

## Locking down

a Hitachi ID Management Suite server



Organizations that are either considering deployment of Hitachi ID Password Manager or have already deployed it need to understand how to secure the Password Manager server. Password Manager is a sensitive part of an organization's IT infrastructure and consequently must be defended by strong security measures.

This document is intended to form the basis of a "best practices" guide for securing a Password Manager server. The objective of a secure Password Manager server is to have a reliable, high availability server which is difficult or impossible for users and intruders to compromise.

# Contents

- 1 Introduction** **1**
  
- 2 Basic precautions** **2**
  
- 3 Operating system** **3**
  - 3.1 Authentication into the server . . . . . 3
    - 3.1.1 Domain membership . . . . . 3
    - 3.1.2 Accounts . . . . . 3
  - 3.2 Securing services . . . . . 4
  - 3.3 Network and session security . . . . . 5
    - 3.3.1 Packet filtering . . . . . 5
    - 3.3.2 Harden the IP stack . . . . . 6
  
- 4 Web server** **9**
  - 4.1 Apache . . . . . 9
  - 4.2 IIS (Internet Information Server) . . . . . 9
    - 4.2.1 Use separate NTFS partitions . . . . . 9
    - 4.2.2 Remove non-essential web server content . . . . . 10
    - 4.2.3 Remove RDS registry keys . . . . . 11
    - 4.2.4 Remove ODBC drivers . . . . . 11
    - 4.2.5 Restrict IUSR and IWAM account permissions . . . . . 12
  
- 5 Service packs** **13**
  
- 6 Communication defenses** **14**
  
- 7 Data protection** **15**

<b>8 Auditing</b>	<b>16</b>
<b>9 Physical security</b>	<b>17</b>
<b>10 Conclusions</b>	<b>18</b>

## 1 Introduction

Organizations that are either considering deployment of Hitachi ID Password Manager or have already deployed it need to understand how to secure the Password Manager server. Password Manager is a sensitive part of an organization's I.T. infrastructure and consequently must be defended by strong security measures.

Password Manager houses sensitive data, which may include:

- **Administrator credentials** to target systems, which the Password Manager server uses to attach to target systems and reset user passwords.
- **Support staff passwords**, which may be used to log into user support screens in Password Manager.
- **Personal user data**, which may be managed by Password Manager and used to authenticate users when they need to access a self-service function, and have forgotten or locked out their password.

It is important to protect both the Password Manager server itself and the data it contains.

The remainder of this document is organized as follows:

- **Basic precautions**  
Some common-sense security precautions.
- **Operating system**  
How to configure a secure Windows server operating system for use with Password Manager.
- **Web server**  
How to select and configure a web server.
- **Communication defenses**  
How to protect the data transmitted into and out of each Password Manager server.
- **Data protection**  
How the data stored on each Password Manager server is protected.
- **Auditing**  
Why auditing is important.
- **Physical Security**  
Suggestions on how to control the physical access to the Password Manager server.
- **Conclusions**

## 2 Basic precautions

Some of the most effective security measures are common sense:

1. Use a single-purpose server for Hitachi ID Password Manager. Sharing this server with other applications introduces more complexity and more administrators, each of which carries its own incremental risk.
2. Use strong passwords for every administrative account on the server.
3. Maintain a current, well-patched operating system on the Password Manager server. This eliminates well-known bugs that have already been addressed by the vendor (Microsoft).
4. Keep the Password Manager server in a physically secure location.
5. Do not leave a login session open and unattended on the Password Manager server's console.
6. Place the Password Manager server on your internal network, rather than on the Internet, if this is at all possible in your environment.

If required, you can still expose the Password Manager web UI to the Extranet using a reverse web proxy, such as Apache, or using a "shadow instance" program available at no extra charge from Hitachi ID Systems.

## 3 Operating system

The first step in configuring a secure Hitachi ID Password Manager server is to harden its operating system.

Hitachi ID Systems suggests that Password Manager be installed on the Windows 2003 server operating system. The following are suggestions on how to lock down this operating system.

