

Self-Service Anywhere

Implementation Guide

Software revision: 12.2.4
Document revision: 30072
Last changed: 2022-03-01

Contents

I	SELF-SERVICE ANYWHERE	1
1	Self-Service Anywhere	2
1.1	Password expiry warning for mobile users	2
1.1.1	Setting up expiry notification and self-service password reset for mobile users	3
1.2	Reset forgotten, cached passwords while away from the office	4
1.2.1	Setting up local self-service password reset for mobile users	5
1.3	Unlock encrypted hard disk	5
1.4	Smart card PIN reset	6
1.4.1	Setting up smart card PIN reset	7
1.5	Low cost multi-factor authentication using mobile phones	7
II	LOCAL RESET EXTENSION	9
2	Resetting cached credentials	10
2.1	Resetting cached credentials on a user's workstation	10
2.1.1	The problem for remote users	10
2.1.2	The <i>Hitachi ID Bravura Pass</i> solution using the Local Reset Extension	11
2.1.3	Updating locally protected resources	12
2.2	Installing Local Reset Extension	12
2.2.1	Local Reset Extension installer for Internet Explorer 11 and Microsoft Edge Legacy	13
2.2.2	Excluding users and groups	15
2.2.3	Installing Local Reset Extension automatically on Internet Explorer	16
2.2.4	Installing Local Reset Browser Extension on Chrome or Edge Chromium	16
2.2.5	Installing Local Reset Browser Extension on Firefox	17
2.3	Configuring the Local Reset Extension plugin	18

2.3.1	Usage	18
2.3.2	Requirements	18
2.3.3	Customization	19
2.3.4	Use case	19
2.3.5	Testing	20
III	LOGIN ASSISTANT (SKA)	22
3	Resetting Passwords from a Login Prompt	23
3.1	Types of secure kiosk account implementation	23
3.2	Login Assistant software	24
3.2.1	Credential Provider for Windows	24
3.2.2	Remote access	25
3.3	What happens when users log in	27
3.4	Enabling password changes from a login prompt	28
3.4.1	Domain-level secure kiosk account	28
3.4.2	Workstation secure kiosk account	28
3.5	Notes on usage	29
3.5.1	Local password cache	29
4	Installing Login Assistant Software on Workstations	30
4.1	Windows	30
4.1.1	Requirements	30
4.1.2	Running the installer	31
4.1.3	Command-line Cisco anyConnect VPN parameters	37
4.1.4	Displaying JavaScript Errors	37
4.1.5	Uninstalling	38
4.1.6	Troubleshooting	38
5	Setting up Login Assistant for Remote Users	39
5.1	User Experience	39
5.2	Technical requirements	40
5.2.1	VPN requirements	42

5.2.2	Active Directory requirements	42
5.3	Configuration and usage notes	43
5.3.1	Timeout	43
5.3.2	Credential provider and the help account	43
5.3.3	Connections over VPN	44
5.3.4	Logging SKA remote connection failure	44
5.3.5	Password propagation delays between DCs	45
5.3.6	Disaster recovery	45
6	Setting up Login Assistant on a Domain (No Workstation Software)	46
6.1	Creating a help user	47
6.2	Configuring the runurl program	47
6.3	Creating the group policy	48
6.3.1	Active Directory 2012, 2016 and 2019 group policy settings	49
6.3.2	Active Directory 2008R2 group policy settings	51
6.4	Advertising Login Assistant	53
6.4.1	Displaying message text to users at logon	53
IV	INTERACTIVE VOICE RESPONSE SYSTEMS	55
7	Integrating with Interactive Voice Response Systems	56
7.1	Architecture	57
7.2	IVR with touch-tone identification	58
7.2.1	Assigning unique, numeric IDs	58
7.2.2	Numeric mapping of alphanumeric login IDs	58
7.2.3	Selecting an IVR ID source	58
7.3	IVR with touch-tone authentication	59
7.3.1	IVR question sets	59
7.3.2	Configuring IVR question sets	60
7.4	IVR with voice print authentication	61
7.4.1	Registering voice prints	61
7.5	Implementation Options	63
7.5.1	Buying a new IVR system vs. extending an existing system	63

7.5.2	Turn-key IVR options offered by Hitachi ID Systems	64
7.5.3	Leveraging an existing authentication process	64
7.6	Managing RSA SecurID tokens from a telephone	64
7.7	Password resets from a telephone	65
7.7.1	Enabling password resets from a telephone	65
V	ENCRYPTED SYSTEMS	67
8	Unlocking encrypted systems via the <i>Bravura Pass</i> web interface	68
8.1	Overriding the string format for challenge/response codes	69
8.1.1	Examples	70
A	Installing Add-on Software	73
A.1	Using MSI installers	73
A.1.1	Requirements	73
A.1.2	Manual installation	74
A.1.3	Customizing an MSI	74
A.1.4	Automatic installation using a group policy	74
A.2	Enabling logging	76
A.3	Configuring ActiveX security	76
A.3.1	Configuring internet options on a workstation	77
A.3.2	Using GPOs to globally configure Internet Explorer/ActiveX security settings	77
B	Customizing installer (MSI) options	82
B.1	pslocalr.msi / pslocalr-x64.msi	83
B.1.1	Features	83
B.1.2	Properties	83
B.2	ska.msi / ska-x64.msi	83
B.2.1	Features	83
B.2.2	Properties	84
C	SKA client: runurl	88
C.1	Requirements	88
C.2	Usage	89

- C.3 Enabling or disabling key combinations 90
- C.4 Examples 91
- D skautil 92
- E File Locations 93
 - E.1 Bravura Security Fabric directories and files 93
 - E.1.1 Instance directory 94
 - E.1.2 Log directory 96
 - E.1.3 Locks directory 97
 - E.2 Connector pack directories and files 98
- Index 99

Part I

SELF-SERVICE ANYWHERE

Self-Service Anywhere

1

Hitachi ID Bravura Pass includes key features to assist mobile users:

1. Email notification to users about upcoming password expiry, since the notice displayed at the Windows login prompt is not shown to users away from the office.
2. Support for resetting forgotten encryption keys for users whose PCs are protected with full disk encryption.
3. Support for resetting forgotten passwords or PINs from the login prompt, even if the user is away from the office and is not physically attached to the Internet.

These features are collectively referred to as *Self Service, Anywhere (SSA)*. Using these features, users can resolve problems with their passwords, smart cards, tokens or full disk encryption software both at the office and mobile, from any endpoint device.

1.1 Password expiry warning for mobile users

Problem	Mobile users are not notified by Windows when their passwords are about to expire. Users who infrequently connect their laptop to the office network, instead checking email with a solution such as Outlook Web Access, suffer regular password expiry and require frequent password resets.
Solution	<i>Hitachi ID Bravura Pass</i> sends users emails warning of imminent password expiry. Users change passwords using a web browser. Password Manager Local Reset Extension refreshes the password on their laptop.

The solution involves the following components:

Components	Purpose
Notification Service (psntfsvc)	<p>updates the database with information about notification events and compliance rules, and runs plugins that:</p> <ul style="list-style-type: none"> • Check if a user is in compliance for a particular event • Send reminders to non-compliant users, either by web or email • Take action if the reminder limit for a user is exceeded • Generate a list of non-compliant users for batch notification
<i>User notifications</i> (PSN) module	Can be used to notify users of pending password expiry via a web page.
<i>Change passwords</i> (PSS) module	Enables users to change passwords for one or more of their accounts.
Password Manager service (idpm)	Can be used to queue password changes if they fail on a target system.
Local Reset Extension	Resets passwords and clears cached credentials on users' local workstations.
cgilocalr.exe	The program that supplies HTML to the password status page of the <i>Change passwords</i> (PSS) module for the S STATUS EXT plugin point.
cgilocalr.cfg	The configuration file for cgilocalr.exe .

1.1.1 Setting up expiry notification and self-service password reset for mobile users

To set up self-service password reset for mobile users:

1. Set up web-based password management features, including expiry notification, as described in the [Bravura Security Fabric Documentation](#).
2. Enable the Local Reset Extension, as described in [Resetting cached credentials](#).

1.2 Reset forgotten, cached passwords while away from the office

Problem	Laptop users sometimes change their password before leaving the office and may forget the new password when they need to use it while not attached to the corporate network. Without a technical solution, the IT help desk cannot resolve these users' problem until they return to the office. User laptops are rendered inoperable until they return to the office.
Solution	A <i>Hitachi ID Bravura Pass</i> client software component allows users who forgot their primary, cached Windows password and cannot sign into their PC 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. Once the user's laptop is on the Internet, <i>Bravura Pass</i> establishes a temporary VPN connection and launches a kiosk-mode (full screen, locked down) web browser. The user steps through a self-service password reset process and <i>Bravura Pass</i> uses an ActiveX component to reset the locally cached password to the same new value as was set on the network back at the office.

The solution involves the following components:

Components	Purpose
<i>Change passwords</i> (PSS) module	Enables users to change passwords for one or more of their accounts.
Password Manager service (idpm)	Can be used to queue password changes if they fail on a target system.
<i>Login Assistant</i>	client software that works with a specially constructed and locked-down account, defined on a Windows workstation (7 or higher). It is typically used to allow users, who forgot or otherwise disabled their login password, access to a self-service password reset facility.
Password Manager Local Reset Extension	Resets passwords and clears cached credentials on users' local workstations.
<code>cgilocalr.exe</code>	The program that supplies HTML to the password status page of the <i>Change passwords</i> (PSS) module for the S STATUS EXT plugin point.
<code>cgilocalr.cfg</code>	The configuration file for <code>cgilocalr.exe</code> .

1.2.1 Setting up local self-service password reset for mobile users

To set up local self-service password reset for mobile users:

1. Set up web-based password management features as described in the [Bravura Security Fabric Documentation](#).
2. Enable the Local Reset Extension, as described in [Resetting cached credentials](#).
3. Enable the *Login Assistant*, as described in [self-service-anywhere.pdf](#).

1.3 Unlock encrypted hard disk

Problem	<p>Organizations deploy full disk encryption (FDE) software to protect against data leakage in the event that a corporate laptop is lost or stolen. Users with FDE on their PCs normally have to type a password to unlock their hard disk, before they can boot up an operating system. This password is normally synchronized with the user's primary Windows password, so that the user only has to remember and type a single password at login.</p> <p>If a user forgets his hard disk encryption unlock password, the user will be unable to start his operating system or use his computer. This is a serious service disruption for the user and can contribute to significant support costs for the IT help desk.</p>
IVR solution	<p>Most FDE packages include a key recovery process at the PC boot prompt. This normally involves a challenge/response process between the FDE software, the user, an IT support analyst and a key recovery server. <i>Hitachi ID Bravura Pass</i> can front-end this process using an integrated telephony option, so that users can perform key recovery 24x7, from any location, using their telephone and without talking to a human help desk technician.</p>
Web solution	<p>Users with access to the <i>Bravura Pass</i> web interface can also recover an encrypted system through the <i>Unlock encrypted systems/accounts</i> (HDD) module, which will provide them with instructions on how to acquire a challenge code for the system, if required. The relevant connector will use this challenge code to generate a response code that can be used to unlock the encrypted device.</p>

The components used in the solution depend on the type of FDE software, and other requirements of your organization. *Hitachi ID Connector Pack* ships with connectors for systems including Check Point, McAfee EndPoint Encryption, and PGP Whole Disk Encryption (WDE).

- The Check Point connector works with *Phone Password Manager* or a custom application to communicate between Check Point and *Bravura Pass* servers.
- The PGP WDE connector works with *Phone Password Manager* and an ActiveX control, `nplocalr`, to update locally protected resources.

For more information see:

- [Integrating with Interactive Voice Response Systems](#) to learn how to interface with interactive voice response (IVR) systems.
- [Configuring the Local Reset Extension plug-in](#) to learn how to enable the `nplocalr` Local Reset Extension.
- The *Phone Password Manager* Configuration Guide for details on installing and configuring *Phone Password Manager*.
- [Unlocking encrypted systems via the Bravura Pass web interface](#) for information about configuring the *Unlock encrypted systems/accounts* (HDD) module.
- The Connector Pack Integration Guide for information about integrating with hard drive encryption systems.

