Bravura Pass Implementation: Credential Provider and Secure Kiosk Account

Hitachi ID Bravura Pass includes a key feature to assist mobile users with support for resetting forgotten passwords from the login prompt, even if the user is away from the office and is not physically attached to the Internet. Using this feature, users can resolve problems with their passwords both at the office and mobile, from any endpoint device.

1 Requirement

Users may forget their initial workstation / network login passwords, or lock themselves out of their workstation, and therefore be unable to access their own web browsers. *Login Assistant* uses a secure kiosk account (SKA), a specially constructed and locked down account, to provides users with secure access to the *Hitachi ID Bravura Pass* password change interface from the login prompt on their workstations.

1.1 Initial considerations

Answer the following questions to determine the best solution for the secure kiosk account (SKA).

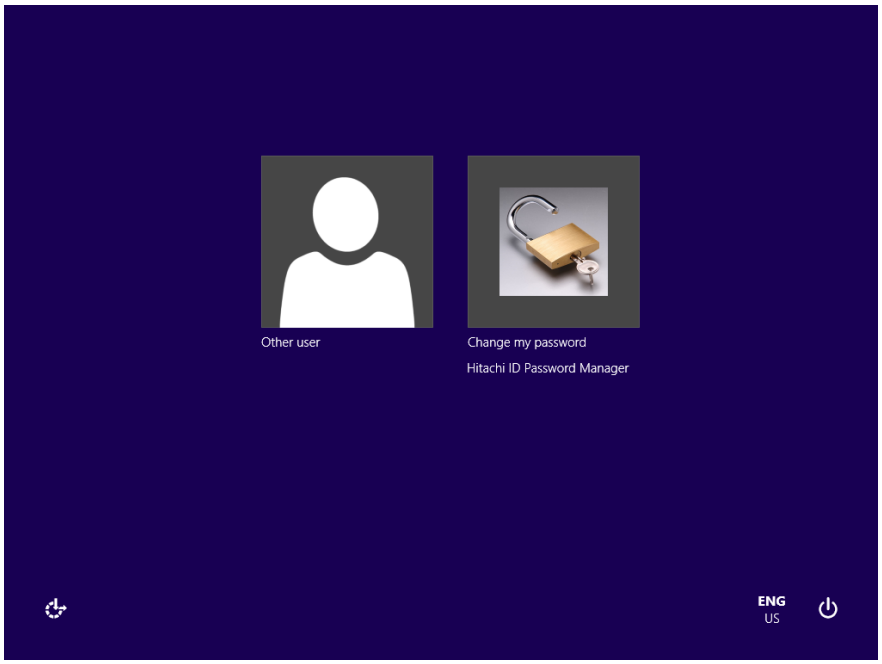
1. Will users be accessing the SKA only from a locally connected network?
2. Will users need to access the SKA from remote locations such as a WiFi hotspot?
3. Will the Credential Provider be installed on a user's workstation or will a domain-level SKA be required?

This document contains:

- Solution: Local Secure Kiosk Account and Credential Provider
- Solution: Credential Provider and Remote access
- Solution: Domain-level Secure Kiosk Account
- Use case: Installing the Local Secure Kiosk Account and Credential Provider
- Use case: Configuring the Domain-level Secure Kiosk Account

2 Solution: Local Secure Kiosk Account and Credential Provider

If a user is locked out of his account because his password has expired or he has entered an incorrect password too many times, or he wants to change his password using *Bravura Pass*, the user can click **Switch User** or **Other Credentials** to access the **Change my password** tile.



The *Hitachi ID Bravura Pass* Credential Provider software adds a **Change my password** tile to the Windows login screen. Clicking the tile launches the secure kiosk account (SKA). The user can then use *Bravura Pass* to change his password or unlock his account.

Alternatively, the user can enter the username and password of the help account to launch the SKA.

3 Solution: Credential Provider and Remote access

The *Login Assistant* client allows locked-out users to connect to the Internet over a WiFi hotspot or using an AirCard. Locked-out users can also establish a temporary Internet connection using their home Internet connection or a hotel Ethernet service.