### 3.1 Authentication into the server

Since the Hitachi ID Password Manager server contains sensitive information (please see [Section 7](#) on [Page 15](#) for how this information is stored), it makes sense to limit the number of users who can access its files.

#### 3.1.1 Domain membership

One way to limit the number of users who can access the Hitachi ID Password Manager server is to remove it from any Windows / Active Directory domains. When the Password Manager server is not a member of any domain, domain administrators are prevented from using their Windows credentials to attempt to compromise privileged credentials on other systems with which Password Manager has been integrated.

Ensuring that the Password Manager server is not a domain member also reduces the risk of lockouts due to concurrent domain logins by the Password Manager server - some by the Password Manager software, and others by an administrator interactively logged into the server's console.

#### 3.1.2 Accounts

The Hitachi ID Password Manager setup program creates one local user on the Password Manager server, typically called `psadmin`.

The account is, by default, a member of the local Administrators group. It is the only account needed by Password Manager. We recommend removing unused accounts, leaving just:

- `psadmin` - The Password Manager service account.
- One account to be used by the Password Manager administrator to log into the server's console.

**Note:** Use the DENY NETWORK LOGON feature in the local security policy to protect the Administrator account against remote access attempts using brute force password attacks.

- If (and only if) required, one account to run an FTP service.

If you need other accounts on the Password Manager server, then we recommend the following:

- Remove all guest account and “Everyone” access to resources.
- Do not increase the default level of access for the default USERS group.
- Do not assign files/directories to the EVERYONE group.
- Limit the number of administrator-level accounts needed to manage the system. As stated above, the Password Manager server only requires one administrator-level account.
- Remove the terminal services user account `TsInternetUser` if it is not needed.

Additionally, a regular review of accounts, groups and group memberships should be carried out, to ensure that access permissions are appropriate.

### 3.2 Securing services

An important way to secure a server on any platform is to reduce the amount of software that it runs. This eliminates potential sources of software bugs that could be exploited to violate the server’s security.

The following services, at most, are needed on the Hitachi ID Password Manager server:

- DNS Client - Required to resolve host names
- Event Log - Core O.S. component
- IIS Admin Service - Only required if IIS is used
- IPSEC Policy Agent - Core O.S. component
- Logical DiskManager - Core O.S. component
- Network Connections - Required to manage network interfaces
- Plug and Play - Hardware support
- Protected Storage - Core O.S. component
- Remote Procedure Call (RPC) - Core O.S. component
- Removable Storage - Required to open CD-ROM drives
- RunAs Service - Core O.S. security component
- Security Accounts Manager - Core O.S. security component
- TCP/IP NetBIOS Helper Service - Only required if directly managing Windows 2000/2003/2008 passwords
- Workstation - Only required if directly managing Windows 2000/2003/2008 passwords
- World Wide Web Publishing Service - Only required if IIS is used

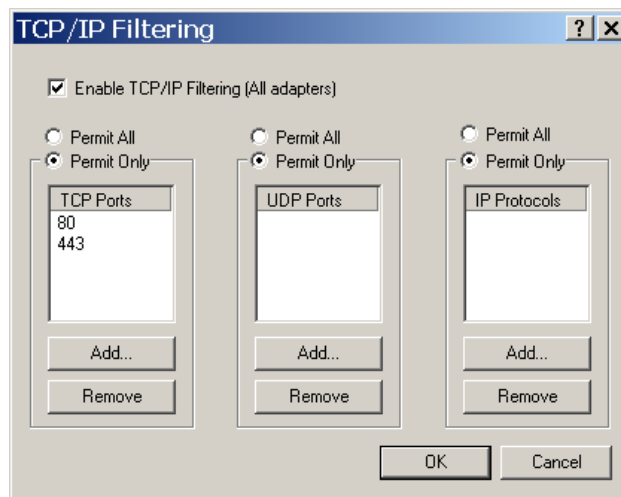
If additional services are required during implementation, then Hitachi ID Systems will notify organization.