1.4 Smart card PIN reset

Problem	Organizations deploy smart cards to strengthen their authentication processes. Users typically sign into their PC by inserting their smart card into a reader and typing a PIN. If users forget their PIN or leave their smart card at home, they cannot sign into their PC. PIN reset is a complex support process since the new PIN has to be physically installed on the user's smart card. This means that IT support may trigger a physical visit to the help desk.
Solution	<i>Hitachi ID Bravura Pass</i> allows users to access a self-service web portal from anywhere, including from the locked out login screen of their laptop, even away from the office (even using WiFi, as described earlier). Once a user signs into the self-service portal, <i>Bravura Pass</i> can download an ActiveX component to the user's web browser, to communicate with the smart card and reset the forgotten PIN. <i>Bravura Pass</i> can also be used to assign a user a temporary login password (often a very long and random one) to be used in the event that a user left his smart card at home.

The solution involves the following components:

Components	Purpose
<i>Change passwords</i> (PSS) module	Enables users to change passwords for one or more of their accounts.
Password Manager service (idpm)	Can be used to queue password changes if they fail on a target system.
<code>scpinplugin</code>	The <code>scpinplugin</code> works with the ActiveX control <code>HISCPINToolAX.ocx</code> to reset smart card PINs. PIN strength checking can be done by checking the combinations of rules specified in a configuration file and the <i>Bravura Pass</i> password policy.

1.4.1 Setting up smart card PIN reset

To set up local self-service smart card PIN reset:

1. Set up web-based password management features as described in the [Bravura Security Fabric Documentation](#).
2. Configure the smart card PIN reset plugin as described in [CGI / HTML](#) in the *Bravura Security Fabric Reference Manual*.

1.5 Low cost multi-factor authentication using mobile phones

Hitachi ID Bravura Pass supports low-cost, multi-factor authentication into its own request portal, using a smart phone as a secondary authentication factor.

This solution is implemented using two technologies included with *Bravura Pass*:

1. Managed enrollment, which automatically invites users to:
 - (a) provide their mobile phone number; and/or
 - (b) provide their personal email address; and/or
 - (c) install the *Hitachi ID Bravura One* app on their phone.
2. Having enrolled,
 - (a) If the user connects from outside the private/secure corporate network, start with a CAPTCHA.
 - (b) Next, prompt for the user's login ID.
 - (c) Fingerprint the user's browser – if the indicated user has signed on successfully from the same browser before, this fact can act as an unobtrusive authentication factor.
 - (d) If the user connects from a browser or location not seen before, prompt for another factor, which may be any of the following:
 - i. If the user has been activated to use a third party MFA technology, such as a one time password token (e.g., RSA SecurID) or a third party app (e.g., Duo Security, Okta Verify), use that.
 - ii. If the user had previously installed *Mobile Access* on their phone, either use push notification to display a PIN on their phone or display a cryptographic challenge in the login screen as a QR code, which the user scans with the app.
 - iii. If the user had previously enrolled their mobile phone number, send a PIN to the user's phone, via SMS and prompt the user to enter it.¹

¹Note: an SMS broker is required to do this, which may cost as much as a few cents per message.

- iv. If the user had previously enrolled their personal email address, send a PIN to that address, on the assumption that the user has email access on their phone.
- (e) Users may be prompted to select one of several MFA options or one of several alternatives for the same option (e.g., send a PIN via SMS to one of multiple mobile numbers or email addresses).
- (f) Finally, depending on whether the user remembers his password, prompt the user to enter it or answer a series of security questions. Using a second, "knowledge" factor reduces the risk of compromised authentication due to lost or stolen phones or hardware tokens.

See the Hitachi ID Bravura One Configuration Guide for detailed information about installing and configuring Hitachi ID Bravura One.

Part II

LOCAL RESET EXTENSION

Resetting cached credentials

2

Hitachi ID Bravura Pass uses a Local Reset Extension to update cached network credentials on a user's Windows client workstation after a successful web-based password reset. This addresses the issue of intruder lock-outs caused by workstations continuing to log into network resources using cached, no-longer-valid passwords.

2.1 Resetting cached credentials on a user's workstation

After a password change with a web-based password management system, the cached credentials on a user's workstation may become unsynchronized with the user's new domain password:

- When a user logs into Windows, the workstation stores their domain credentials in a cache in memory.
- When the user logs into other resources on the workstation (shares, printers, Outlook/Exchange mail boxes, IIS web sites), it first tries its cached domain password, and if this fails, it prompts the user to type the correct password.
- If the user changes their domain password from the workstation there are no issues updating the local cache. On Windows for example, with the **[Ctrl]-[Alt]-[Delete]** process, Windows updates the local cache, and there is no problem.
- If the Help desk, another workstation, or a web application changes the user's password on the domain, then the workstation cache becomes unsynchronized with the new domain password. Subsequent attempts to access network resources from the workstation use the cached password, increment the user's "failed login attempts" counter, and ultimately trigger an intruder lockout.

2.1.1 The problem for remote users

When a remote user logs into an internal network using an RAS or VPN connection, their current workstation may cache the user's login credentials. If the user did not log into a domain (they have IP connectivity only), the cached credentials do not get updated when the user resets their passwords using the *Hitachi ID Bravura Pass* web interface.

If a user's cached and domain (current) credentials conflict, they will be unable to log back into their workstation without first logging into the domain. If RAS is configured to use the cached Windows password, the user will not be able to log back into the RAS network even when IP connectivity is restored.

2.1.2 The Bravura Pass solution using the Local Reset Extension

To eliminate these problems, *Hitachi ID Bravura Pass* utilizes the component of Local Reset Extension on most browsers including Internet Explorer, Chrome, Edge Chromium and Firefox, that can silently update the user's password cache on the workstation after a web-based password change.

The Local Reset Extension:

- Works on Windows client versions 7 and newer for both 32-bit and 64-bit versions.
- Is able to recognize users who log in with IDs in the `<userid>@<domain>` format as well as the standard Profile ID.
- Works with Internet Explorer, Google Chrome, Microsoft Edge Chromium and Mozilla Firefox. In IE, browser settings "Download signed ActiveX controls" and "Run ActiveX controls and plugins" must both be enabled, as with any ActiveX controls.
- Is signed by Hitachi ID Systems.
- Is normally cached by the supported web browser, so is generally only downloaded once.

Where Local Reset Extension is used to update cached domain passwords, the user's workstation must be on the network and be able to authenticate to the domain. This works for locally-attached users and users on a corporate VPN connection. Local Reset Extension cannot update cached passwords for users accessing *Bravura Pass* through a reverse web proxy from outside the corporate network.

The extension automatically integrates with *Login Manager* when both programs are installed on the workstation, ensuring that *Login Manager* is made aware of all cached password updates.

It is recommended that, after users reset their cached password using Local Reset Extension, they then log out and then log back into the workstation in order to ensure network connectivity. The *Change passwords* (PSS) module displays a message after a password reset:

If you were logged into your workstation, log out now. You must log in with your new password to ensure that your workstation does not try to use your old password to access network resources.

2.1.2.1 Notes on using the Local Reset Extension with Login Assistant on IE

If both the Local Reset Extension ActiveX control and *Login Assistant* are installed together on the same workstation, and users reset their passwords after choosing the Credential Provider tile, or logging in directly with the secure kiosk account (SKA), the cached passwords will not be reset successfully using the default configuration.

Internet Explorer settings must be modified to allow cached password to be reset successfully. The required changes for the security zone vary based on your organization's corporate policy. See [Configuring ActiveX security](#) for more information.

Contact Hitachi ID for assistance to create a customized transform file for `pslocalr.msi` or `pslocalr-x64.msi`.

Note that this does *not* apply when users reset their passwords within Windows, since the settings for Internet Explorer may be directly modified using that method.

Alternatively you may also configure a domain policy for a GPO to create the required Internet Explorer registry entries for the help account. See [Using GPOs to globally configure Internet Explorer/ActiveX security settings](#).

2.1.3 Updating locally protected resources

The Local Reset Extension for Internet Explorer includes **nplocalr.ocx**, which is designed to update locally protected resources. It can be used to clear PGP WDE cache passwords so that the new password can be used on the next start-up of the PGP client.

See the Connector Pack Integration Guide for information about integrating with PGP WDE encryption clients.

2.2 Installing Local Reset Extension

The Password Manager Local Reset Extension can be used with the following browsers:

- Internet Explorer 11
- Microsoft Edge Legacy
- Edge Chromium
- Google Chrome
- Firefox

Note: The Local Reset Extension only works on Windows. Mac OS X and other operating systems are not supported.

The Password Manager Local Reset Extension can be installed by:

- Manually running the appropriate installer:
 - **firefox-extension-win-x86.msi** or **firefox-extension-x64.msi** for Firefox.
 - **browser-extension-win-x86.msi** for Edge Chromium or Google Chrome.
 - **pslocalr.msi** / **pslocalr-x64.msi** for Internet Explorer 11 and Microsoft Edge Legacy.

Note: Firefox, Edge Chromium and Google Chrome require a Hitachi ID Systems browser extension to be installed in addition to the native extension. The user will be prompted to install the browser extension the first time they attempt to reset their password.

See the following section to learn how to install on Internet Explorer 11 or Microsoft Edge Legacy:

- [Internet Explorer 11 or Microsoft Edge Legacy \(p13\)](#)

- Automatically downloading when a user resets a password using *Hitachi ID Bravura Pass*.

See the following sections to learn how to install on specific browsers:

- [Internet Explorer \(p16\)](#)
- [Chrome or Edge Chromium \(p16\)](#)
- [Firefox \(p17\)](#)

- Automatically running the appropriate MSI installer using group policy.

Note: Firefox, Edge Chromium and Google Chrome require a Hitachi ID Systems browser extension to be installed in addition to the native extension. The user will be prompted to install the browser extension the first time they attempt to reset their password.

2.2.1 Local Reset Extension installer for Internet Explorer 11 and Microsoft Edge Legacy

This section shows you how to manually install the Local Reset Extension for Internet Explorer 11 and Microsoft Edge Legacy using the Windows Installer. See:

- [Installing Add-on Software](#) for general requirements for using a client MSI installer, configuring ActiveX security, and instructions for automatic installation using a group policy.
- [pslocalr.msi / pslocalr-x64.msi](#) for Password Manager Local Reset Extension installation options.
- [Add-on Installers](#) in the *Reference Manual* for a listing of MSI properties.

The installers are included in the `addon` directory:

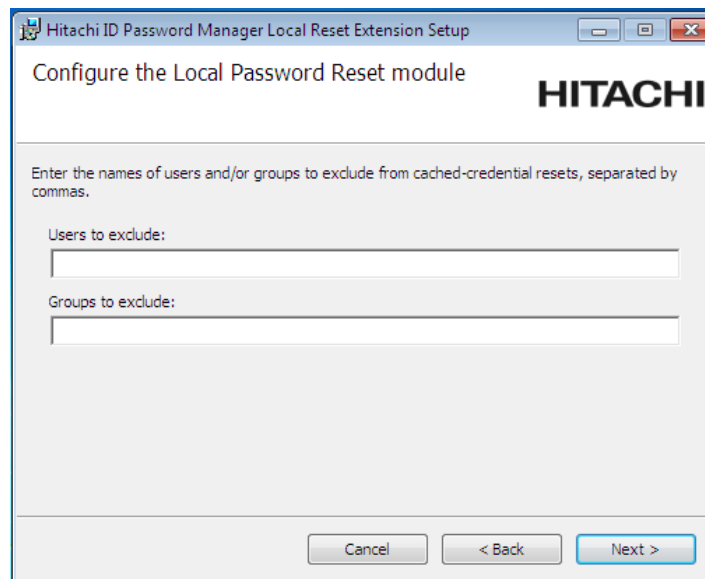
- `pslocalr.msi` for supported Windows 32-bit clients
- `pslocalr-x64.msi` installer for supported Windows 64-bit clients

The `pslocalr.msi` installer may also be used on a Windows 64-bit system, but only the 32-bit Local Reset Extension will be installed for use with Internet Explorer 32-bit. You must use `pslocalr-x64.msi` if you need support for Internet Explorer 64-bit. The `pslocalr-x64.msi` installer is compatible with both the 32-bit and 64-bit versions of Internet Explorer on Windows 64-bit systems.

Note: The `pslocalr-x64.msi` installer adds two copies of `pslocalr.ocx` and `nplocalr.ocx` on Windows 64-bit systems; one in the `C:\Program Files` directory for the 64-bit version, and another in the `C:\Program Files (x86)` directory for the 32-bit version. The registry settings are also duplicated for both the 32-bit and 64-bit locations. This is required in order for the Local Reset Extension to work with both the 32-bit and 64-bit versions of Internet Explorer.

