Change Service Account Password

This document contains:

1 Objective

Hitachi ID Bravura Security Fabric utilizes a service user (**psadmin**) account in various locations. Organizations require the ability to rename this account, use a different account or change the password.

2 Solution

When changes are made to the Hitachi ID Systems service user (**psadmin**) account, such as renaming it, changing the password, or changing to a different account, use the **serviceacct** program to update known locations where the service user account is used.

Note: If you have multiple instances using the same service account, you must run **serviceacct** under each instance when the service account is modified. If the service account is a domain account, you must prefix it with domain name "domain\user" when running the utility.

3 Usage

Before running **serviceacct**, navigate to the \\<*instance*>\\ directory and run **instance.bat** to configure necessary environment variables.

```
serviceacct.exe [-account] [-password] [-restart] [-noverify]
```

Table 1: serviceacct arguments

Argument	Description
-account	Prompt for a new account ID
-noverify	Skip verifying the supplied credentials This is only used when the utility verification process failed and you know the new account/password are valid
-password	Prompt for a new password (will not be echoed)
-restart	Restart all running services

4 Examples

1. After changing the password of the current service user account, run the following command to update all known locations where the account is used:

   ```
   serviceacct -password
   <NEWPASSWORD>
   ```

2. After changing the user ID of current service user account, run the following command to update all known locations where the account is used:

   ```
   serviceacct -account
   <NEWUSERID>
   ```

3. After swapping to a new service user account, run the following command to update all known locations where the account is used:

   ```
   serviceacct -account -password
   <NEWACCOUNTNAME>
   <PASSWORD>
   ```

Note: It is recommended to restart all services related to the *Bravura Security Fabric* instance to make sure everything is working properly after you run the utility.

The **serviceacct** programs stops and starts all currently running services when used with the `-restart` option.

5 Known locations

The following are known locations where the service user (**`psadmin`**) account will be updated by **`serviceacct`**:

- All services related to the *Hitachi ID Bravura Security Fabric* instance
- The application and <*instance*>\docs virtual directories in IIS
- The registry key value:

  ```
  HKEY_LOCAL_MACHINE\Software\Hitachi ID\IDM Suite\<instance>\User
  ```

- "USERID" and "PASSWORD" values in idmsetup.inf
- Windows scheduled jobs created during the installation of *Bravura Security Fabric*, including HID Health Check and HID External Data Store Replicator

6 Use cases: Change to a new psadmin account

Use case 1: Change to a new local psadmin account (Used SQL Server logins to connect with SQL server)

This use case demonstrates the processes when user want to swap to a new local Hitachi ID Systems service user (**`psadmin`**) account when using SQL Server logins to connect with SQL server.

1. Create a new local psadmin account and add it to the Administrators group.
2. Give the new account the "Logon as a service" right under Local Security Policy settings.
3. Run **`serviceacct`** from the command line to update the known locations where the account is used with the new psadmin account information.

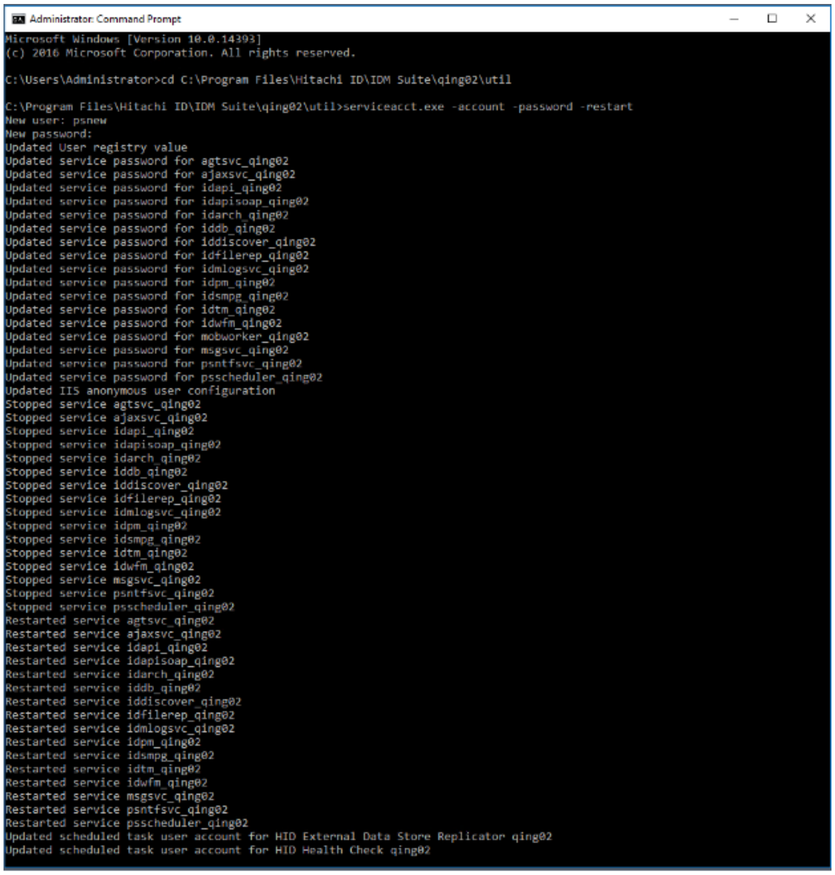
   (a) Open the command line as administrator.

