

Hitachi ID Password Manager

Frequently Asked Questions
for Password Manager Administrators



Contents

1	How do I reset the superuser application ID's password?	1
2	Where does Password Manager store Q&A data?	1
3	How do I write reports that directly query the Password Manager database?	1

1 How do I reset the superuser application ID's password?

In the event that the Hitachi ID Password Manager administrator forgets his own application password into Password Manager, Password Manager comes with the ADM_SET utility that allows a user with an administrative console login on the Password Manager server to reset the Password Manager application administrator password. This program can also be used to unlock/enable a superuser ID. ADM_SET is only accessible from an administrative command prompt on the Password Manager server.

2 Where does Password Manager store Q&A data?

Hitachi ID Password Manager normally stores security questions, used to authenticate users who forget their passwords, in its internal identity cache. The questions and answers are encrypted using 128-bit AES using a secret key. Alternatively, Password Manager can be tied to an external repository (e.g., LDAP, AD, Oracle, etc.) where it reads and writes security questions and login ID profiles.

3 How do I write reports that directly query the Password Manager database?

Hitachi ID Password Manager stores data using an embedded database engine, which acts both as an identity cache (managing a rolling snapshot of information about users drawn from target systems) and as a place to store configuration information and persistent user data, such as password history.

The identity cache is local to the Password Manager server, which makes the user interface much more responsive. It is not authoritative for user profile data, as data is refreshed from target systems regularly and automatically (typically every night).

The following data is stored in Password Manager:

- User profiles:
 - User ID, name (plaintext)
 - Login IDs attaching users to target systems (plaintext)
 - Password history (Hashed, salted old passwords)
 - Authentication profile (Optional. If stored, encrypted using 128-bit AES and a server-designated 128-bit key.)

Frequently Asked Questions for Password Manager Administrators

- System configuration:
 - Target system information
 - Target system login credentials (encrypted: 128-bit AES and a server-designated 128-bit key)
 - Password policy rules
 - List of events that should be intercepted and trigger outbound integration with systems such as BMC/Remedy ARS
 - Various other configuration data
- System event logs – capturing historical events, including:
 - Requesting user.
 - Target/recipient user.
 - Target system involved, if any.
 - Operation.
 - Time/date.
 - Result code and message.

These logs are typically retained indefinitely, for reporting purposes.

Password Manager comes with various built-in reports that can be generated through the web interface. To access these reports:

1. Log in as an admin user who has the right to view the server monitor.
2. Click **Server Monitor** → **Run Reports** to see the **Password Manager Run Reports** page.
3. Click on the type of report you want to generate.

Additionally, if custom reports need to be created, then the database files can be copied to another location. This will allow another tool to read the database and allow you to generate custom reports.