To manually install the *Hitachi ID Bravura Pass* local reset extension:

1. Copy the `pslocalr.msi` or `pslocalr-x64.msi` installer from the *Bravura Pass* server to a scratch directory (C:\temp) on the workstation, or to a publicly accessible share.
2. Launch the `pslocalr.msi` or `pslocalr-x64.msi` 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 install the ActiveX component and configure users or groups to exclude from cached-credential resets.Or,
 - **Typical** to install the ActiveX component only, without configuring users or groups to exclude from cached-credential resets.



5. If you selected **Complete** installation, enter the names of users and/or groups to exclude from cached-credential resets, separated by commas. These are users and groups whose passwords you do not want to be managed by *Bravura Pass*.

Note: Do not include domain as part of the excluded users and groups.

Click **Next**.

6. If the **Groups to exclude** field was configured then you must type the **Username** and **Password** of the help administrative account. You must specify the name of the primary domain controller that the help administrative account resides on as part of the **Username**.

The Local Reset Extension uses the help administrative account to verify that a user belongs to one of the excluded groups. This must be an existing non-administrative account with read access to group membership for all users on the primary domain.

WARNING!: The help administrative account must not have the same username as *Login Assistant's* help account.

7. Click **Install** to start the installation.

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

8. Click **Finish** to exit.

2.2.2 Excluding users and groups

The **pslocalr.msi** and **pslocalr-x64.msi** installers allow you to customize the installation by specifying users and groups that are to be excluded from cached-credential resets. You can also set this list manually, by modifying appropriate registry settings:

For Windows 32-bit or Windows 64-bit (64-bit pslocalr):

HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi ID\IDM Suite\Local Reset Extension\EXCLUDED_USERS

HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi ID\IDM Suite\Local Reset Extension\EXCLUDED_GROUPS

For Windows 64-bit (32-bit pslocalr):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi ID\IDM Suite\Local Reset Extension\  
EXCLUDED_USERS
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi ID\IDM Suite\Local Reset Extension\  
EXCLUDED_GROUPS
```

WARNING!: Ensure that you are comfortable and knowledgeable in the mechanics of the registry before you attempt to change any configuration settings. Contact support@Hitachi-ID.com if in doubt.

2.2.3 Installing Local Reset Extension automatically on Internet Explorer

Automatic download occurs when a target system is configured to use the local reset extension, and the user clicks **Change password** in the *Change passwords* (PSS) module. If the ActiveX control is already installed, and a newer version is installed on the server, the control is automatically upgraded. Only the 32-bit extension can be downloaded using a 32-bit Internet Explorer client.

In order to use the download method, users must have administrative access to install and register the ActiveX control. If administrative access to install is not available, you must install the ActiveX controls using the MSI installer.

To install the ActiveX control on Internet Explorer as an end user:

1. Reset a password using *Hitachi ID Bravura Pass* in the *Change passwords* (PSS) module using Internet Explorer.

A installation link will display after the password is reset successfully on the target system that is configured to use the local reset extension.

2. Click **Install**.

This opens a pop-up window for the ActiveX component installation.

3. Install and allow the plugin.

2.2.4 Installing Local Reset Browser Extension on Chrome or Edge Chromium

A Chrome extension as well as a native browser extension is required to reset a user's password cache on a workstation when using either Chrome or Edge Chromium. A download link will be available to install the extensions if they have not been installed yet.

To install the Chrome and native browser extension as an end user:

1. Reset a password using *Hitachi ID Bravura Pass* in the *Change passwords* (PSS) module using Chrome or Edge Chromium.

An installation link will display after the password is reset successfully on the target system that is configured to use the local reset extension.

2. Click **Install chrome extension**.

This opens a new browser tab to the Hitachi ID Browser Extension in the Chrome web store.

3. Click **Add to Chrome**.

4. Click **Add extension**.

5. On the password reset result page, click on **Install native extension**.

6. Run the `browser-extension-win-x86.msi` file. Alternatively, download and save the file onto your workstation and run the file.

When running the installer on Windows as an administrator, you can choose to install the browser extension for yourself or for all users on the workstation.

2.2.5 Installing Local Reset Browser Extension on Firefox

A native browser extension is required to reset a user's password cache on a Windows workstation when using Firefox. A download link will be available to install the extensions if it has not been installed yet.

To install the native browser extension on Firefox as an end user:

1. Reset a password using *Hitachi ID Bravura Pass* in the *Change passwords* (PSS) module using Firefox.

A installation link will display after the password is reset successfully on the target system that is configured to use the local reset extension.

2. Click **Install firefox extension**.

A prompt to allow and install the Hitachi ID Browser Add-On is displayed in the browser.

3. On the password reset result page, click on **Install native extension**.

4. If using a Windows 32-bit workstation, run the `firefox-extension-x86.msi` file. If using a Windows 64-bit workstation, run the `firefox-extension-x64.msi` file. Alternatively, download and save the file onto your workstation and run the file.

When running the installer on Windows as an administrator, you can choose to install the browser extension for yourself or for all users on the workstation.

2.3 Configuring the Local Reset Extension plugin

The **cgilocalr** plugin works with ActiveX controls to update local resources and run commands after a web-based password change via *Hitachi ID Bravura Pass*.

- **pslocalr.ocx** silently updates the user's Windows password cache. With this plugin the user may continue using domain resources without logging out and back into their workstation after a password change.
- **nplocalr.ocx** is designed to update locally protected resources. It can be used to clear PGP WDE cache passwords so that the new password can be used on the next start-up of the PGP client.
See the Connector Pack Integration Guide for information about integrating with PGP WDE encryption clients.
- **hidgeneric.ocx** is a generic control that can be used to run arbitrary commands after a password changes.

2.3.1 Usage

The **cgilocalr** plugin triggers local resource updates when a self-service password reset succeeds on a target system as specified in **cgilocalr.cfg**.

To enable **cgilocalr**:

1. Click **Manage the system** → **Modules** → **Change passwords (PSS)**.
2. Add **cgilocalr.exe** in the **S STATUS EXT** field.
The field accepts a comma-delimited list for multiple plugins.
3. Click **Update**.

2.3.2 Requirements

The **cgilocalr** plugin requires a configuration file. The **cgilocalr.cfg** file in the **samples** directory includes example configurations for **pslocalr.ocx**, **nplocalr.ocx** and **hidgeneric.ocx**. Copy the file to the **\<instance>\script** directory, then edit the configuration.

2.3.2.1 Generic control

The generic control, **hidgeneric.ocx**, requires the following parameters for running arbitrary commands:

id Used to identify the generic control

files Download from *Hitachi ID Bravura Pass* instance server's directory `wwwdocs/x86` or `wwwdocs/x64` depending on the client workstation operating system's bitness.

program (optional) The program to run in the `cgilocalr` plugin.

If left blank, `rundl132.exe` will be used.

arguments Arguments or parameters to pass to the **program** or `rundl132.exe`.

2.3.3 Customization

You can customize the user interface text in the `plugin-pslocalr.m4` file. The ActiveX's result messages can also be modified in this M4 file. See the [Bravura Security Fabric Documentation](#) for more information.

2.3.4 Use case

The `cgilocalr` plugin uses the configuration file to specify the target system and AD domain for which passwords should be changed locally, where:

- Each target system on which you want to enable the Local Reset must have an entry containing the target system ID.
- Legacy Active Directory target systems must have a `logonDomain` value. Users passwords will only be reset if they are logged on to their workstation with credentials from this domain.
- `targetid`, `control` and `logonDomain` are case insensitive.

Note: For Active Directory DN targets, the domain information is taken implicitly from the *longid*, and does not need to be explicitly specified by *logonDomain*, which is only used for legacy Active Directory target systems.

For example, a company has an Active Directory Domain Controller managing the domain OFFICE. A target system for this domain controller has already been added with a target system ID of INTERNAL-AD. The following script configures the Local Reset Extension for passwords changed using the web-based interface. The user must be logged onto a workstation that is a member of the domain OFFICE. When the user changes his password on INTERNAL-AD the plugin will immediately update the user's local Windows password cache. Either `pslocalr.ocx` or `hidgeneric.ocx` can be used.

```
# cgilocalr plugin config file to use pslocalr
# KVGROUP-V2.0
"" "" = {
    "targetid" "INTERNAL-AD" = {
        "control" "pslocalr" = {
            "protocol" = "2";
            "attributes" "" = {
                "logonDomain" = "OFFICE";
            };
        };
    };
};
```

```
};
};
```

or,

```
# cgilocalr plugin config file to use generic control
# KVGROUP-V2.0
"" "" = {
  "targetid" "INTERNAL-AD" = {
    "control" "generic" = {
      "id" = "pslocalr";
      "files" "" = {
        "file" = "pslocalr.ocx";
      };
      "arguments" = "pslocalr.ocx,ResetCachedPassword2 %HID_ENCRYPTED_DATA%";
      "attributes" "" = {
        "logonDomain" = "OFFICE";
      };
    };
  };
};
};
```

Furthermore, workstation lock down after successfully updating the user's local Windows password cache also can be configured by adding "useLockWstn" = "true" to the config file. Either using **pslocalr.ocx** or **hidgeneric.ocx**. For example,

```
# KVGROUP-V2.0
"" "" = {
  "targetid" "INTERNAL-AD" = {
    "control" "pslocalr" = {
      "protocol" = "2";
      "attributes" "" = {
        "logonDomain" = "OFFICE";
        "useLockWstn" = "true";
      };
    };
  };
};
};
```

2.3.5 Testing

To test the correctness of the configuration file, attempt a password reset for one of the users on that system. If the syntax of the configuration file is invalid, the end user will not see any errors, but the server will log details about the parse error encountered:

```
Failed to parse file [C:\<path-to-instance>\script\cgilocalr.cfg]:
[Line: 36, Pos: 14]: Parse error: expected '=' "
```

See also:

- [Providing HTML to the change passwords pages](#) in the *Reference Manual* for more information about this plugin point.

Part III

LOGIN ASSISTANT (SKA)

Resetting Passwords from a Login Prompt

3

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 provide users with secure access to the *Hitachi ID Bravura Pass* password change interface from the login prompt on their workstations.

This chapter includes:

- Types of secure kiosk account implementation
- Login Assistant software
- What happens when users log in
- Enabling password changes from a login prompt
- Setting up Login Assistant for Remote Users

3.1 Types of secure kiosk account implementation

There are two main methods that you can use to implement a SKA:

- Domain-level account

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 SKA.

- Workstation-level account

A help account is defined on a user's workstation instead of in a network operating system directory such as a Windows domain. The account is added to the *Log on Locally* user rights assignment policy. Users can then log into their workstations with the local ID *help*. Logging into the account launches the SKA.

3.2 Login Assistant software

Login Assistant is composed of:

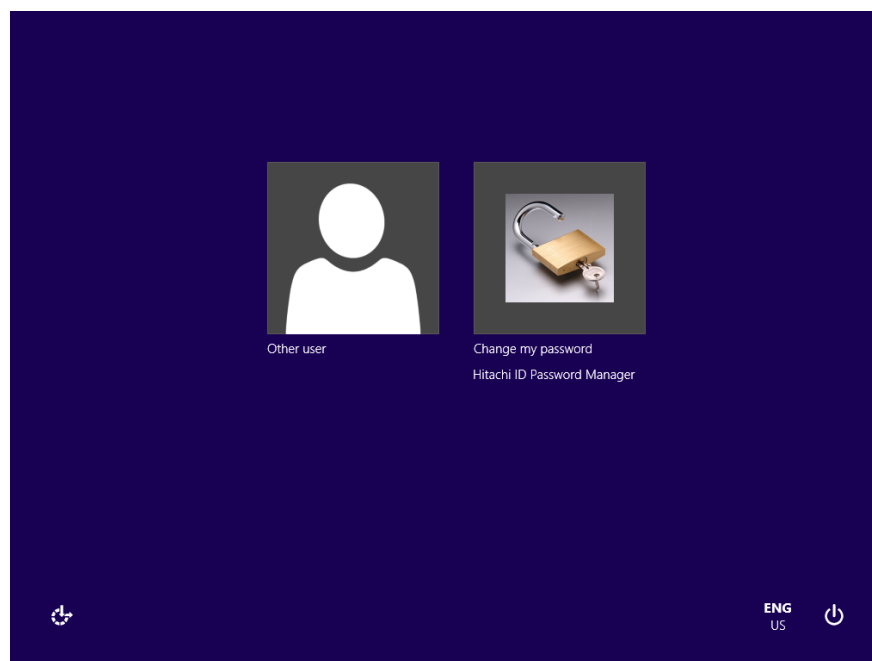
- The secure kiosk account SKA, working with client software (**runurl**)
- Credential Provider extensions for Windows 8 and newer

3.2.1 Credential Provider for Windows

Working with the help account, the *Hitachi ID Bravura Pass* Credential Provider software provides a **Change my password** tile on the Windows login screen.

Clicking the tile logs into the help account, which launches the SKA and allows users to change their passwords and unlock their accounts using *Bravura Pass*. The Credential Provider extension works with both the local and domain-level help account.

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



Security considerations of integrating the Credential Provider tile

When the user clicks on the tile or logs in with the help account, *Login Assistant* starts a web browser with the help account's limited permissions and security profile.

3.2.2 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 Internet service.

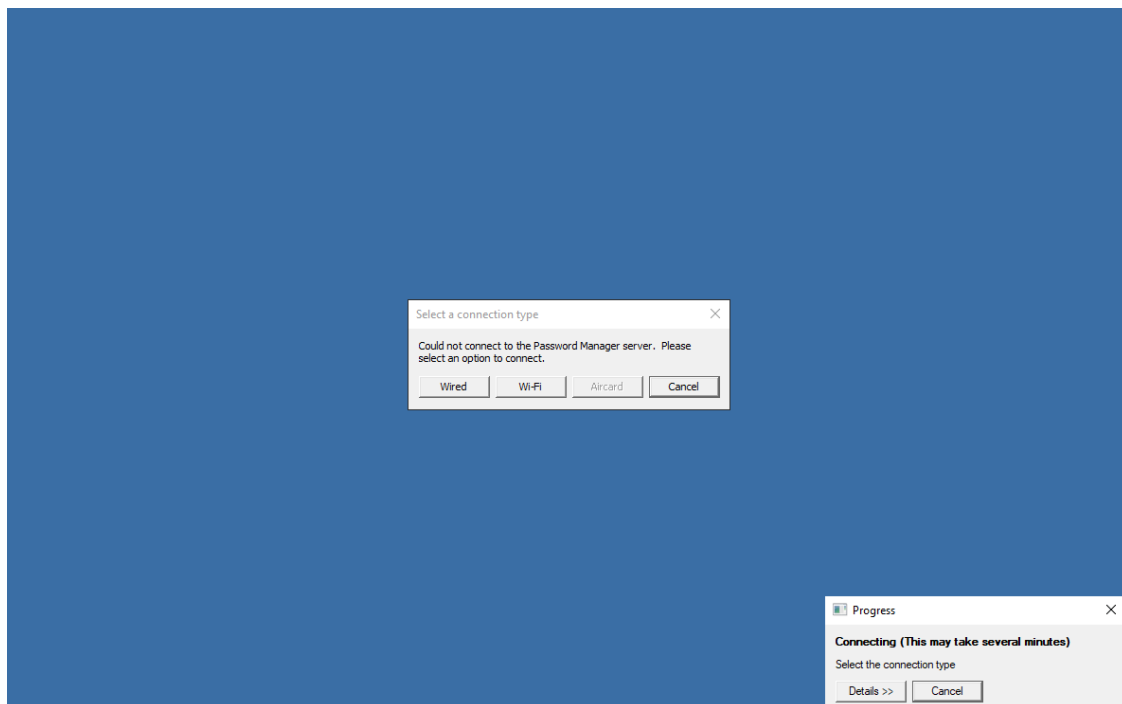
When the *Login Assistant* is run, it can do an immediate check to see if it is connected to the Internet using the external URL and expected data as specified during installation (See [Installing Login Assistant Software on Workstations](#)). If connected, then it immediately works the same as a regular *Login Assistant*.

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

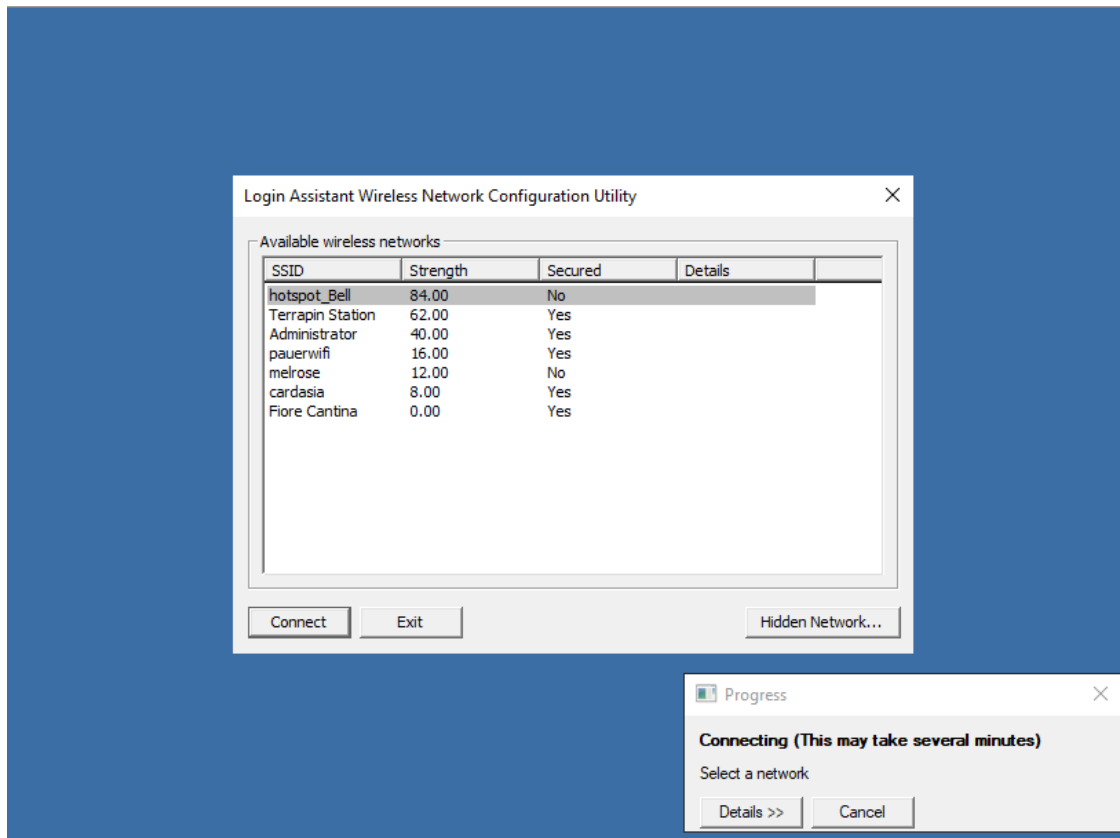
Wired attempt another direct connection

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.

3.3 What happens when users log in

When users log in to their workstations using any of these methods, the `runurl` program is executed. If you are using the domain-level secure kiosk account, this program is loaded from a public network share (typically on the *Hitachi ID Bravura Pass* server, or each logon server's NETLOGON or SYSVOL share).

If you are using a local secure kiosk account this program is loaded from the local workstation.

The program locks down workstations by intercepting certain input event types (keyboard, mouse), and starts a web browser in kiosk mode with the appropriate URL. *Bravura Pass* determines from the URL that the incoming request is for a SKA and displays a special, locked-down skin. Users then authenticate to *Bravura Pass* using security questions or some other authentication method to change their forgotten passwords.

When the *Login Assistant* is launched, the login ID of the domain user that is currently logged into Windows is automatically passed to the URL so that the domain user does not need to retype it in the *Login Assistant*. The login ID is passed to the URL when any of the following occurs:

- The user changes their password by pressing **[Ctrl]+[Alt]+[Del]** and then clicking **Change a Password**.
- The workstation is locked and the user enters an invalid password to log back into Windows, then clicks **OK** to change the password using *Bravura Pass*.
- The user attempts to log into their account when it is locked, then clicks **OK** to unlock the account using *Bravura Pass*.
- The domain user's password is soon to expire or already expired, and the user enters the correct password to log in to Windows and clicks **OK** to change the password.

Note: The soon-to-expire, expired, account-locked and password-change cases are *not* supported by the Credential Provider.

BEST PRACTICE

Access to self-service password reset should be available at the workstation login screen, which means deploying *Login Assistant* to all workstations. If significant numbers of users work off-site and sign into their workstation with cached AD domain credentials, then integrate *Login Assistant* with the corporate VPN, to enable password reset and update of cached credentials when off-site.

Install the Local Rest Extension, which allows *Login Assistant* to cause locally cached passwords to be updated after a successful password reset using the IE web browser (which is what *Login Assistant* will launch).

Use a secure and easy-to-use second authentication factor, such as the mobile Hitachi ID Bravura One App (see [Low cost multi-factor authentication using mobile phones](#)).

3.4 Enabling password changes from a login prompt

This section provides an overview of steps required to enable password changes from a login prompt using *Hitachi ID Bravura Pass*.

3.4.1 Domain-level secure kiosk account

To implement password changes from a login prompt using a domain-level SKA:

1. Create a user named “help” on the Microsoft Active Directory domain. Use a hard-to-guess password and ensure that you:
 - (a) Select the following options:
 - **User cannot change password**
 - **Password never expires**
 - (b) Deselect the following options:
 - **User must change password at next logon**
 - **Account is disabled**
2. 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.
3. Install Credential Provider software on users’ workstations to allow them to access the domain help account.

See [Installing Login Assistant Software on Workstations](#) for details about installing the software.

Alternatively, if you do not want to install software on users’ workstations, you must carry out steps outlined in [Setting up Login Assistant on a Domain \(No Workstation Software\)](#) and educate users to use the help account manually.

3.4.2 Workstation secure kiosk account

To implement password changes from a login prompt, using a workstation-level SKA use the installer for Windows to create the help account and install the required *Login Assistant* software on users’ workstations. The installer package can be executed on the following client operating systems:

- Windows 7 (32-bit or 64-bit)
- Windows 8 (32-bit or 64-bit)
- Windows 8.1 (32-bit or 64-bit)
- Windows 10 (32-bit or 64-bit)

See:

- [Installing Login Assistant Software on Workstations](#) for details about installing the software.
- [Setting up Login Assistant for Remote Users](#) for a common use-case.

BEST PRACTICE

Configure a special VPN account with a static password, which *Login Assistant* will use to connect to the network and update locally-cached passwords when users are off-site.

Presuming that the VPN service you use is capable of this, apply the following limits to this account on the VPN server side:

1. Create a new, dedicated read-only AD domain controller (DC).
2. Configure *Bravura Pass* to always push new AD password resets to this DC along with any others.
3. Configure the VPN user to only be able to access:
 - (a) The IP of this DC (all TCP ports).
 - (b) The HTTPS URL of *Bravura Pass* – typically via a load balancer.
4. Set a connection timeout on the VPN user to 10 minutes.
5. Disable intruder lockouts on the VPN user, to minimize the potential for a denial-of-service attack on user access to self-service.

3.5 Notes on usage

3.5.1 Local password cache

When the *Hitachi ID Bravura Pass* local reset extension (**pslocalr.ocx** (p10)) client tool is *not* installed, a user must manually log out of Windows and then log back in to reset his locally cached password after he uses the SKA to change his password within Windows by pressing **[Ctrl]+[ALT]+[Delete]** and then clicking **Change password**.

If a user uses the SKA to change his password, and the *Bravura Pass* local reset extension (**pslocalr.ocx**) client tool is installed, then he is not required to log out of Windows and then log back in.

See [Configuring ActiveX security](#) for information about ActiveX configuration options to allow the local reset extension to run on the client's workstation Internet Explorer or Edge Legacy browser, and **pslocalr.msi** / **pslocalr-x64.msi** for **pslocalr/nplocalr** installer options.

Installing Login Assistant Software on Workstations

4

This chapter shows you how to install the *Login Assistant* client software and set up the help account on local workstations. Before you start, read [Resetting Passwords from a Login Prompt](#).

Hitachi ID Bravura Pass provides installer packages, to create the help account and install the required software on users' workstations, for:

- Windows client workstations version 7 and newer (`ska.msi`, or `ska-x64.msi` for 64-bit systems)

Note: You cannot install *Login Assistant* on a Domain Controller. The installer will abort safely if a DC is detected.

See [Windows](#).

4.1 Windows

4.1.1 Requirements

- In order to create the help accounts and install the software on Windows workstations, you must launch the appropriate Windows Installer package using elevated privileges.

Note: If you need to launch the Windows Installer package from an account without the necessary elevated privileges, you can specify a privileged administrative account to perform the installation using the `ADMIN_USERNAME` and `ADMIN_PASSWORD` installation options (see [Properties](#)).

- Ensure that Internet Explorer 9 or newer is installed on each workstation.
- Ensure that the CleanupPolicy GPO ("Delete user profiles older than a specified number of days on system restart") is disabled before installing *Login Assistant*. This policy is incompatible with the use of the secure kiosk account.
- If users must use a domain help account, rather than a local workstation account, ensure that you set up the domain account according to [Domain-level secure kiosk account](#).

CAUTION: Before installation on a Windows workstation, you *must* assign the “SeBackupPrivilege” to the Windows Installer service.

On a Windows 7 or Vista workstation, execute **MsiServerCfg.vbs** from the command line under administrative privileges. The script is located in the `addon\login assistant\win\` directory. Alternatively, install the following Microsoft hotfix:

<http://support.microsoft.com/kb/2514642>

If “SeBackupPrivilege” is *not* assigned, the installer provides the warning message: “Failed to load profile for user help: A required privilege is not held by the client.”

Note: If you are using a Cisco anyConnect VPN connection, there are additional settings that can only be set by running the MSI on the command line. See [Command-line Cisco anyConnect VPN parameters](#).

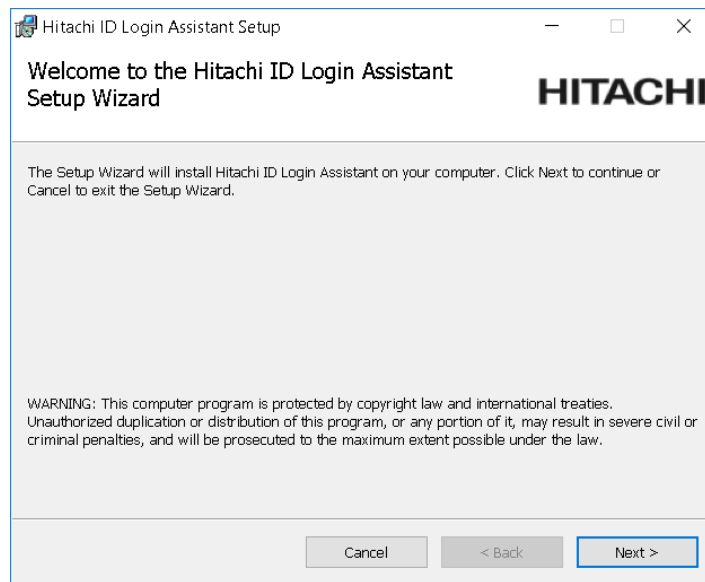
4.1.2 Running the installer

This subsection 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.
- [ska.msi / ska-x64.msi](#) for *Login Assistant* installation options.
- [Add-on Installers](#) in the *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**.

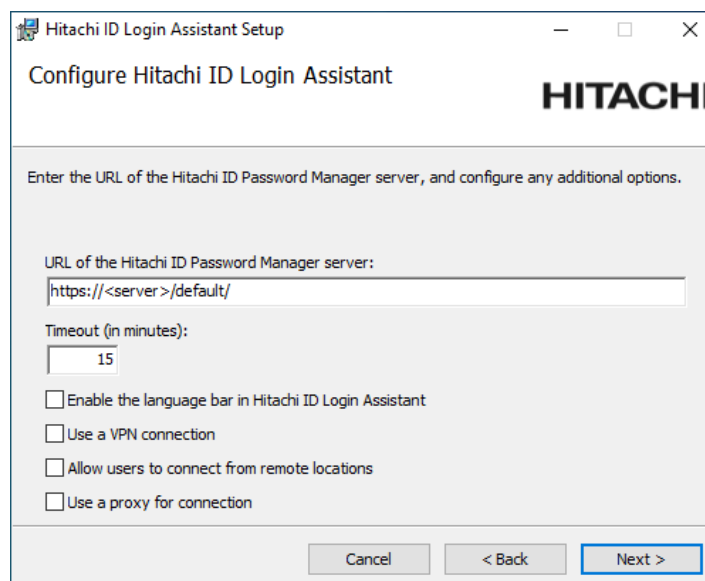
3. Read and accept the license agreement.

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:

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

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

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

Disconnection 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 `runur1` program should wait before checking to see if connectivity has been established after the VPN connect program has run. Default value is 30.

Retries Number of times to test for connectivity after the VPN connect program has run. If this value is blank, there will only be one retry attempt. Default value is 3.

Click **Next**.

Note: If you are using a Cisco anyConnect VPN connection, there are additional settings that can only be set by running the MSI on the command line. See [Command-line Cisco anyConnect VPN parameters](#).

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 NCSE`.

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.

Captive portal time limit (seconds) Specify the length of time to wait to see if a connection has been established by the captive portal used to create a connection.

The time limit may be set between 0 and 600 seconds. The default is 300.

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.

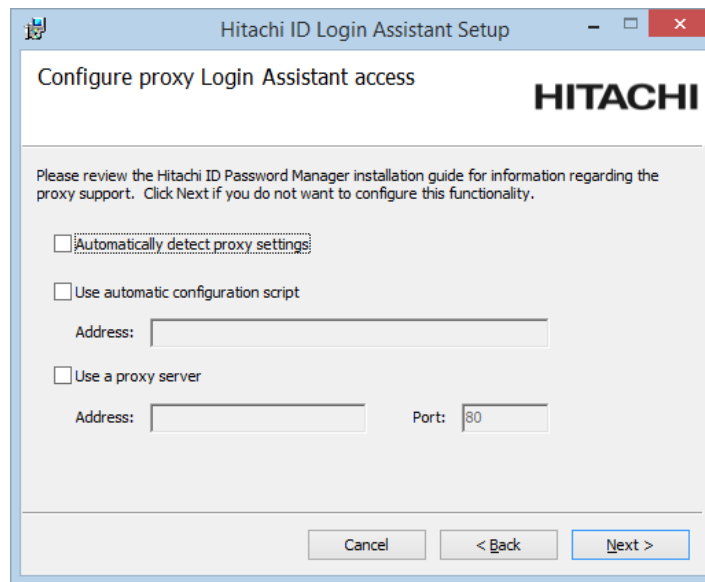
Click **Next**

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".

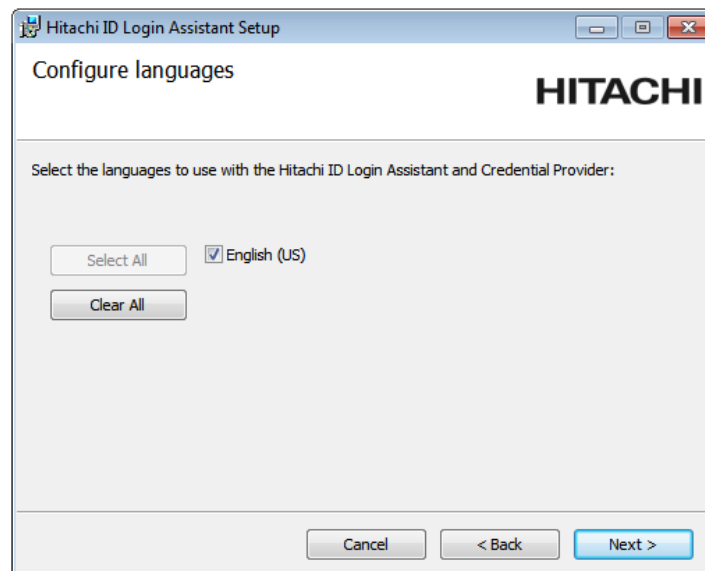
Use automatic configuration script Sets the proxy server to use "Use automatic configuration script".

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**.

i

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.

4.1.3 Command-line Cisco anyConnect VPN parameters

If you are using a Cisco anyConnect VPN connection, the following additional settings that can only be set by running the MSI on the command line:

VPN_CONNECT_STDINPUT is a [~] separated list of lines that go to standard input. The value is written as a registry entry with multi-string value called **vpn-connect-stdin**. It does not allow for empty lines as the registry value type does not either.

Run **vpnccli.exe** manually and interactively to determine what input is needed. Input lines will replace %USERID% with the VPN userid and %PASSWORD% with the VPN password; for example:

```
<vpn profile>
%USERID%
%PASSWORD%
y
```

The *<vpn profile>* should be replaced with VPN connect profile, and the *y* is to accept VPN terms of use. This translates into the following MSI command line parameter:

```
VPN_CONNECT_STDINPUT="profile[~]%USERID%[~]%PASSWORD%[~]y"
```

VPN_CONNECT_TERMINATE is to optionally terminate any running programs before trying to launch the VPN client, as Cisco anyConnect will fail if **vpnccli.exe** or **vpnuui.exe** are running. The value is written as a registry entry called **vpn-connect-terminate**. This is optional but recommended. The value is a comma-separated list of process names; for example:

```
VPN_CONNECT_TERMINATE="vpnccli.exe, vpnuui.exe"
```

VPN_HIDE_WINDOW is used to hide the pop-up console window that **vpnccli.exe** starts. **VPN_CONNECT_TERMINATE** is written as a registry entry called **vpn-hide-window**. By default, it is off, as the showing of the console window is the default behavior and is required for some VPN clients. To disable set:

```
VPN_HIDE_WINDOW = 1
```

For other SKA installer command-line options, see [ska.msi](#) / [ska-x64.msi](#).

4.1.4 Displaying JavaScript Errors

If there are JavaScript errors in the page loaded by the SKA, users do *not* receive error messages by default. The messages may be obscure and confusing during normal operation, but may be useful during troubleshooting.

You can display these messages for users by modifying the appropriate registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi ID\IDM Suite>Login Assistant\HideErrors
```

This setting has a default value of 1, which means JavaScript errors will be hidden. Changing this value to 0 will cause JavaScript errors to be displayed.

WARNING!: Ensure that you are comfortable and knowledgeable in the mechanics of the registry before you attempt to change any configuration settings. Contact support@Hitachi-ID.com if in doubt.

This registry key can also be set using the HIDEERRORS installation option on the command line.

4.1.5 Uninstalling

Upon uninstall, the help account and the associated profile folder will be deleted, but the registry hive still be present, especially if there were options added manually. Before installing another version of *Login Assistant*, check that the:

- Key HKEY_LOCAL_MACHINE\SOFTWARE\Hitachi ID is deleted in the workstation's registry and
- Folder C:\Program Files\Hitachi ID\IDM Suite is deleted from the workstation's file system

4.1.6 Troubleshooting

If you see the following errors when installing the *Login Assistant*:

Failed to open token for user help. Error 1385. Review the group policies on the domain controller to ensure that users can log into a local workstation before and after joining a domain.

Installer service failed to respond. Review the group policies on the domain controller to ensure that users can log into a local workstation before and after joining a domain.

Failed to open token for user help. Error 1314. A required privilege is not held by the client. Ensure that `ska.msi` is run with elevated privileges (see [Using MSI installers](#)).

The system does not allow you to logon interactively Ensure that the help user is able to log in locally. In some situations Windows may apply domain policies upon reboot that cancel this right for local users.

Setting up Login Assistant for Remote Users

5

Consider the scenario where a corporate user is off-site with their corporate-domain laptop. The user is at the Windows login screen and has forgotten their AD domain password, and cannot log in to Windows. A phone call to their corporate help desk would enable the user to have their domain account password reset by the help desk, but unfortunately the user is still off-site (remote) and so the laptop's locally cached credentials cannot be updated with the new password.

As a result, the new network password cannot yet be used by the user to log in to their laptop, and the password reset has not actually helped the remote user in the least.

Laptop users sometimes forget their password while off-site from the corporate network. Without a technical solution, the users' laptops are rendered inoperable until they return to the office. In this scenario, the IT help desk can do nothing to assist.

Hitachi ID Systems' *Self Service, Anywhere (SSA)* solution allows users to securely reset their Active Directory password *and* their locally cached password together, without needing to know the current value. This chapter describes the technologies and configuration required to deploy SSA in this scenario.