All other services should be disabled unless there is some specific reason (not related to Password Manager) to enable them. Once you have identified a minimum set of services for your server, save the list. Check which services are running after applying service packs and other operating system updates, and disable services as required to return to your original list.

### 3.3 Network and session security

#### 3.3.1 Packet filtering

The Hitachi ID Password Manager server can also take advantage of simple packet filtering services in Windows 2003, to block all inbound connections other than those to the web service, as shown in the figure below:



Open ports are an exploitable means of system entry. By limiting the number of open ports, you effectively reduce the number of potential entry points into the server.

A hardened Password Manager server can be port scanned to identify available services. Following is a typical port scan result:

```
delli:/data/idan/vmware/win2ksrv# nmap -sT 192.168.100.8

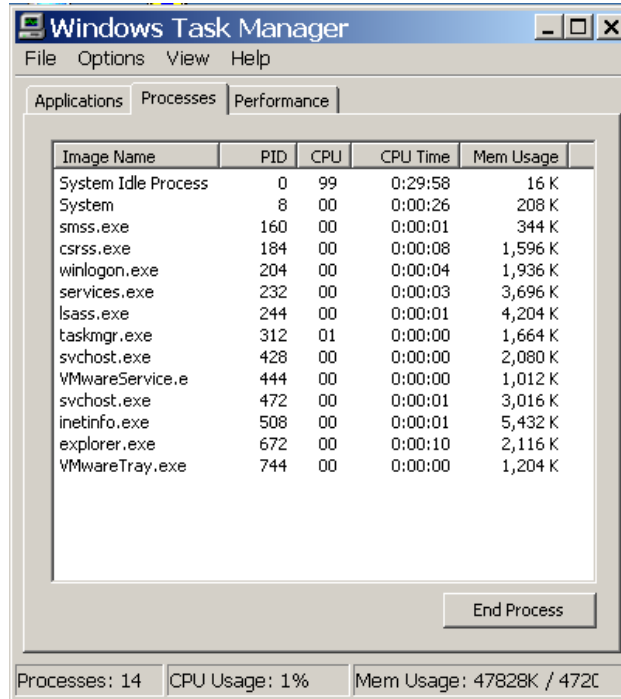
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.100.8):
(The 1551 ports scanned but not shown below are in state: closed)
Port      State      Service
80/tcp    open      http
443/tcp   open      https

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
delli:/data/idan/vmware/win2ksrv# nmap -sU 192.168.100.8
```

```
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
All 1459 scanned ports on (192.168.100.8) are: filtered
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 91 seconds
```

The process table on the same server looks like this:



Note: VMWare entries in the figure reflect the fact that this sample was taken from a VMWare virtual PC.

This server was running with just the mandatory services described earlier.

### 3.3.2 Harden the IP stack

Enable the following TCP/IP registry settings as shown below to make the Hitachi ID Password Manager server resistant to denial of service (DOS) attacks:

**Note:** Some of the settings may cause some applications to fail. Be sure to test all settings before implementing.

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\SynAttackProtect

**Type:** REG\_DWORD

**Value:** 1 - reduced re-transmission retries and delayed RCE (route cache entry) creation of the **TcpMaxHalfOpen** and **TcpMaxOpenRetried** settings are satisfied (see below).

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\TcpMaxHalfOpen

**Type:** REG\_DWORD

**Value:** 100 - for Windows 2000 Professional or Server **Value:** 500 - for Windows 2000 Advanced Server

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\TcpMaxHalfOpenRetried

**Type:** REG\_DWORD

**Value:** 80 - for Windows 2000 Professional or Server **Value:** 400 - for Windows 2000 Advanced Server

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\TcpMaxPortsExhausted

**Type:** REG\_DWORD

**Value:** 5

The following keys, not present on a default Windows server installation, are also helpful to protect against a variety of attacks against the IP stack:

- HKLM\System\CurrentControlSet\Services  
  \AFD\Parameters\EnableDynamicBacklog

**Type:** REG\_DWORD

**Value:** 1

- HKLM\System\CurrentControlSet\Services  
  \AFD\Parameters\MinimumDynamicBacklog