   (b) Go to `<instance>/util`.

   (c) Run:

   ```
   serviceacct -account -password -restart
   ```

   (d) Input the new account name and password.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files\Hitachi ID\IDM Suite\qing02\util

C:\Program Files\Hitachi ID\IDM Suite\qing02\util>serviceacct.exe -account -password -restart
New user: psnew
New password:
Updated User registry value
Updated service password for agtsvc_qing02
Updated service password for ajaxsvc_qing02
Updated service password for idapi_qing02
Updated service password for idapisoap_qing02
Updated service password for idarch_qing02
Updated service password for iddb_qing02
Updated service password for iddiscover_qing02
Updated service password for idfilerep_qing02
Updated service password for idmlogsvc_qing02
Updated service password for idpm_qing02
Updated service password for idsmpg_qing02
Updated service password for idtm_qing02
Updated service password for idwfm_qing02
Updated service password for mobworker_qing02
Updated service password for msgsvc_qing02
Updated service password for psntfsvc_qing02
Updated service password for psscheduler_qing02
Updated IIS anonymous user configuration
Stopped service agtsvc_qing02
Stopped service ajaxsvc_qing02
Stopped service idapi_qing02
Stopped service idapisoap_qing02
Stopped service idarch_qing02
Stopped service iddb_qing02
Stopped service iddiscover_qing02
Stopped service idfilerep_qing02
Stopped service idmlogsvc_qing02
Stopped service idpm_qing02
Stopped service idsmpg_qing02
Stopped service idtm_qing02
Stopped service idwfm_qing02
Stopped service msgsvc_qing02
Stopped service psntfsvc_qing02
Stopped service psscheduler_qing02
Restarted service agtsvc_qing02
Restarted service ajaxsvc_qing02
Restarted service idapi_qing02
Restarted service idapisoap_qing02
Restarted service idarch_qing02
Restarted service iddb_qing02
Restarted service iddiscover_qing02
Restarted service idfilerep_qing02
Restarted service idmlogsvc_qing02
Restarted service idpm_qing02
Restarted service idsmpg_qing02
Restarted service idtm_qing02
Restarted service idwfm_qing02
Restarted service msgsvc_qing02
Restarted service psntfsvc_qing02
Restarted service psscheduler_qing02
Updated scheduled task user account for HID External Data Store Replicator qing02
Updated scheduled task user account for HID Health Check qing02
```

Use case 2: Change to a new domain psadmin account (Used SQL Server logins to connect with SQL server)

This use case demonstrates the processes when user want to swap to a new domain Hitachi ID Systems service user (**psadmin**) account when using SQL Server logins to connect with SQL server.

1. Create a new domain psadmin account and add it to the Domain admins group.
2. Give the new account the "Logon as a service" right under Local Security Policy settings.
3. Run **serviceacct** from the command line to update the known locations where the account is used with the new psadmin account information.
   (a) Open the command line as administrator.
   (b) Go to <*instance*>/util.
   (c) Run:

   ```
   serviceacct -account -password -restart
   ```

   (d) Input the new account name (prefix it with domain) and password.

Use case 3: Change to a new local psadmin account (Used Windows authentication to connect with SQL server)

This use case demonstrates the processes when user want to swap to a new local Hitachi ID Systems service user (**psadmin**) account when using Windows authentication to connect with SQL server. The IDM instance and the database must be on the same server.

1. Create a new local psadmin account and add it to the Administrators group.
2. Give the new account the "Logon as a service" right under Local Security Policy settings.
3. Add the new user account into database
   (a) Start Microsoft SQL Server Management Studio and connect to the server as a system administrator.
   (b) Create a new login as the new account and set it in the database.
4. Run **serviceacct** from the command line to update the known locations where the account is used with the new psadmin account information.
   (a) Open the command line as administrator.
   (b) Go to `<instance>/util`.
   (c) Run:

   ```
   serviceacct -account -password -restart
   ```

   (d) Input the new account name and password.

Use case 4: Change to a new domain psadmin account (Used Windows authentication to connect with SQL server)

This use case demonstrates the processes when user want to swap to a new domain Hitachi ID Systems service user (**psadmin**) account when using Windows authentication to connect with SQL server.

1. Create a new domain psadmin account and add it to the Domain admins group.
2. Give the new account the "Logon as a service" right under Local Security Policy settings.
3. Add the new user account into database
   (a) Start Microsoft SQL Server Management Studio and connect to the server as a system administrator.
   (b) Create a new login as the new account and set it in the database.
4. Run **serviceacct** from the command line to update the known locations where the account is used with the new psadmin account information.
   (a) Open the command line as administrator.
   (b) Go to `<instance>/util`.
   (c) Run:

   ```
   serviceacct -account -password -restart
   ```

   (d) Input the new account name (prefix it with domain) and password.