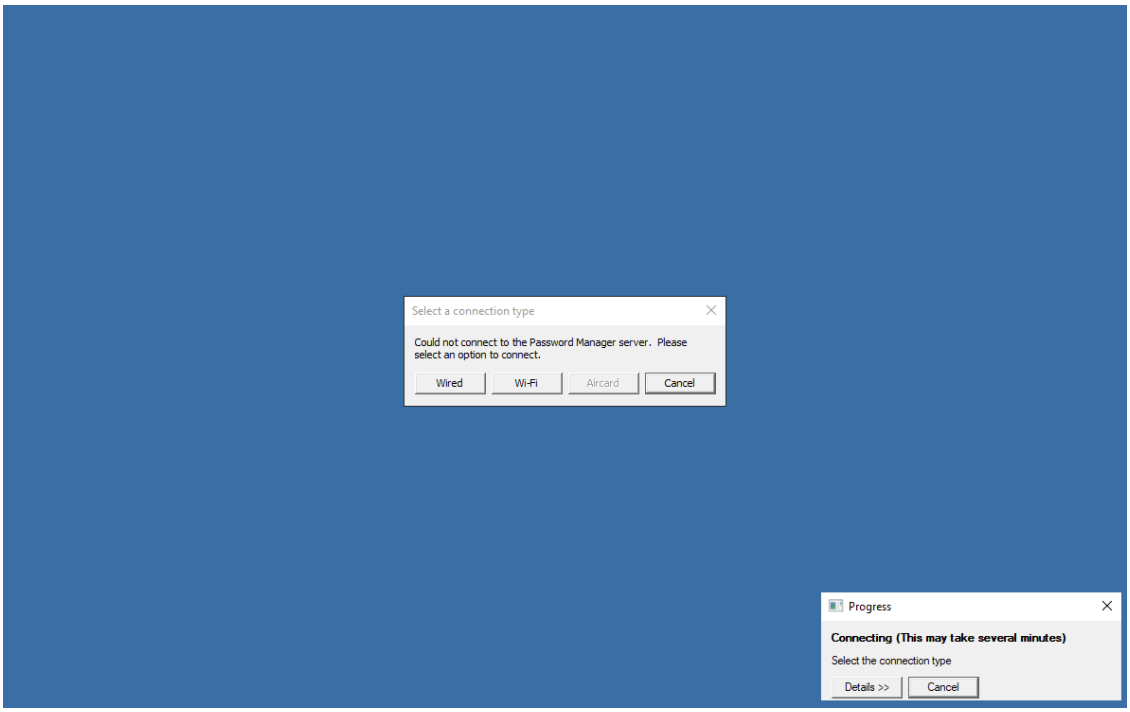
When the *Login Assistant* is run, it can do an immediate check to see if it is connected to the Internet using the external URL and expected data as specified during installation. If connected, then it immediately works the same as a regular *Login Assistant*.

If it cannot connect to the Internet, a prompt asks users to select how to connect, with these options:

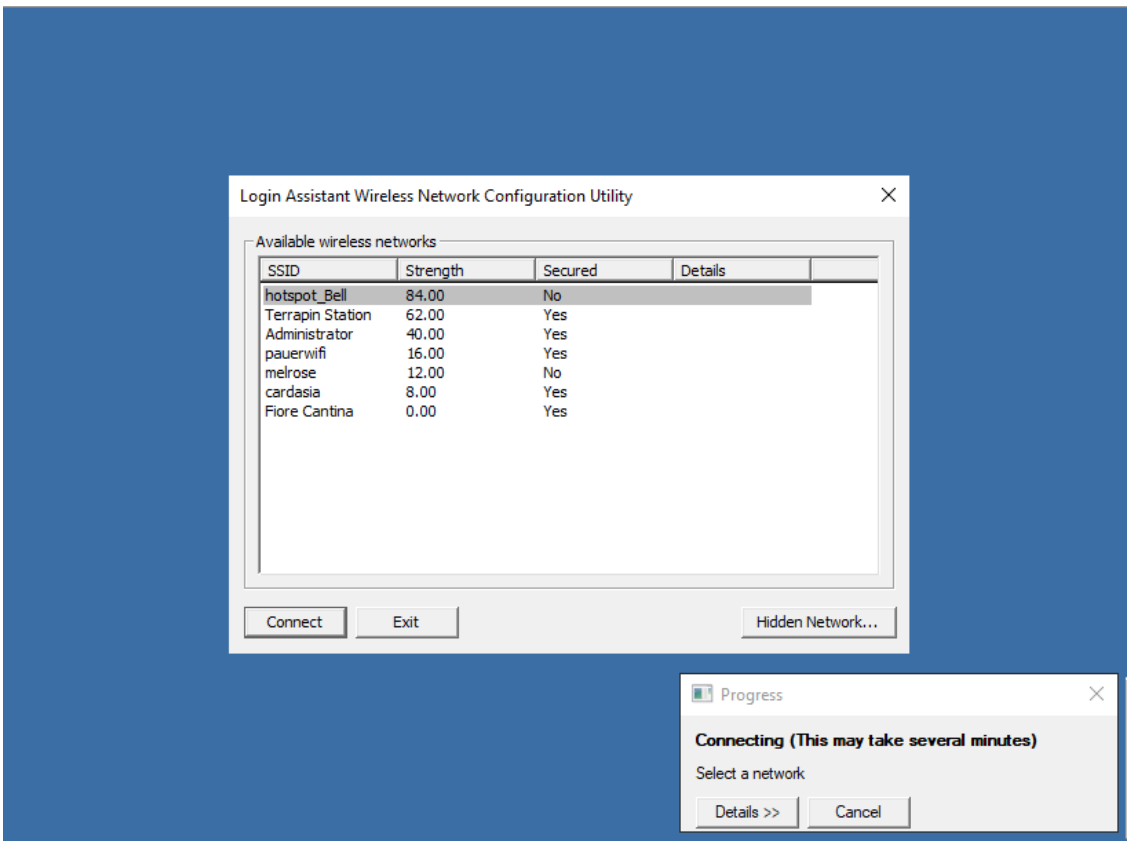
Wired attempt another direct connection

WiFi allow the user to select a WiFi network to connect through

AirCard use a wireless stick if configured.



If WiFi is selected, the *Login Assistant* displays a list of detected networks, allowing the user to select one and potentially enter a network key.



A **Hidden Network...** button allows the user to specify an SSID and password for a hidden wifi connection.

If AirCard is selected, the *Login Assistant* will display the third party application. Once the user has connected the application will disappear.

4 Solution: Domain-level Secure Kiosk Account

You can set up a domain-level SKA if you do *not* want to install software on users' workstations.

A domain-level secure kiosk account is a network login account defined in an Active Directory domain. It typically has a *help* login ID. A security policy is applied to the *help* account that restricts access to the operating system and network resources when using the secure kiosk account (SKA).

5 Use case: Installing the Local Secure Kiosk Account and Credential Provider

5.1 Running the installer

This section shows you how to manually install or upgrade *Login Assistant* on a workstation. See:

- Installing add-on software for general requirements for using a client MSI installer, and instructions for automatic installation using a group policy.
- Add-on Installers in the Bravura Security Fabric *Reference Manual* for more information about setting MSI properties in a transform file or from the command line.

To manually install or upgrade *Login Assistant* on a workstation:

1. Copy the **`ska.msi`** installer, or **`ska-x64.msi`** installer for 64-bit systems, from the addon directory to a scratch directory (C:\temp) on the local workstation or to a publicly accessible share.
2. Launch the installer.

Click **Next**.

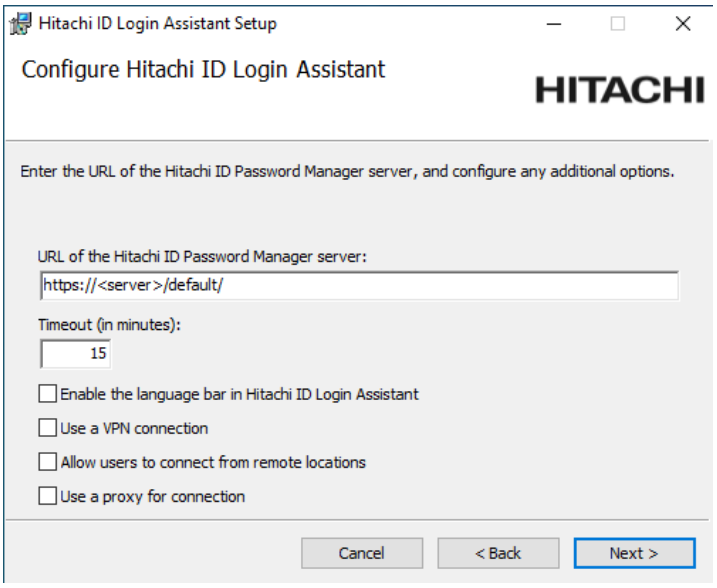
3. Read and accept the license agreement.

   Click **Next**.

4. Click **Typical** to install the Credential Provider.

   Click **Next**.

5. Configure the *Login Assistant*:



URL of the Hitachi ID Bravura Pass server The full path to the *Hitachi ID Bravura Pass* server. The URL can include skin name or other parameters. Do *not* set this URL to a redirect page.

Timeout This is the maximum amount of time the *Login Assistant* secure kiosk account can be used before it automatically closes. Default is 15 minutes.

Enable the language bar in the Login Assistant Select this option if you want users to be able to select a different language while using the *Login Assistant*.