5.1 User Experience

In this scenario, the key client-side components are VPN, *Login Assistant* with Credential Provider and the Local Reset Extension (**pslocalx**) software. The Credential Provider creates a password-less login tile – a **Change my password** button – within the Windows 8+ login screen.

A user opens their Windows workstation to the log in screen and realises they have forgotten their password. The user clicks the Credential Provider tile and is automatically logged into the help account. Instead of reaching the Windows desktop, however, a secure, kiosk-mode web browser is loaded. This application allows the user to:

1. Negotiate a corporate network and VPN connection,
2. Connect to the web interface of their organization's instance of *Hitachi ID Bravura Pass* (as a full-screen, non-navigable web page) using *Login Assistant*,
3. Log in to *Bravura Pass* using security question or other authentication,
4. Reset their password, including the locally-cached one using *Local Reset Extension*, and
5. Exit out to the login screen. (This will also tear down any temporary corporate network connections that were established.)

Because the *Password Manager Local Reset Extension* provides the ability to refresh locally-cached passwords during a password reset from the user's workstation, the user is able to log into their Windows workstation immediately and does not need to travel to an on-network location to resynchronize the cached and network password values.

5.2 Technical requirements

To deploy *Login Assistant* in the scenario described above, the following high-level requirements are needed:

- Install and configure *Hitachi ID Bravura Pass* for web-based password management. See the [Bravura Security Fabric Documentation](#) for details.
- Set up VPN infrastructure to support the refresh of locally cached network credentials on Windows workstations:
 - A command-line capable VPN client must be installed on each end-user workstation or laptop that will be used for remote connections.
 - An application-level VPN user account must be provisioned for exclusive use by the *Bravura Pass* client components. (This should normally be distinct from any VPN accounts assigned to individual end-users — see [VPN requirements](#).)
 - One or more VPN endpoints should be setup:
 - * These should be setup in perimeter networks (“DMZs”).
 - * They must honor the above “application-level” VPN user credentials.
 - The VPN endpoint(s) should be configured with network address/port access control list restrictions.
- Allocate/provision a dedicated “site” within Active Directory:
 - One or more read-only domain controllers (RODCs) should be assigned to the AD site mentioned above.
 - * These RODCs will also be deployed in the perimeter network(s) of the VPN endpoint(s).
 - This site will need to include an IP subnet to be defined below.
- Provision an IP subnet which:
 - Is used by the VPN endpoints as the IP address pool(s) offered to connecting VPN clients.
 - Can reach the RODCs mentioned above over the network.
 - Is assigned within the AD to the AD site mentioned above.
 - Can reach either the *Bravura Pass* server or a suitably configured reverse proxy by HTTPS.

Note: The VPN endpoint, IP subnet and associated AD site should be provisioned within a perimeter network (“DMZ”).

- Ensure timely delivery of the new password to the RODC. (See [Password propagation delays between DCs.](#))
- Install the *Login Assistant with Credential Provider* software on remote client laptops and workstations, and configure it to use the locally installed VPN command-line client with specified credentials.

CAUTION: On Windows 7 and Vista systems, installation of the Credential Provider software may fail unless the *Windows Installer* service has the “SeBackupPrivilege” right.

On a Windows 7 or Vista workstation, execute **MsiServerCfg.vbs** from the command line under administrative privileges. The script is located in the `addon\login assistant\win\` directory. Alternatively, install the following Microsoft hotfix:

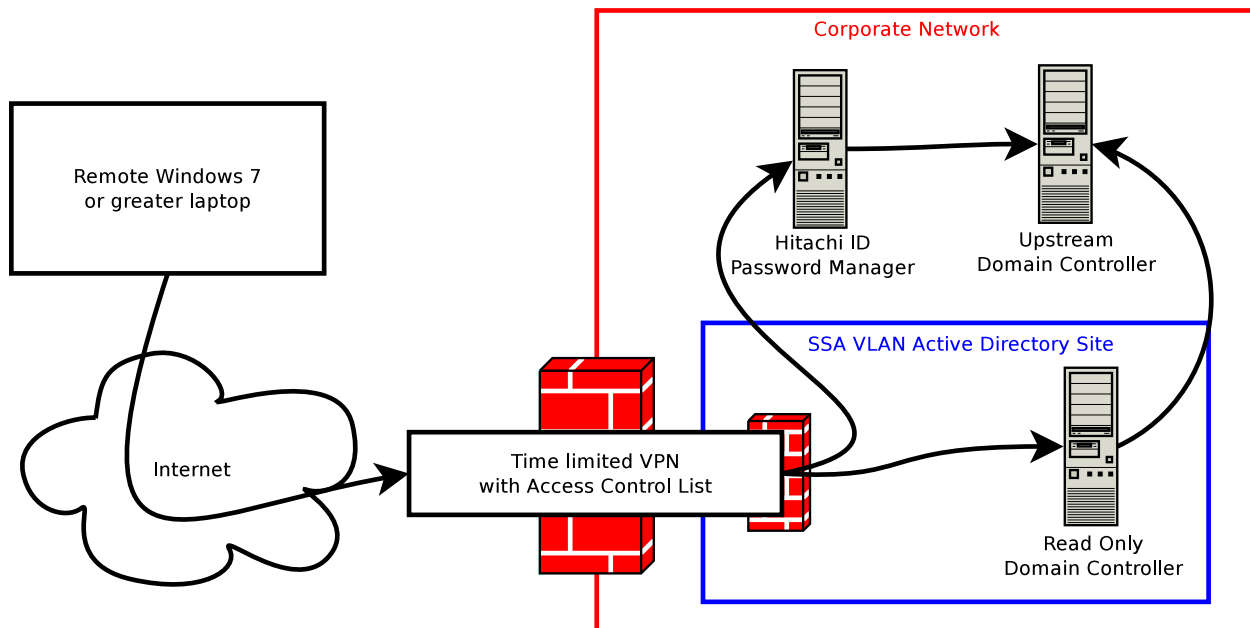
<http://support.microsoft.com/kb/2514642>

On newer Windows systems, the installer can assign the “SeBackupPrivilege” when it is run with elevated privileges.

- Either install the *Bravura Pass Local Reset Extension* (pslocalr) on remote client workstations/laptops, or set it up for remote execution from the *Bravura Pass* server. (For more information see [Resetting cached credentials.](#))

Note: Downloading the ActiveX control over a very slow line (eg. hotel rooms) may take a minute or more, making pre-installation attractive.

Network architecture diagram



5.2.1 VPN requirements

A VPN connection is required during the credential refresh phase, where the Local Reset Extension updates the local Windows credential cache with the end user's new AD password. If no VPN is available, then attempts to refresh the locally cached AD credentials will fail, and the user will still be locked out of their laptop.

Hitachi ID Systems only tests the **Cisco AnyConnect VPN client** with product feature integrations. It is the only officially supported VPN client integration with Hitachi ID Systems products. Other VPN clients may work, but Hitachi ID Systems does not test or officially support them.

As the user's personal VPN credentials may include the forgotten password, VPN authentication for Self Service, Anywhere (SSA) cannot include this password. There are two alternatives for SSA VPN authentication:

1. Authenticate the VPN using the end-user's pre-existing OTP credential. For example, RSA SecurID or similar. There is less need to restrict VPN network access in this case.
2. Use a static password known to the credential provider software, but not to any human. Connections made using this password should be severely restricted. There may be one password per device, one shared password for all devices, or one password per group of devices.

To function with Credential Provider, it must be possible to start and stop this VPN connection using a command-line program. When the OTP method is implemented, the VPN command-line connect command must launch an interface where the OTP can be manually input by the end user. On the other hand, if using static credentials, the Credential Provider supports dynamically substituting two values — a "username" and a "password" — into the connect and disconnect command lines. Where used, these values are stored encrypted within the Windows registry.

The VPN endpoints must also be configured to issue IP addresses to the connecting systems from a dedicated pool of IP addresses. This is needed as a part of a larger mechanism that will ensure that connecting VPN clients use the correct AD domain controllers.

If using a static password for the VPN credential, then VPN connections should terminate in a perimeter network ("DMZ") rather than the main, corporate network.

5.2.2 Active Directory requirements

Some Active Directory configuration is required for SSA to function properly. As a result, it is necessary to take steps to ensure that connecting SSA clients will use one of the specially-configured DCs for their login server.

- A dedicated AD "site" must be provisioned.
- The IP subnets from which the VPN clients will be assigned addresses must also be assigned to this site within AD.
- One or more domain controllers must be provisioned, and assigned to the dedicated site. These domain controllers should be *read-only* domain controllers.

- All DCs in the dedicated site must be configured to use a fixed TCP port for NTDS and NetLogon RPC traffic.
- The DCs must be deployed into the same network to which VPN clients connect. This also applies to VPN clients connecting to a perimeter network (“DMZ”).

Note: Architectural considerations for deploying read-only domain controllers into a perimeter network is out of scope for this document. For information on perimeter network AD deployments, see [http://technet.microsoft.com/en-us/library/dd728034\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd728034(v=ws.10).aspx).

Note: Microsoft provides some documentation for how to configure [RPC dynamic port allocation](#) and RPC to use certain ports and how to help secure those ports by using IPsec

Note: Hitachi ID Systems does not believe port filtering is required between an RODC and its upstream, writable DC. Nonetheless, organizations may port filter such traffic at their discretion and responsibility if they wish to do so.

Note: Contact support@Hitachi-ID.com for a more detailed document with a detailed breakdown of implementation tasks.

5.3 Configuration and usage notes

5.3.1 Timeout

When the SKA is launched using the **Change Password** button, it automatically closes after two minutes if no activity takes place on the web page, which is default Windows behavior. The page can also be configured to close after a pre-determined amount of time regardless of activity using the **Timeout** option. In this case, the user is notified 30 seconds before the session is terminated.

Once countdown hits 0 it will wait for 2 minutes before it closes automatically. Clicking OK on the countdown prompt after it reaches 0 closes the SKA page immediately. Clicking OK when the countdown is still running closes the *Login Assistant* page after the remaining amount of time.

5.3.2 Credential provider and the help account

The Credential Provider component uses the help account to login and execute **runur1** to launch the SKA. When the Credential Provider is installed, it is recommended that you configure the help account with a [random password](#) (p33) and that you do not advertise the help account to users. In this setup, the help account should only be used by the Credential Provider component, and users should access *Hitachi ID Bravura Pass* through the Credential Provider.

5.3.3 Connections over VPN

When using a VPN to connect to the instance, **runurl** will search for one of three HTML tags used to uniquely identify the *Hitachi ID Bravura Pass* login page. The tags expected by **runurl** are:

- A hidden `<input>` element with `name="TRANSACTION"` and `value="F_LOGIN"`.
- A hidden `<input>` element with `name="TRANSACTION"` and `value="C_AUTHCHAIN_LOGIN"`.
- A comment containing a GUID that was created specifically for **runurl.exe** to match:

```
<!-- 81A84EBD-2CE5-4794-8341-E1828711FFBC -->
```

If **runurl** cannot identify any of these values, it will default to attempting a reconnection through other means.

Note: When VPN connection credentials is changed, you can use **skauti1** to update the encrypted VPN credential, the help account, and their cached password values kept in registry. This utility does not change the actual underlying password. See **skauti1** for more information.

5.3.4 Logging SKA remote connection failure

When the SKA remote connection fails, debugging information is provided in the SKA progress window which displays on the right bottom corner on the locked-down SKA page. By enabling a registry key called **debugska**, the debugging information also can be captured in a log file which is generated by using **loguti1.exe**. The following example demonstrates how to capture debugging information:

WARNING!: Ensure that you are comfortable and knowledgeable in the mechanics of the registry before you attempt to change any configuration settings. Contact support@Hitachi-ID.com if in doubt.

1. On the workstation where SKA is installed, create an entry in the Login Assistant registry key to enable SKA debug:

```
HKLM\SOFTWARE\Hitachi ID\IDM Suite\Login Assistant\Login Assistant\debugska
```

Entry name	debugska
Value	1
Data type	REG_DWORD

2. Copy the **loguti1** program from the `\<instance>\utils` folder on the instance server to a folder on the workstation where SKA is installed.
3. Run a command like the following to launch **loguti1** to start logging:

```
loguti1 -level 5 -instance "Login Assistant" -logfile log.txt
```

4. Lock the workstation and then go to the user log on windows page.
5. Click on the **Change my password** tile to launch SKA.
6. Click the **details >>** button displaying on the progress window to browse error messages provided when remote connection fails.
7. Exit the SKA page.
8. Log back to the workstation as the user and stop `logutil.exe`.
9. Open the log file.