**Type:** REG\_DWORD

**Value:** 20

- HKLM\System\CurrentControlSet\Services  
  \AFD\Parameters\MaximumDynamicBacklog

**Type:** REG\_DWORD

**Value:** 5000

- HKLM\System\CurrentControlSet\Services  
  \AFD\Parameters\DynamicBacklogGrowthDelta

**Type:** REG\_DWORD

**Value:** 20

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\EnableDeadGWDetect

**Type:** REG\_DWORD

**Value:** 0

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\KeepAliveTime

**Type:** REG\_DWORD

**Value:** 300,000

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\PerformRouterDiscovery

**Type:** REG\_DWORD

**Value:** 0

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\EnableICMPRedirects

**Type:** REG\_DWORD

**Value:** 0

- HKLM\System\CurrentControlSet\Services  
  \Tcpip\Parameters\DisableIPSourceRouting

**Type:** REG\_DWORD

**Value:** 2

## 4 Web server

The web server is a required component since it provides all user interface modules. It should therefore be carefully protected.

Since Hitachi ID Password Manager does not require any web server functionality beyond the ability to serve static documents (HTML, images) and to execute self-contained CGI executable programs, all non-essential web server content should be removed.

Several web servers are commonly available for Windows servers, including Apache, IIS, iPlanet and more. Hitachi ID Systems suggests that the Apache or IIS web server be used with Password Manager. As such, this document will detail how to lock down the Apache or IIS web server.

### 4.1 Apache

The Apache server is recommended, as it is well supported and has had a very good security track record. Most recent web server security vulnerabilities have been specific to IIS, and would not affect Apache.

If you select Apache, you can harden it by:

- Denying access from all clients except those coming from the internal domain. Do this by using the *Allow*, *Deny* directives for the Hitachi ID Password Manager virtual directories.
- Ensuring that you use only Apache modules that are needed by Password Manager. For example, you do not need modules for PERL, PHP or any other scripting languages. Read through the Apache configuration file and disable *LoadModule* directives by deleting or commenting them out in `httpd.conf`.
- Moving the *DocumentRoot* to a different drive than your system disk (e.g., if your WINNT directory is on C:, then move DocumentRoot to D:).

### 4.2 IIS (Internet Information Server)

IIS is more than a web server - it is also an FTP server, indexing server, proxy for database applications and a server for active content / applications.

If you run Hitachi ID Password Manager on IIS, you should disable most of these features, as each of them may represent a security risk, due to the possibility of software bugs.

Lock down IIS as follows:

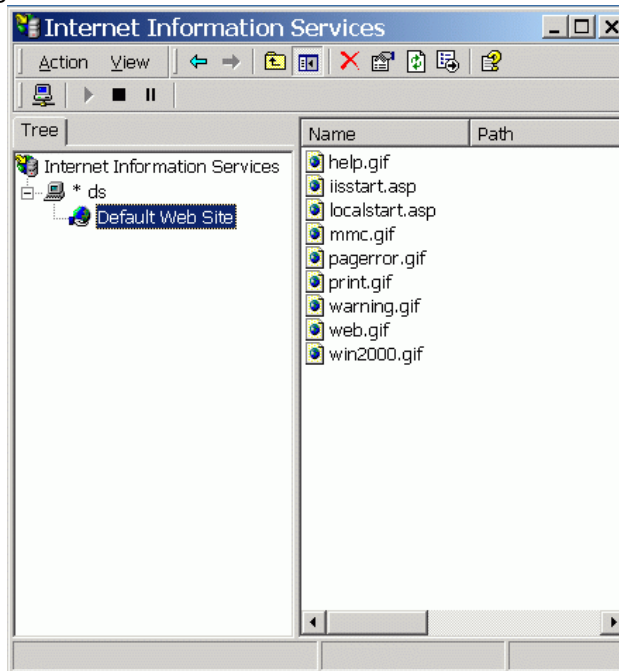
#### 4.2.1 Use separate NTFS partitions

Create two separate NTFS partitions - one for the operating system and one for IIS. This will separate most of the operating system files from the application files, allowing a more controlled distribution of permission