Use a VPN connection Select this option if you want to establish a VPN connection before opening the *Bravura Pass* login page in a kiosk browser.

Allow users to connect from remote locations Select this option if you want users to be able to connect from remote locations, using direct connection, WiFi hotspot, or AirCard. This is generally used along with a VPN connection.

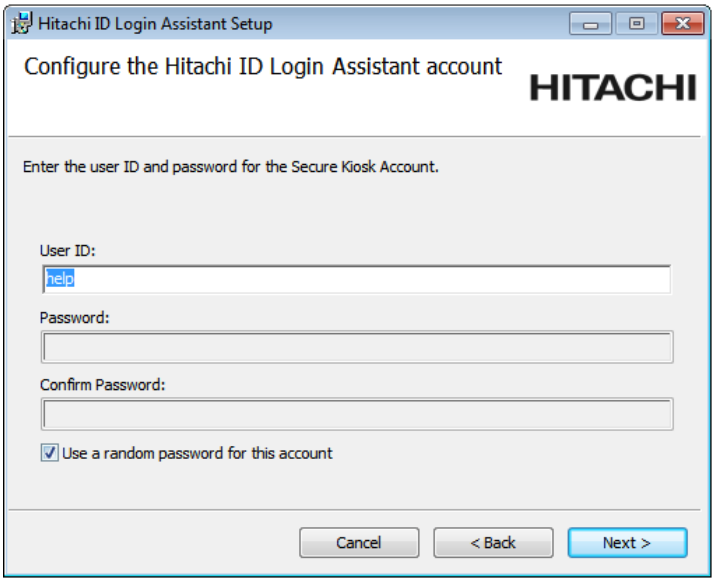
Use a proxy for connection Select this option if you want the secure kiosk account browser to use the Internet Explorer proxy server to connect to the *Bravura Pass* instance. You can configure settings for the proxy in Step 9.

Click **Next**.

6. Set up the help account.

   Type the **User ID** (default is `help`). The help account is used to login and launch **`runurl`**.

   Use the format `<User ID>@<Domain>` or `<Domain>\<User ID>` if the help account is a domain user.



If the **Use random password for this account** checkbox is selected, you do *not* need to enter a password. A random password will be used instead. You must specify a password if you are only installing the *Login Assistant* and not the Credential Provider, or if you are using a domain account.

Click **Next**.

7. Configure a VPN connection program if you selected that option in step 5:

Connect program Name and full path of the program to run in order to establish a VPN connection.

Connect program arguments Command-line arguments for the VPN connect program; for example `-u %USERID% -p %PASSWORD%`.

Disconnect program Name and full path of the program to run to disconnect from the VPN.

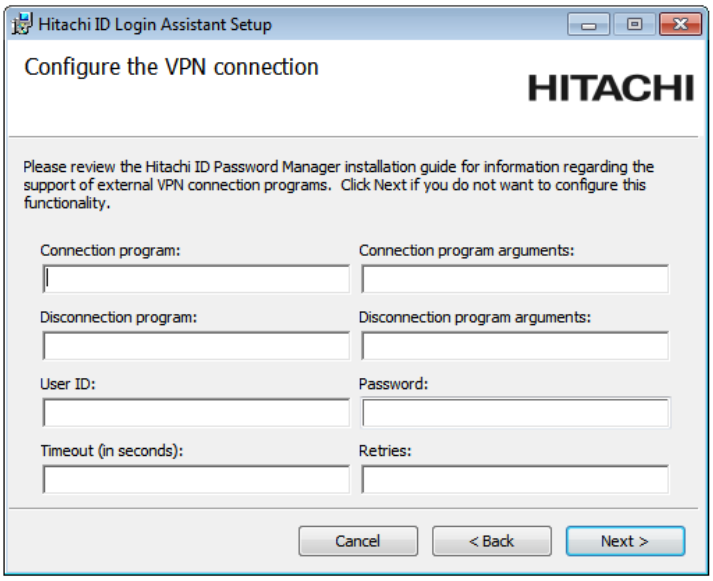
Disconnect program arguments Command-line arguments for the VPN disconnect program; for example `-u %USERID% -p %PASSWORD%`.

User ID To be used with the VPN connect and disconnect programs.

Password For the VPN user ID.

Timeout The period in seconds that the **`runurl`** program should wait before checking to see if connectivity has been established after the VPN connect program has run. The value must be greater than zero.

Retries Number of times to test for connectivity after the VPN connect program has run. The value must be greater than zero.



Click **Next**.

