Bravura Pass Implementation: Transparent synchronization for Windows

Hitachi ID Bravura Pass can intercept password changes on a Windows-based trigger system using the Hitachi ID Password Change Notification Module and trigger automatic password synchronization for other accounts belonging to the same user.

This document contains:

1 Requirement

Organizations may require a seamless process to monitor a user's password changes in Windows systems and propagate the change to the user's other accounts on other systems.

2 Solution

In integrated environments containing many types of targets and users, who may have multiple accounts across these systems, propagating password changes may be time consuming.

This document will focus on using the Hitachi ID Password Change Notification Module on a Windows-based target to detect a user's desktop password changes and communicate the change to a non-Windows-based target.

3 Installation of components

In a typical scenario, imagine that a user is working on a Windows workstation and wants to change their password. The user also wants to propagate the password change to another Linux system target automatically.

You will be shown, by the following instructions, how to install and configure the Hitachi ID Password Change Notification Module onto a Microsoft Active Directory domain controller (DC) and use the software module to trigger the transparent synchronization process.

Installation

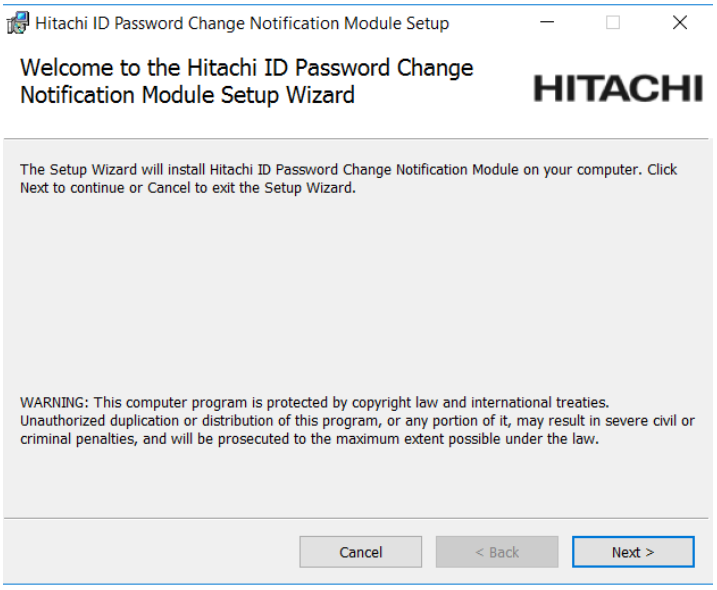
Before you begin:

- Note the communication key (or Master Key) used to encrypt communication between Hitachi ID Systems components on the network.

  The CommKey value is encrypted in *Bravura Pass*. If you did not record the key in a secure location, copy the **`idmsetup.inf`** file from <*instance*>\psconfig\ on the *Bravura Pass* server to the same location as the installer. The installer will extract the Communication Key value from the file.

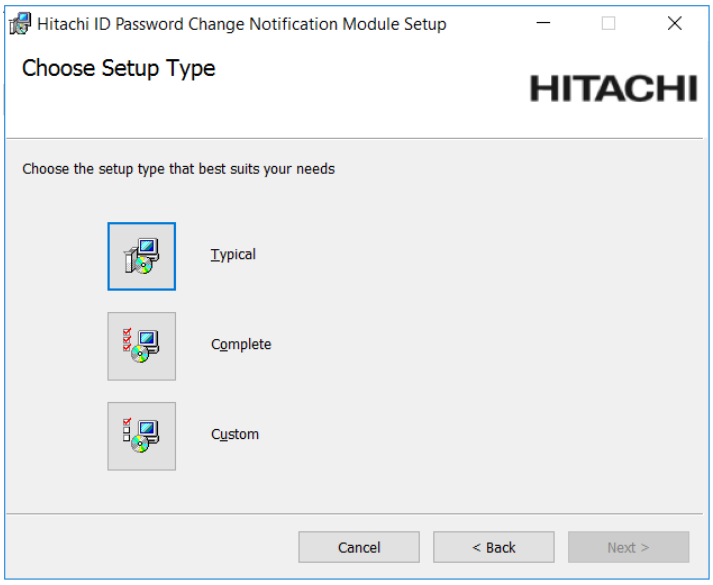
To manually install the Hitachi ID Password Change Notification Module:

1. Copy the **`intcpt.msi`** or **`intcpt-x64.msi`** installer from the *Hitachi ID Bravura Pass* server to a scratch directory (C:\temp) on the server or DC, or to a publicly accessible share.
2. Launch the Windows Installer package.

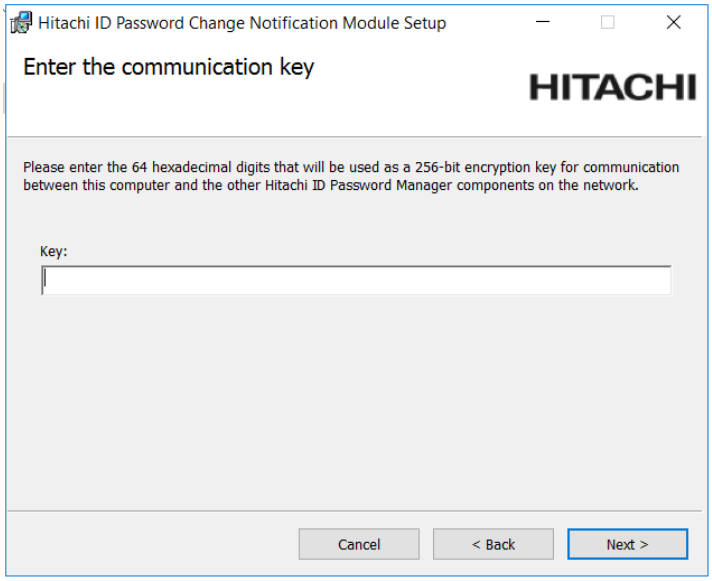


Click **Next**.

3. Read the *Bravura Pass* license. Select **I accept the terms in the License Agreement** if you agree to the terms and click **Next**.



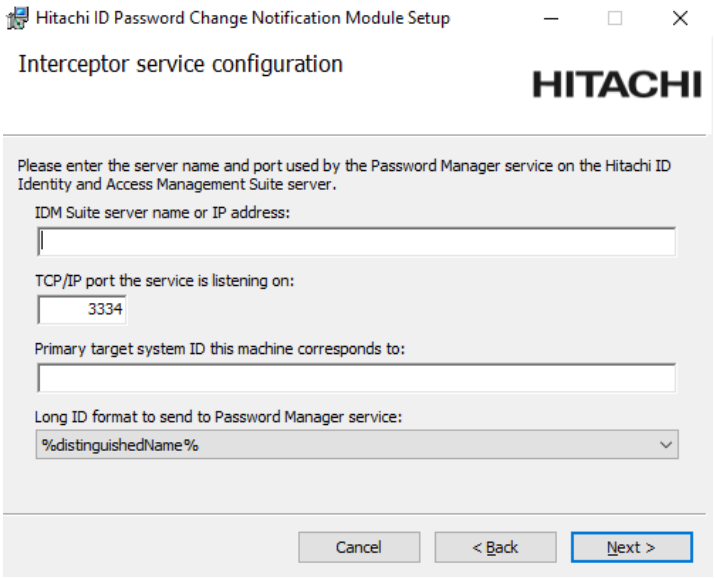
4. Click **Complete** to include the Password Change Notification Module and configuration utility programs.



5. Type the communication key.

   Network communication between Hitachi ID components is protected using a secret encryption key. Enter the same key here as you did on the main *Bravura Pass* server (communication key (or Master Key)). If you copied the **`idmsetup.inf`** file from the *Bravura Pass* server the key is entered automatically.