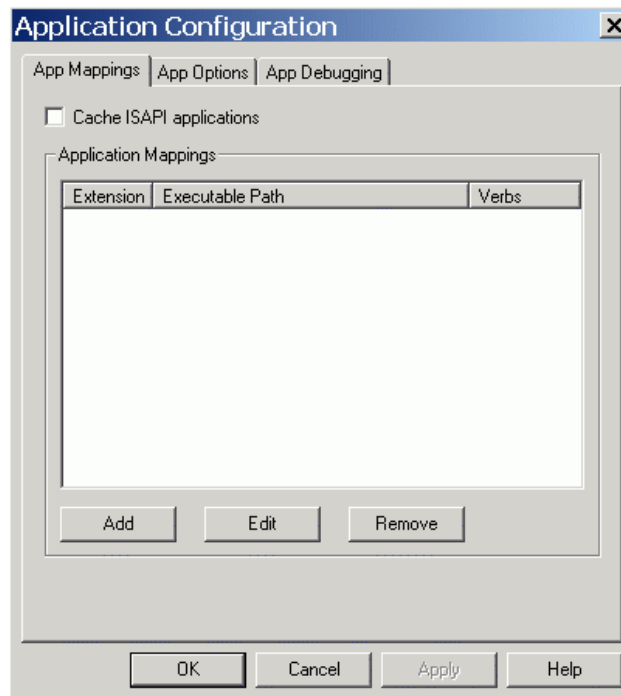
sets.

#### 4.2.2 Remove non-essential web server content

As stated previously, Hitachi ID Password Manager only requires the web server to serve static documents (HTML, images) and to execute self-contained CGI executable programs, which means all non-essential web server content should be removed. This means removing IISAdmin, Printers, Scripts and similar folders, as shown in the figure below:



The web server's scripting, indexing and data access subsystems should likewise be removed as shown in the figure below:



#### 4.2.3 Remove RDS registry keys

As an extra precaution, remote data services (RDS) should be disabled by removing the following registry keys:

- `HKLM\System\CurrentControlSet\Services  
    \W3SVC\Parameters\ADCLaunch\RDS\Server.DataFactory`
- `HKLM\System\CurrentControlSet\Services  
    \W3SVC\Parameters\ADCLaunch\AdvancedDataFactory`
- `HKLM\System\CurrentControlSet\Services  
    \W3SVC\Parameters\ADCLaunch\BusObj.VbBusObjCls`

#### 4.2.4 Remove ODBC drivers

All ODBC drivers that are not required (and Hitachi ID Password Manager uses none) should also be disabled because they can introduce possible security concerns for IIS. To disable the ODBC drivers, remove the data sources manually and add this entry to the registry:

- `HKLM\Software\Microsoft\Jet\4.0\engines\SandBoxMode = 3`

The above registry entry will ensure that no `cmd.exe` commands can be chained with ODBC queries.

Consult the following *Microsoft Knowledge Base* article for more information:

<http://support.microsoft.com/support/kb/articles/Q239/1/04.asp>

#### **4.2.5 Restrict IUSR and IWAM account permissions**

The IUSR account is created during the IIS installation and provides the mechanism that allows web clients to access the web server anonymously. The IWAM account is used to start out-of-process web applications in IIS. Do not add these accounts to a privileged group such as *Administrators*. Delete these accounts if possible as Hitachi ID Password Manager does not use them (it creates and uses the `psadmin` user for anonymous access).

## 5 Service packs

Install the latest service packs, as these frequently include security patches and updates.

Service packs for Windows 2003 may be found at:

<http://www.microsoft.com/windows2003/downloads/default.asp>

Service packs for Windows 2000 may be found at:

<http://www.microsoft.com/windows2000/downloads/default.asp>

We recommend that to be notified of the latest security upgrades for Windows 2003, you subscribe to the Microsoft's security bulletin at:

<http://www.microsoft.com/technet/security/bulletin/notify.asp>

Equally important to installing the latest service pack is testing the service pack installation before deployment on a production platform. This will ensure there are no adverse affects on Hitachi ID Password Manager.