8. Configure the remote account access if you selected that option in step 5:

External URL to test for connectivity This will be the URL of a website that used to determine if the computer is connected to the Internet, or still behind a registration screen or captive portal. This defaults to www.msftncsi.com/ncsi.txt.

Data expected from URL This is a string that is expected from the above website. It should be unique enough to ensure that a registration page will not have the data, but always present on the external URL. The default is `Microsoft NCSI`.

Program to use to create a connection If users will be using an AirCard or Internet stick, this is the name of the program to run in order to connect. This program will be run from the *Login Assistant* to allow the user to connect.

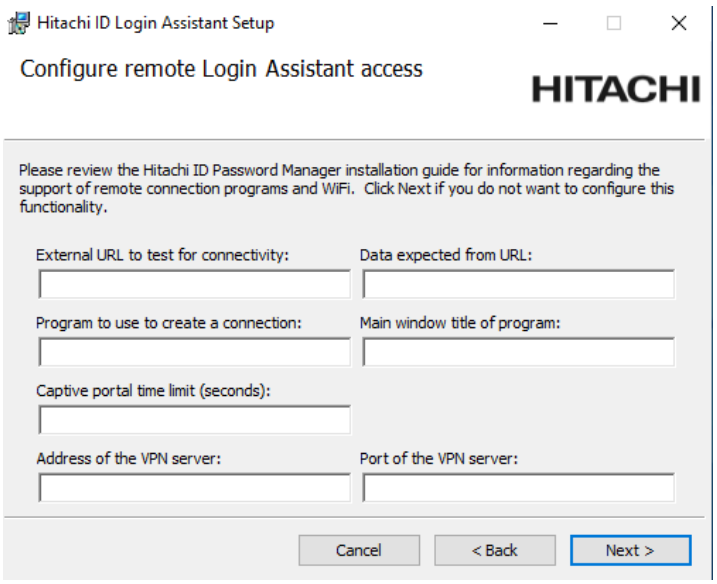
Main window title of program If the **Program to use to create a connection** is used, this is the main window title of the program when run. In AirCard, this is listed under the **Task** column on the **Applications** tab.

Timeout Specify the length of time to wait to see if a connection has been established by the program used to create a connection. The default is 2 seconds.

The defaults should work unless the wireless card connection tends to take a very long time.

Retries The number of times to test for connectivity. The default is 30.

Address of the VPN server / **Port of the VPN server** If specified these allow the remote *Login Assistant* to test a connection to the VPN server to see if it can be accessed before starting the VPN. This can help with better diagnosis and faster connection times.



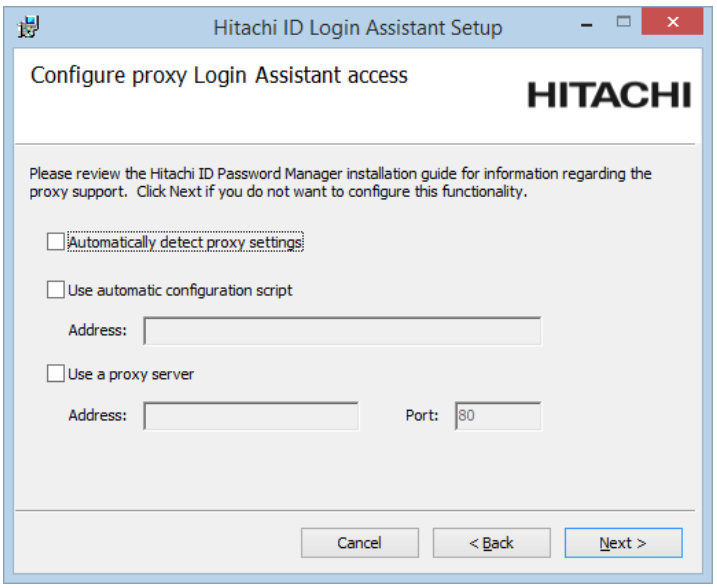
Click **Next**

9. If you chose to use a proxy for connection in step 5, configure the Internet Explorer proxy server for the secure kiosk account. These settings match those set in Internet Explorer → Internet Options → Local Area Network (LAN) Settings:

   Automatically detect proxy settings Sets Internet Explorer proxy server to "Automatically detect settings".