Debugging information displayed in the progress window should be available in the log file as well.

5.3.5 Password propagation delays between DCs

The Password Manager Local Reset Extension updates locally cached passwords on the end-user's PC by re-authenticating to the domain using the new password. The *Hitachi ID Bravura Pass* server will typically reset the user's password on one domain controller ("DC1"), while the user's PC will attempt to authenticate to another domain controller ("DC2"). This creates a risk that the new password has not yet propagated from DC1 to DC2, or to other "upstream" DCs such as the *PDC Emulator*, before the user's PC attempts re-authentication.

While *Bravura Pass* always issues password resets to Active Directory *before* attempting the cache-refresh authentication, it is still possible for network congestion or other factors to result in the subsequent authentication attempt *failing*.

To mitigate the risk of timing-induced failures, Hitachi ID recommends using *Bravura Pass's sub-host plugin* feature to dynamically control which domain controllers receive password resets. If this is not practical, other mitigation strategies may also be considered:

1. Within *Bravura Pass*, explicitly target one of the DCs in the SSA site, or
2. Use *Bravura Pass* to target the domain (rather than any particular DC), but assign the *Bravura Pass* server's /32 subnet address to the SSA site, or to the best-connected Active Directory site on the network.

5.3.6 Disaster recovery

Enterprises should consider whether remote, end-user password reset scenarios should be part of disaster recovery (DR) planning. If required for DR, then multiple VPN end points should be used, in at least two different regions or physical locations. Furthermore, enterprise Active Directory architects should be consulted on suitable Active Directory site layout changes needed to leverage those end points.

Setting up Login Assistant on a Domain (No Workstation Software)

6

You can set up access to a domain-level SKA by installing Credential Provider software on users' workstations, as outlined in [Enabling password changes from a login prompt](#). Use the steps in this chapter 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 SKA for Microsoft Active Directory:

1. [Create the help user](#) (p47).
2. [Configure the `runurl` program](#) (p47).
3. Create a policy to lock down [Windows workstations](#) (p48).
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](#) (p53).

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

6.1 Creating a help user

To create a *help user* to serve as an 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](#)).

6.2 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 [SKA client: runurl](#) 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.

6.3 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 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.

6.3.1 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

... continued on next page

Policy	Setting
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
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

... continued on next page

Policy	Setting
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

6.3.2 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

... continued on next page

Policy	Setting
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
→ 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

... continued on next page

Policy	Setting
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

6.4 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.

6.4.1 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.

Part IV

INTERACTIVE VOICE RESPONSE SYSTEMS

Integrating with Interactive Voice Response Systems

7

Hitachi ID Bravura Pass integrates with IVR systems to enable users to authenticate and perform self-service from a telephone.

Bravura Pass enables users to:

- Authenticate to the IVR system and [reset their forgotten or expired passwords](#) (p65), unlock their accounts, or manage their RSA SecurID from a telephone.
- Designate a profile/request attribute to use as an [IVR ID](#) (p58) during [touch-tone identification](#) (p58).
To identify themselves, users either enter the telephone keypad translation of alphanumeric IVR IDs, or simply key in numeric IVR IDs.
- Complete IVR question sets used for [touch-tone authentication](#) (p59).
IVR systems with touch-tone authentication identify users by validating numeric data entered on a telephone keypad.
- Reliably register voice print samples for [voice-print authentication](#) (p61).
IVR systems with voice print authentication identify callers by analyzing their *voice print*, and matching it against a record of each registered user.

7.1 Architecture

The network architecture of an integrated *Bravura Pass* / IVR system is illustrated in [Figure 7.1](#).

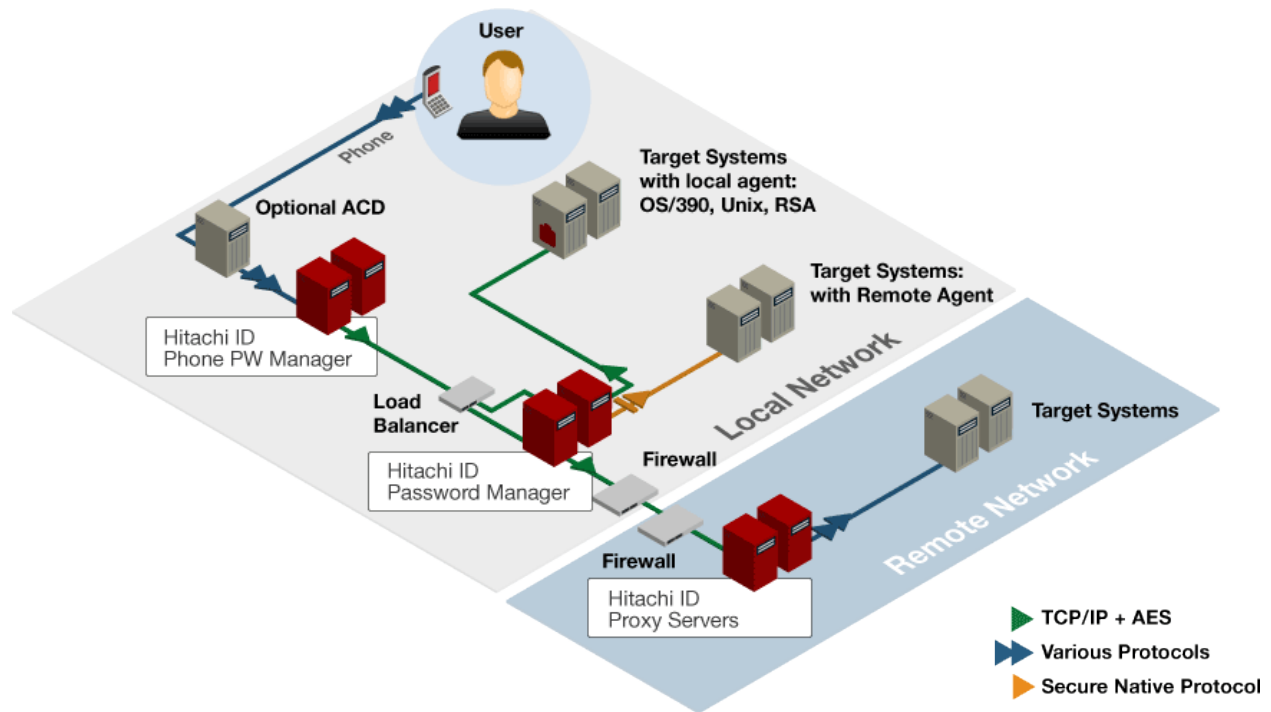


Figure 7.1: Interactive Voice Response integration architecture

See the Phone Password Manager Configuration Guide for more detailed information about how *Hitachi ID Bravura Pass* integrates with IVR systems.

7.2 IVR with touch-tone identification

Users are identified on the network using alphanumeric login IDs. Since most IVR systems do not offer a reliable speech-to-text mechanism, they can only accept numeric input. This presents a challenge for a password reset system: users must enter an alpha-numeric login ID, but the system can only accept a numeric ID.

7.2.1 Assigning unique, numeric IDs

In organizations where each network login ID is already associated with some unique numeric ID, the simple solution is to ask users to log into the IVR system by keying in their numeric ID on the telephone touch pad. Examples of such numeric ID include employee numbers, or home telephone numbers.

Alternately, if a user registration process will be used (e.g., to collect personal security question data for user authentication), then users may be asked to key in or select a new numeric personal identifier. An example might be the user's driver's license number. In this case, users will log into the IVR with their new numeric ID.

7.2.2 Numeric mapping of alphanumeric login IDs

In some cases, numeric IDs are not available. This may happen if there are no existing numeric IDs available for all users, or if what numeric IDs exist are not correlated to network login IDs, or if a registration process is undesirable.

In these cases, users may be asked to log in by pressing the keys on their telephone marked with the letters and numbers of their network login ID. For example, the user smith01 would type 7648401.

Since the digit mapping of two different alpha-numeric login IDs may produce the same number (e.g., poguh01 also maps to 7648401), an IVR system that uses this technique must allow for number collisions, and ask the caller to select the correct ID when the entered number resolves to more than one alpha-numeric login ID.

7.2.3 Selecting an IVR ID source

You can change the profile and request attribute that is used as a source of users' IVR IDs (the digits users enter to identify themselves to the IVR phone system). By default, the telephone keypad translations of users' profile IDs are used as their IVR IDs. *Phone Password Manager* finds a users' profile ID by searching on their "numid" and "altnumid".

The **TPM ID ATTR** option allows you to change the source of IVR IDs by specifying a new profile and request attribute. When **TPM ID ATTR** is in use, *Phone Password Manager* finds users' profile IDs by searching on the specified attribute.

For example:

Using the default setup of profile ID Find user “test123” by entering 8378123 on the keypad. This is the telephone keypad translation of the user’s profile ID.

Using TPM ID ATTR If user “test123” has their “Telephone number” attribute specified as “4035550740”, then set **TPM ID ATTR** to “Telephone number”, and enter 4035550740 on the telephone keypad to find the user.

Note: For the **TPM ID ATTR** option to work as defined above, you must associate the “Telephone” profile/request attribute with the account attribute “telephoneNumber”.

Note: **TPM ID ATTR** requires the specified attribute to only contain numeric characters; it *cannot* contain alphabetic or special characters.

7.3 IVR with touch-tone authentication

IVR systems with touch-tone authentication identify users by validating numeric data entered on a telephone keypad. This includes *Phone Password Manager*.

7.3.1 IVR question sets

A simple process to authenticate users is to ask them to answer one or more security questions with numerical answers. Numerical security questions should have the following characteristics:

- Answers should be private – relatively hard for anyone other than the user to come by.
- Answers should be easy – users should be able to quickly and reliably answer the questions, without having to remember anything new, and with a low likelihood of making mistakes.

Here are a few examples of numerical security questions that meet the above criteria:

- Social Security Number
- Employee number (if this is typically secret)
- Driver’s license number
- Insurance policy number (if printed on a card the user carries with him, or if used often)
- Date of birth (of self or a close family member)
- First or current home telephone number

Since all of these may be acquired by a third party, it makes sense to use more than a single question, to randomize which questions are used for any given authentication session, and to lock out users who repeatedly fail to authenticate.

Note: Using too few numerical security questions, or using data that is too easily acquired by an intruder, has the effect of reducing password strength on the network. [Biometric voice print verification \(p61\)](#) is a stronger technology.

7.3.2 Configuring IVR question sets

You can set up one or more question sets for IVR systems that use touch-tone authentication. Users authenticate over the phone by keying in numerical answers to questions that you define in *Hitachi ID Bravura Pass*.

Ensure that:

- **Ask users to answer questions from this set** is checked.
- **Ask telephone users to answer questions from this set** is checked.
- All of the questions in the question set require all-numeric answers of a fixed length. To do this:

Set the **Minimum length of answers** and **Maximum length of answer** fields to the same value, and set the **Formatted string for answer** field to contain the required number of Ns. For example, set the minimum and maximum number of characters to 5, and write NNNNN as the formatted string.

Note: Users must provide answers for all required questions in the IVR question sets in *Bravura Pass* prior to using the IVR system.

Note: You must record vocals (usually *.wav files) for each of the IVR questions. The IVR system plays these vocals for callers, prompting them to enter their numeric answers.

See [Question Sets](#) for more information about adding question sets.

7.4 IVR with voice print authentication

IVR systems with voice print authentication reliably identify callers by analyzing their *voice print* and matching it against a record of each registered user. This is a simpler and more secure caller authentication process, compared to IVR question sets, but is more costly.

Biometric voice print verification is commercially available, can yield effectively zero false-positive recognitions, and low false-negative failures (approximately 1% to 2% of valid authentication attempts end with a failure to recognize the speaker).

Note: *Voice print verification* is not related to *voice recognition* technology – the former identifies a speaker, while the latter attempts to “understand” what was said. Voice print verification is reliable, fast and independent of language, accent and the common cold.

