

Hitachi ID Password Manager

Frequently Asked Questions
for Security Officers



Contents

1	How does Password Manager improve security?	1
2	How does Password Manager authenticate users?	1
3	How does Password Manager get challenge/response data for non-password authentication?	2
4	Can one user “claim” another user’s login ID?	2
5	Does Password Manager transmit all sensitive data encrypted?	3
6	Does Password Manager store all sensitive data encrypted?	4

1 How does Password Manager improve security?

Hitachi ID Password Manager improves the security of authentication processes:

- A strong, uniform password policy prevents the use of easily guessed passwords and ensures that all passwords are changed regularly.
 - Password synchronization discourages written passwords (“sticky notes”).
 - Consistent, reliable authentication processes ensures that users are reliably identified before accessing sensitive services, such as a help desk password reset.
 - IT support staff can be empowered to assist callers without having administrator accounts on every system and application.
 - Extensive audit logs create accountability for password resets.
 - Encryption ensures that passwords are not stored or transmitted in plaintext.
-

2 How does Password Manager authenticate users?

Users may authenticate into Hitachi ID Password Manager as follows:

- – By typing their current password to a trusted system (e.g., Windows/AD, LDAP, RAC/F, etc).
 - – By answering security questions.
 - – Using a security token (e.g., SecurID pass-code).
 - – Using a smart card with PKI certificate.
 - – Using Windows-integrated authentication.
 - – Using a SAML assertion issued by another server.
 - – By typing a PIN that was sent to their mobile phone via SMS.
 - – Using a combination of these mechanisms.
 - Using a telephone, calling an automated IVR system:
 - – By keying in numeric answers to a series of security questions (e.g., employee number, date of hire, driver’s license number).
-

- By speaking one or more phrases, where the Password Manager server compares the new speech sample to one on record (biometric voice print verification)
 - Using a telephone, calling a (human) analyst on the help desk:
By answering a series of security questions, where the analyst must type the answers into a web UI to authenticate the caller.
-

3 How does Password Manager get challenge/response data for non-password authentication?

Users can authenticate to Hitachi ID Password Manager by answering security questions, where the data is stored in the Password Manager identity cache or on an existing system (e.g., Oracle, LDAP, mainframe, etc.)

If the data is stored in Password Manager, then it is normally encrypted using 128-bit AES and a server-designated key. Password Manager will use its own methods to retrieve the challenge/response data.

If the data is stored on an existing system, then Password Manager runs a plug-in program to retrieve and validate the data when it is required. Out of the box, Password Manager comes with a plug-in that is capable of retrieving questions and answers from an LDAP directory or AD and another that works with SQL Server.

4 Can one user “claim” another user’s login ID?

To claim another ID in Hitachi ID Password Manager, the user must supply the ID he/she wants to claim and the password for that ID. Consequently, one user can only claim another user’s ID into his own profile if he already knows the password for that ID – i.e., this reflects a security compromise that has already happened.

The process to register or “claim” user IDs in Password Manager is as follows:

1. **Password Manager web server:** prompts user to type his network login ID.
 2. **User:** types his network login ID.
 3. **Password Manager web server:** prompts user to type his current NOS password.
 4. **User:** types current password.
 5. **Password Manager web server:** validates the password against the indicated system.
repeat if authentication failed, lockout if too often.
-

6. **Password Manager web server:** display a profile of already-attached login IDs / accounts. Prompts for an additional ID/password.
 7. **User:** types his login ID and current password for a system that does not yet appear on the list.
Note: the user does not explicitly specify which system the login ID is for.
 8. **Password Manager server:** finds instances of this ID on the network, from the previous night's list. Eliminates already-assigned IDs. Tries to connect to each remaining system with the ID/password entered by the user. For systems where the login worked, adds the ID to the user's profile. Discards the password.
 9. **Password Manager web server:** notifies user of success / failure.
repeat as necessary.
-

5 Does Password Manager transmit all sensitive data encrypted?

Data transmitted to and from Hitachi ID Password Manager on the network is cryptographically protected, as illustrated by the following examples:

Data transmitted to/from the Password Manager server

To/From	Algorithm	Key length
<i>Interactive sessions</i>		
User browser	SSL (varies)	128 bits.
<i>Trigger password synchronization</i>		
From Win2K/2K3 AD DC	128-bit AES	128-bit shared secret.
From z/OS		
From Unix		
From LDAP server		
<i>Set passwords, Create/update users</i>		
To SSH scripted target	SSH	Varies by SSH configuration
To Unix agent	128-bit AES	128-bit shared secret.
To z/OS task		
To RSA Authentication Manager		
To proxy server		
<i>API (application programming interface) Session - socket</i>		
From calling system / IVR (interactive voice response)	128-bit AES	128-bit shared secret.
<i>API Session - web services</i>		
From calling system / IVR	HTTPS	128 bits.
<i>Set passwords, Create/update users</i>		
To target system	native	Varies. Use proxy server when native protocol is inadequate.

6 Does Password Manager store all sensitive data encrypted?

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

Frequently Asked Questions for Security Officers

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