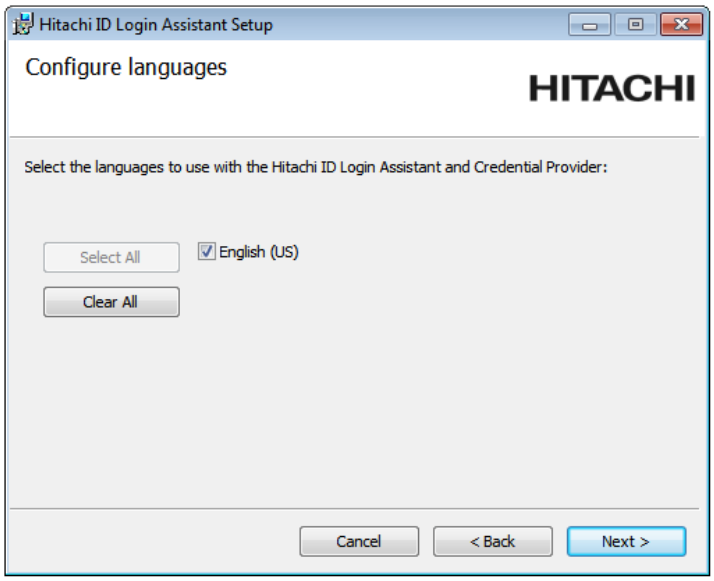
   Use automatic configuration script Sets the proxy server to use "Use automatic configuration script".

   Use a proxy server Sets proxy server to use a manually defined proxy server.

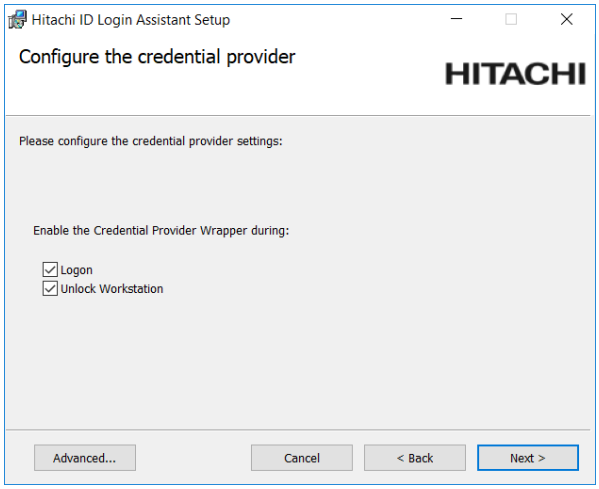


Click **Next**.

10. Select the languages to be displayed by the *Login Assistant*.



Click **Next**.



11. Once you have finished configuring the various installation options, you are prompted to start the installation.

    Click **Install**.

    The installer begins copying files to your computer. The ***Installation Complete*** dialog appears after the software has been successfully installed.

12. Click **Finish** to exit.

    Depending on your installation options, you may be prompted to restart Windows.

6 Use case: Configuring the Domain-level Secure Kiosk Account

Use the following steps if you want to set up a domain-level SKA but do *not* want to install software on users' workstations.

In order to configure an secure kiosk account (SKA) for Microsoft Active Directory:

1. Create the help user (p11).
2. Configure the **runurl** program (p12).
3. Create a policy to lock down Windows workstations (p13).
4. Remove the help account from the *Hitachi ID Bravura Pass* account list, to prevent users from changing the help account password or attaching the ID.
5. Advertise the help account to *Bravura Pass* users (p17).

> **Note:** Unless otherwise stated, all steps are performed on an Active Directory DC (domain controller), and must be performed using administrator credentials. Details vary depending on your version of Windows

7 Creating a help user

To create a *help user* to serve as an secure kiosk account (SKA):

1. Open **Active Directory Users and Computers**.
2. Create a new user with the **User logon name**: `help` and a hard-to-guess password that complies with your password complexity rules. Ensure that you:
   (a) Select the following checkboxes:
      - **User cannot change password**
      - **Password never expires**

   (b) Deselect the following boxes:
      - **User must change password at next logon**
      - **Account is disabled**
3. Create a new global security group named `Help SKA`.
4. Add the help user to the Help SKA group. Set this group as the user's primary group.
5. Close **Active Directory Users and Computers**.

See Microsoft's documentation for detailed steps on how to create an account.

Next:

Configure the **`runurl`** program (Configuring the runurl program).

8 Configuring the runurl program

If you do not install Credential Provider software on users' workstations to allow them to access the domain help account, the **runurl** program, which is used to launch a web browser in kiosk mode, must be installed on a public share accessible to computers in the domain. You can then add **runurl** to the group policy for the help user, and it will be executed when the help user logs into the domain.

To configure the **runurl** program:

1. Copy the files from the addon\Domain Login Assistant\ directory in your *Hitachi ID Bravura Pass* installation to the SYSVOL share on each domain controller.

   You can determine the location of your SYSVOL share by typing `net share` from the command prompt on your DC.