## 6 Communication defenses

Hitachi ID Password Manager sends and receives sensitive data over the network. Its communications include user passwords, administrator credentials and personal user information. These are all valuable assets that must be defended.

Network attacks typically fall into two classes:

- **Passive attacks**, where an intruder listens to a communication stream and extracts useful data from it.
- **Active attacks**, where an intruder abuses either an available network service, or an open communication session.

Hitachi ID Systems strongly recommends that users access Password Manager using SSL (HTTPS). To do this, you must:

- Assign a fixed IP address to each Password Manager server.
- Assign a fixed DNS name to each Password Manager server.
- Install a web server.
- Create a certificate signing request (CSR) file.
- Submit the CSR file to a certificate authority (e.g. Verisign, Thawte, etc.).
- Receive and install a signed certificate.

As long as the Password Manager server is configured with an SSL certificate, and configured to require HTTPS client communication, no sensitive data will be transmitted in plaintext. This will protect communications against both passive and active attacks.

## 7 Data protection

The Hitachi ID Password Manager server houses some sensitive data, and this data must be protected against anyone who has physical access to the server, or has a legitimate right to log into it.

All sensitive data on the Password Manager server is encrypted, as follows:

Encryption is used to protect stored Password Manager data as follows:

**Data stored on the Password Manager server**

Data	Algorithm	Key
Privileged passwords, used to log into target systems	128-bit AES	128-bit random
Answers to security questions	128-bit AES	128-bit random
User old password history	SHA-1	64-bit random salt

Of the above, the only mandatory data is administrator credentials for target systems. Everything else may be pulled by Password Manager from other systems (database, directory, etc.), on demand. Note, however, that moving sensitive data to another system generally introduces more security problems (communication, storage) than it solves, and is not recommended as a solution to security concerns.

As a result of this encryption, someone with access to the filesystem of the Password Manager server would not be able to readily decipher sensitive data on that server. They would first have to figure out where the data is stored, then how it is encoded, then how it is encrypted, and then they would have to find a suitable key (itself encrypted, in the Password Manager server's registry).

This provides as much protection as possible to sensitive data on the server, without compromising its functionality.

## 8 Auditing

Audit logs are an important measure to identify and analyze suspicious activity.

Since anyone with administrator access to the Hitachi ID Password Manager server can alter or remove audit logs, arrange for periodic archive of audit logs to a different server, managed by different administrators.

Windows 2003 provides various audit logs through the “Event Viewer.” Additionally, IIS provides configurable logging information with `W3C Extended Log File Format`.

An audit log is only effective if it is examined. These logs provide the best indications of break-ins, fraud and misuse. Therefore, regular examination of the logs is recommended.

## 9 Physical security

Hitachi ID Password Manager servers should be physically protected, since any logical security measures can be bypassed by an intruder with physical access to the server, time and skill.

Suggestions for physically securing the Password Manager server include:

- **Location and access**

Put the Password Manager server(s) in a locked and secured room. Restrict access to authorized personnel only. Access should be logged.

- **Power**

Protect the Password Manager server with uninterruptable power sources (UPS). UPS equipment will protect the server from temporary power loss that could cause a server crash or corruption of critical user files.

- **Removable media**

Restrict the boot process so it is more difficult for intruders to circumvent Windows 2003 security by booting from floppy disks or a CD-ROM. Specifically, use a BIOS-level password, disable boot from a floppy drive, flash device or CD-ROM drive and lock the system BIOS to prevent unauthorized changes to the BIOS configuration.

## 10 Conclusions

This document highlights the fact that Hitachi ID Password Manager is a sensitive server, and should be managed carefully. In particular, it should be installed on a locked-down server, and managed with close attention to security.

This document illustrates the best-practice measures that should be implemented to protect Password Manager servers.

To learn more about hardening a Windows 2003 server, please refer to the Microsoft site:

<http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en>

In case the above URL changes, search <http://microsoft.com> for the document titled "Windows Server 2003 Security Guide."