   Click **Next**.



6. Configure the service by entering the:

   - **IDM Suite server name or IP address**
   - **TCP/IP port the service is listening on**
   - **Primary target system ID this machine corresponds to**
     You must enter the ID of the target system you are installing on as it is configured in the *Bravura Pass* primary server.
     This target must be configured as a *Bravura Pass* target system on the primary server before Password Change Notification Module will function properly.
   - **Long ID format to send to Password Manager service**
     The longid must match the longid on the target system. Choose the format based on the target system setting and how the user's longid is being listed.

   Click **Next**.

7. Click **Install** to start the installation.
   The installer begins copying files to your computer. The ***Installation Complete*** page appears after the software has been successfully installed.

8. Click **Finish** to exit.

9. Click **Yes** to restart Windows now, or **No** if you will manually restart later.

After you reset Windows, native password changes will be intercepted by the Password Change Notification Module and forwarded to the *Bravura Pass* server for transparent synchronization.

Configuration

1. Log into the *Hitachi ID Bravura Pass* server as a superuser.

2. Navigate to **Manage the system** → **Maintenance** → **Services.** Select the **Hitachi ID (idpm) Password Manager Service.**

3. Enter the IP address of the AD server with the appropriate mask into **Comma-delimited list of IP addresses with CIDR bitmask that are allowed to send socket requests.** For instance, if the AD server IP is 10.0.23.76 and it is the only server to contact then the entry would be 10.0.23.76/32.
4. Click the **Update** button.
5. Stop the `idpm` service.
6. Start the `idpm` service.

4 Use case: A user changes their password on a Windows workstation

Requirements

This use case assumes that:

- *Hitachi ID Bravura Pass* and *Hitachi ID Connector Pack* are installed.
- An Active Directory target system is added as a source of profiles.
- A Linux target system is also added as a source of profiles.
- A user has an account on both target systems.
- The user is working on a Windows workstation that has been added to the domain.

Method of Use

For demonstration, a user named adam0000 with an AD account and a Linux account will be used on a workstation that is connected to the AD network. The IP of the Linux server is 10.0.23.77.

1. Log into the Windows workstation as adam0000.
2. Press Ctrl+Alt+Del and choose **Change a password.**
3. Enter the current password for adam0000.
4. Enter the new password and confirm in the appropriate places.
5. Click the arrow to complete the process and confirm that the password change was successful.
6. Check the instance logs to verify that the password change was detected. Something similar to the following log examples should be present on a successful password change:

   2021-02-02 13:41:20.331.2337 - [] idpm.exe [1800,5888] Info: Sending reply: code=[200], message=[Strength check success]

   2021-02-02 13:41:21.097.4324 - [] idpm.exe [1800,5888] Info: Sending reply: code=[200], message=[Request queued]

   2021-02-02 13:41:25.937.4569 - [] agtssh.exe [2172,2240] Info: line 403: Password for account [adam0000] has been changed.

   2021-02-02 13:41:26.142.1307 - [] agtssh.exe [2172,2240] Info: [verifyreset] succeeded

7. Log adam0000 into the Linux server.
8. You will be prompted for adam0000's password. Enter in the new password.
9. If the new password was accepted, the password change was successfully propagated and adam0000 will now be logged in.

5 Troubleshooting

If the password change fails to propagate, double check the following:

- Ensure that the instance and AD server firewalls have the correct settings. Incorrect firewall settings will block the change password request from reaching the instance server and the password change will not be propagated.
- The domain controller has been added to list of IP addresses allowed to send socket requests to the IDPM Password Manager Service. Once again, the password change request will not be propagated with the wrong IP address.
- There might be a mismatch on the longid format. As stated before, it must match the longid on the target system.

See also:

See the Transparent Password Synchronization Configuration Guide (**`transparent-sync.pdf`**) for more information about transparent synchronization, including setup on other target system types.