2. Locate the **gina.z** file from the skin\default\en-us\ directory and make a copy of that file to the SYSVOL share as well.

3. Create a text file called **runurl.cfg** that contains arguments (separated by whitespace) for the **runurl** program. Place this file with the other **runurl** files on the SYSVOL share.

   See runurl in the *Reference Manual* for argument description and example syntax.

4. Ensure that Internet Explorer 9 or higher is installed on the domain controller and all workstations that will access the help account. The **runurl** program relies on some components that are part of Internet Explorer 9 or higher.

5. Test **runurl** from a command prompt on the Microsoft Active Directory DC by typing:

   ```
   %LOGONSERVER%\sysvol\runurl.exe -cfg %LOGONSERVER%\sysvol\runurl.cfg
   ```

   Ensure that a web browser opens to the specified URL, and that the workstation is locked down according to the options you specified.

6. Test **runurl** from the command prompt of a workstation logged into the domain by typing:

   ```
   %LOGONSERVER%\sysvol\runurl.exe -cfg %LOGONSERVER%\sysvol\runurl.cfg
   ```

   Ensure that a browser window opens to the specified URL, and that the workstation is locked down according to the options you specified.

Next:

Create a group policy for Windows workstations.

9 Creating the group policy

If you do not install Credential Provider software on users' workstations to allow them to access the domain help account, you must set up a group policy to determine the configuration of a user's desktop environment.

To create a group policy for use with an secure kiosk account (SKA):

1. Create the help account policy. Name the group policy `Help SKA`.
   For example, on Windows 2012:
   (a) Open **Group Policy Management**.
   (b) Under the forest domain sub-section, right-click the domain object, then select **Create a GPO in this domain, and Link it here . . . .**
   The ***New GPO*** dialog appears.
   (c) Name the group policy `Help SKA`.
   (d) Right click on the Help SKA policy you just created, then select **Edit**.
   The **Group Policy Management Editor** snap-in appears.
2. Ensure the help account policy is applied *only* to the Help SKA group.

   WARNING!: Failure to perform this step will result in the Help Account Policy being applied to *every* user – making it almost impossible to log back into the domain.

   (a) In the **Group Policy Object Editor** snap-in, while the Policy is selected, navigate to **Actions** → **Properties**.
   (b) Select the **Security** tab.
   (c) Click **Add**, type `Help SKA`, then click **OK** to add the Help SKA group.
   (d) Select the Help SKA group. Under the permissions for this group, ensure that the **Allow** checkbox is selected in the **Apply Group Policy** row.
   (e) Select the Authenticated Users group. Under the permissions for this group, clear the **Allow** checkbox in the **Apply Group Policy** row.
   (f) Click **OK** to apply the policy.
3. Restrict the help user's rights by configuring the group policy settings as described in:
   - Active Directory 2012, 2016 and 2019 group policy settings
   - Active Directory 2008R2 group policy settings

   All other settings should be left in the "Not configured" state.

See Microsoft's documentation for detailed steps on how to create a group policy.

This group policy is now in effect every time the help user logs into the domain. Should it appear that the group policy is not applying properly, check to ensure that your workstations are using a primary DNS server that supports dynamic updates.

9.1 Active Directory 2012, 2016 and 2019 group policy settings

Policy	Setting
Windows Components	
→ **Internet Explorer**	
Disable AutoComplete for forms	Enabled
→ **AutoPlay Policies**	
Turn off Autoplay	Enabled
Turn off Autoplay on: All drives	
Start Menu and Taskbar	
Remove user's folders from the Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove common program groups from Start Menu	Enabled
Remove Documents icon from Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove Search link from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove Pictures icon from Start Menu	Enabled
Remove Music icon from Start Menu	Enabled
Remove Network icon from the Start Menu	Enabled
Add Logoff to the Start Menu	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate command	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Remove access to the context menus for the taskbar	Enabled
Do not keep history of recently opened documents	Enabled
Turn off personalized menus	Enabled
Force classic Start Menu	Enabled
Remove Balloon Tips on Start Menu items	Enabled
Remove pinned programs list from the Start Menu	Enabled
Remove frequent programs list from the Start Menu	Enabled
Remove All Programs list from the Start Menu	Enabled
Remove the "Undock PC" button from the Start Menu	Enabled
Hide the notification area	Enabled

