WebSSO systems provide a self-service password reset capability, it does not address the systems that typically generate the bulk of password problems in an Intranet: the network operating system and mainframe. In most environments, LDAP passwords are subject to relatively weak constraints (simple passwords, infrequent changes), and consequently are not a major contributor to password problem call volume at the help desk.

6.4 Better self-service password reset for web applications

The Hitachi ID Password Manager web user interface can be readily integrated with a WebSSO, and replace the built-in self-service password reset feature with a more secure and globally relevant one.

6.5 Change authorization workflow for the enterprise

Hitachi ID Password Manager access change authorization workflow means that users can simultaneously request updated privileges to both web-based and legacy IT infrastructure. Those requests are routed to appropriate authorizers, and when they are approved are automatically fulfilled globally.

7 Summary

WebSSO systems simplify authentication to multiple web applications, and enable unified user administration that spans a single directory and supports multiple web applications.

Hitachi ID Password Manager manages all forms of user authentication across every system in the enterprise, including directories, network operating systems, client/server and ERP applications, midrange and mainframe systems, etc.

Hitachi ID Identity Manager manages user access to every system in the enterprise, and can create, update and delete accounts based on a change request authorization workflow, central and automated user administration and more.

Enterprises derive maximum value by deploying all three systems: central and delegated administration, plus unified authentication, to web applications, plus streamlined administration of users, passwords and non-password authentication that spans every system, not just web applications.

8 References

WebSSO vendors today include:

Vendor	Product	Web site
CA	SiteMinder	http://www.ca.com/us/products/product.aspx?id=5262
Entrust	GetAccess	http://entrust.com
HP	SelectAccess	http://www.openview.hp.com/products/select/
IBM/Tivoli	Access Manager for e-business	http://www-306.ibm.com/software/tivoli/products/access-mgr-e-bus/
Novell	iChain	http://www.novell.com
Oracle	Access Manager	http://www.oracle.com/technology/products/id_mgmt/coreid_acc/index.htm
RSA	ClearTrust	http://rsa-security.com

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

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

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