. . . continued on next page

Policy	Setting
Do not display any custom toolbars in the taskbar	Enabled
Desktop	
Hide and disable all items on desktop	Enabled
Remove My Documents icon on the desktop	Enabled
Remove Computer icon on the desktop	Enabled
Remove Recycle Bin icon from desktop	Enabled
Don't save settings at exit	Enabled
→ **Desktop**	
Disable Active Desktop	Enabled
Control Panel	
Prohibit access to the Control Panel and PC settings	Enabled
→ **Personalization**	
Enable screen saver	Disabled
System	
Don't display Getting Started welcome screen at logon	Enabled
Custom user interface	Enabled
Interface filename:	%LOGONSERVER%\sysvol\runurl.exe -cfg %LOGONSERVER%\sysvol\runurl.cfg
Run only specified Windows applications	Enabled
List of allowed applications:	runurl.exe
→ **Ctrl+Alt+Del Options**	
Remove Task Manager	Enabled
Remove Lock Computer	Enabled
Remove Change Password	Enabled

9.2 Active Directory 2008R2 group policy settings

Policy	Setting
Windows Components	
→ **Internet Explorer**	
Disable AutoComplete for forms	Enabled
Turn off Managing Phishing filter	Enabled
Select phishing filter mode: Off	
→ **AutoPlay Policies**	
Turn off Autoplay	Enabled
Turn off Autoplay on: All drives	
Start Menu and Taskbar	
Remove user's folders from the Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove common program groups from Start Menu	Enabled
Remove Documents icon from Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove Search link from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove Pictures icon from Start Menu	Enabled
Remove My Music icon from Start Menu	Enabled
Remove Network icon from the Start Menu	Enabled
Add Logoff to the Start Menu	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate command	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Remove access to the context menus for the taskbar	Enabled
Do not keep history of recently opened documents	Enabled
Turn off personalized menus	Enabled
Force classic Start Menu	Enabled
Remove Balloon Tips on Start Menu items	Enabled
Remove pinned programs list from the Start Menu	Enabled
Remove frequent programs list from the Start Menu	Enabled
Remove All Programs list from the Start Menu	Enabled
Remove the "Undock PC" button from the Start Menu	Enabled
Hide the notification area	Enabled
Do not display any custom toolbars in the taskbar	Enabled
Desktop	
Hide and disable all items on desktop	Enabled
Remove My Documents icon on the desktop	Enabled
Remove Computer icon on the desktop	Enabled
Remove Recycle Bin icon from desktop	Enabled
Don't save settings at exit	Enabled

. . . continued on next page

Policy	Setting
→ **Desktop**	
Disable Active Desktop	Enabled
Control Panel	
Prohibit access to the Control Panel	Enabled
→ **Personalization**	
Enable screen saver	Disabled
System	
Don't display Getting Started welcome screen at logon	Enabled
Custom user interface	Enabled
Interface filename:	%LOGONSERVER%\sysvol\runurl.exe -cfg %LOGONSERVER%\sysvol\runurl.cfg
Run only specified Windows applications	Enabled
List of allowed applications:	runurl.exe
→ **Ctrl+Alt+Del Options**	
Remove Task Manager	Enabled
Remove Lock Computer	Enabled
Remove Change Password	Enabled

10 Advertising Login Assistant

If you do not install Credential Provider software on users' workstations to allow them to access the domain help account, users must be educated to use it when they cannot remember their passwords, or when their passwords have been locked out.

There are several ways to do this:

- Add instructions to the help desk voice response system, so that users who call for help are instructed to try to log in with the help account.
- Configure a domain policy to display a message to users attempting to logon.
- Deploy a login screen background image to users' workstations, so that the instructions to try the help account are always on the users' screens.
- Add instructions about the help account to whatever media are distributed to users to tell them about the corporate help desk. For example, some companies print information about how to call the help desk on mouse pads.

10.1 Displaying message text to users at logon

You can configure Windows to display a message to users when they log on. You can customize the message to educate or remind users about the help account. The message appears after the user presses **[Ctrl]**+**[Alt]**+**[Del]**. After the user reads the message and clicks **OK**, they can proceed with the logon process.

The message text to display to users is configured by modifying the domain security policy.

To display a message to users at logon:

1. On the domain controller, start the **Domain Security Policy** snap-in.
   - On Windows 2012, click **Windows Button** → **Apps** → **Local Security Policy**.
2. Expand **Security Settings** → **Local Policies** → **Security Options**.
3. In the right pane, follow these steps to create the message text:
   - On a Windows Server-based domain controller:
     (a) Click **Interactive logon: Message title for users attempting to log on**, and then type the text that you want to appear in the dialog title bar.
     (b) Click **Interactive logon: Message text for users attempting to log on**, and then type the text that you want to appear in the body of the message.

The policy will take effect after the client has been rebooted.