Organizations deploying voice print verification technology in their IVR infrastructure must acquire voice samples from the entire user population. Each voice print must be securely mapped to the particular user's user IDs in order to allow secure password reset. During registration, users are asked to speak one or more phrases, so that their new response can be compared to their registered sample.

Once authenticated, callers may request secure operations, including a password reset. The IVR system uses *Hitachi ID Bravura Pass* to select a strong password for the caller, and to reset the password on all of the user's accounts to the new selected value.

7.4.1 Registering voice prints

You can use *Hitachi ID Bravura Pass* to facilitate an automated, reliable, secure and effective process to:

- Prompt users to register voice prints.
- Authenticate users prior to registration.
- Map users' voice prints to their system IDs.
- Enable the IVR system to securely capture their voice prints.

You can use *Bravura Pass's Generate voice print enrollment PIN* (PSI) module to reliably register voice print samples for all users. You can use this facility for new IVR deployments or for new users on existing systems.

Without *Bravura Pass*, IVR users are commonly provided with a short PIN via email, and are required to key in the PIN when they first register with the IVR system. This presents a security weakness: PINs are short, guessable, and sent via an insecure media (email).

Bravura Pass's Generate voice print enrollment PIN (PSI) module streamlines and increases the security of the registration process by requiring users to authenticate to receive a longer PIN that is only good for a single use, and expires after a definable period.

A user registers in the following way:

1. The user logs into *Bravura Pass* and navigates to the **Generate voice print enrollment PIN** page.
2. *Bravura Pass* generates a random PIN and displays it to the user. The PIN is good for only one use and expires after a defined number of seconds.
If configured, *Bravura Pass* displays additional information and navigation steps for the phone registration system.
3. The user calls the IVR system, follows the voice prompts, enters the PIN, and registers their voice print.

The *Generate voice print enrollment PIN* (PSI) module is *disabled* by default. You must enable it to allow users to access this feature.

To configure IVR registration:

1. Click **Manage the system** → **Modules** → **Generate voice print enrollment PIN (PSI)**.
2. Turn on the **PSI ENABLED** setting.
3. Configure the variables described in [IVR registration options](#) as required.
4. Click **Update** to submit the changes.

Table 7.1: IVR registration options

Option	Description
PSI RANDOM DIGITS	The number of random digits to follow the 2 digit idpm server number in generated PINs. This value must be between 4 and 14. The default value is 4. (required)
PSI RANDOM EXPIRY	The time (in seconds) before the random number generated is expired. The default value is 600.

See also:

- [Enforced enrollment](#) to learn how to prompt and enforce user registration.
- [Controlling the Phone Password Manager source of IVR IDs](#) to learn how to change the source of IVR IDs.
- [vputil](#) in the *Reference Manual* to learn how to remove voice print enrollment data.

7.5 Implementation Options

Self-service password reset, self-service RSA SecurID token management and automated registration of biometric voice print samples can all be implemented by integrating *Hitachi ID Bravura Pass* with an IVR system.

Bravura Pass licensees may choose to purchase a dedicated IVR system from Hitachi ID Systems, specifically for these applications, or to extend an existing IVR system to include new call logic. Integration is available for every kind of existing IVR system, through multiple language and platform bindings of a powerful *Bravura Pass* API.

User identification can be implemented using speech-to-text technology, or user input of unique numeric identifiers or numeric-mapped network login IDs.

User authentication can be implemented using either text prompts for personal information, followed by touch-tone input of responses, or using biometric voice print verification technology.

System integration for a telephony-enabled password management system can range from one or two days of effort to activate a turn-key, touch-tone enabled IVR system up to two or three weeks to extend an existing biometric system.

7.5.1 Buying a new IVR system vs. extending an existing system

Hitachi ID Systems offers two options to customers who wish to enable telephone access to *Hitachi ID Bravura Pass*:

1. Purchase a turn-key IVR system, designed specifically for authenticating callers and providing self-service password resets, from Hitachi ID Systems.

Turn-key system options are described in [Turn-key IVR options offered by Hitachi ID Systems](#).

If an existing Automatic Call Direction (ACD) system is in place, then it must be configured to forward relevant calls to the *Bravura Pass* IVR system.

2. Extend the existing IVR system to provide front end password reset functionality (and potentially, biometric voice print authentication) using *Bravura Pass* as a “back end” to provide user authentication and general password management services.

In this case, the call flow logic on the existing IVR system is modified to prompt the user for identification and authentication information. The IVR is programmed to verify user authentication by calling either:

- (a) *Bravura Pass* (if using keypad PIN authentication), or
- (b) an external voice print biometric system (if using voice prints) implemented by the customer (eg. Nuance, Speechworks).

Once the IVR has authenticated the user, it can make calls to the *Bravura Pass* server to request various password reset services.

Bravura Pass can be integrated with almost any existing IVR system, as described in the Connector Pack Integration Guide.

The software required to integrate *Bravura Pass* with any existing IVR system is included at no additional charge. Particular IVR systems may also require software extensions as available from the IVR vendor; for example, XML over HTTPS.

7.5.2 Turn-key IVR options offered by Hitachi ID Systems

Hitachi ID Systems offers a turn-key IVR option, *Phone Password Manager*, which uses touch-tone caller authentication, and leverages the Web-based *Hitachi ID Bravura Pass* registration process to build user profiles for numeric security question authentication. This solution is tightly integrated with *Bravura Pass*, using the secure API described in the Phone Password Manager Configuration Guide.

Note: *Bravura Pass* has an open interface specification, which allows other IVR biometric voice print authentication systems, such as Vocent, to leverage *Bravura Pass* for general enterprise password management.

See the Phone Password Manager Configuration Guide to learn how to set up *Bravura Pass* to work with the *Phone Password Manager* and voice print authentication systems such as Vocent.

7.5.3 Leveraging an existing authentication process

Organizations with an existing IVR system may choose to continue to use an existing caller authentication process, or to strengthen it prior to activating self-service password reset.

The existing identification and authentication process may have to be replaced because it is not secure enough and would weaken password security if it enables self-service password reset.

7.6 Managing RSA SecurID tokens from a telephone

Users who log into the network, or a remote access service, using a hardware token (most likely an RSA SecurID token) may experience problems and require service.

Possible SecurID token problems include users forgetting their PINs, losing their tokens, or users whose token clocks have drifted significantly away from the time reference on the RSA Authentication Manager server.

These users may require service before accessing the network, so a telephony solution is desirable.

7.7 Password resets from a telephone




Allowing users who have experienced a password problem to access self-service from a telephone to resolve their own problem is advantageous for several reasons:

- It allows users who forgot their initial network login password to resolve their own problem without any special measure to make this available from the workstation login prompt.
- It allows users who forgot their remote access (RAS or VPN) password to access self-service problem resolution without first connecting to the network.
- It encourages the use of self-service password reset in organizations where users are accustomed to getting service primarily with a telephone.

Since user authentication, password generation and password resets are all processed by the *Hitachi ID Bravura Pass* server, the process automatically benefits from *Bravura Pass*'s auto discovery process, user profiles, password policy engine, email integration and call tracking system integration.

7.7.1 Enabling password resets from a telephone

To enable IVR users to authenticate and reset their own forgotten or locked-out passwords from a telephone:

1. Set up the appropriate authentication method for your IVR system:
 - If your IVR system uses voice print authentication to identify users, enable the *Generate voice print enrollment PIN* (PSI) module.
Users log into the *Generate voice print enrollment PIN* (PSI) module to obtain a temporary PIN, allowing them to securely register biometric voice samples.
See [Generate voice print enrollment PIN \(PSI\)](#).
 - If your IVR system uses touch-tone authentication, configure an [IVR question set](#) (p60).
Users log into the *Update security questions* (PSQ) module to register security question information that is used by the IVR system to authenticate users.
2. Enable and start the `idapi` service on the *Hitachi ID Bravura Pass* server:
 - (a) Click **Manage the system** → **Maintenance** → **Services**, then select  the **Hitachi ID Systems (idapi) API Service**.
 - (b) Select  **Enable the service**.
 - (c) Select  **Start the service**.
3. Integrate your system with *Bravura Pass* using the PASSWORD MANAGER REMOTE API.
4. Encourage users to register to use the IVR system, either by submitting a voice sample or by answering questions in the IVR question set.
See [Enforced enrollment](#) to learn how to prompt and enforce user registration.

See also:

- The *Bravura Security Fabric* Remote API guide includes configuration details for connecting to the *Hitachi ID Bravura Pass* API.
- The Phone Password Manager Configuration Guide details Hitachi ID Systems's integrated *Bravura Pass*/IVR solution — *Phone Password Manager*.

Part V

ENCRYPTED SYSTEMS

Unlocking encrypted systems via the *Bravura Pass* web interface

8

Users with access to *Hitachi ID Bravura Pass*'s web interface can recover an encrypted system through the *Unlock encrypted systems/accounts* (HDD) module.

If they have forgotten their password, they can access *Bravura Pass* using another form of authentication. This can be another password on a trusted system, security questions, a hardware token (for example, SecurID, SafeWord), or some other means.

Once logged in, the user clicks **Unlock encrypted systems/accounts** to access the *Unlock encrypted systems/accounts* (HDD) module, which will provide them with instructions on how to acquire a challenge code for the system, if required. The relevant connector will use this challenge code to generate a response code that can be used to unlock the encrypted device.

Once users have regained access to the locked system, it is recommended that they change the encryption key, if this functionality is not already provided through the *Bravura Pass*.

Hard drive encryption system connectors use a default inputmask for its challenge and response codes. These connectors include McAfee Drive Encryption (**agtmcee6**), Sophos Safeguard Enterprise Server (**agtsge**), Bitlocker Hard Drive Encryption (**agtbilocker**), Check Point Endpoint Security (**agtchkpt**), and PGP Whole Disk Encryption Platform (**agtpgwde**).

Generally, the code format will be structured in the same way as displayed in the pre-boot screen of the hard drive encryption system.

To configure options for the *Unlock encrypted systems/accounts* (HDD) module:

1. Click **Manage the system** → **Modules** → **Unlock encrypted systems/accounts** (HDD).
2. Configure the options in [Table 8.1](#) as required.
3. Click **Update** to submit the changes.

Table 8.1: Modules → Unlock encrypted systems/accounts HDD options

Options	Description
HDD CHALLENGE FORMAT	Specify a format for the challenge code string. See Overriding the string format for challenge/response codes in the Bravura Security Fabric Documentation for more information.
HDD ENABLED	Enable/disable the HDD module. This is enabled by default.
HDD RESPONSE FORMAT	Specify a format for the response code string. See Overriding the string format for challenge/response codes in the Bravura Security Fabric Documentation for more information.

8.1 Overriding the string format for challenge/response codes

You can override a challenge/response code string format to fine-tune how the challenge and response codes will be presented to the user.

Challenge code string formats are defined using **HDD CHALLENGE FORMAT**, and response code string formats are defined using **HDD RESPONSE FORMAT**.

To override a challenge code string format:

1. Click **Manage the system** → **Modules** → **Unlock encrypted systems/accounts (HDD)**.
2. Define a challenge code string format for **HDD CHALLENGE FORMAT**.
3. Click **Update**.

To override a response code string format:

1. Click **Manage the system** → **Modules** → **Unlock encrypted systems/accounts (HDD)**.
2. Define a response code string format for **HDD RESPONSE FORMAT**.
3. Click **Update**.

Note: If you choose to manually define a challenge or response code string format, it will be presented the same way for all hard drive encryption systems.

Special formatting characters are used to determine what the expected input/output will be. These characters are:

- 9 - Any numeric character.
- a - Any alphabetic character.
- * - Any alphanumeric character.
- A - Any alphabetic character. The character will be converted to uppercase.
- & - Any alphanumeric character. All alphabetic characters will be converted to uppercase.
- n - Adds a new line. This is only supported in **HDD RESPONSE FORMAT**.

Other characters are used to define optional characters or limit the number of characters a string can have:

- [] - Any characters enclosed in square brackets will be treated as optional characters. This can only be defined once per challenge or response code, and at the end of a format string.
- _{M,N} - A boundary condition in which the recovery string contains a variable number of characters. This can only be defined once per challenge or response code, and at the end of a format string.
_ denotes the special formatting character, M denotes the minimum number of characters that can be entered, and N denotes the maximum number of characters that can be entered.

All other characters will be treated as literals, with the exception of lower-case d, h m s, and y.

8.1.1 Examples

1. To set a fixed string format for challenge codes, consisting of 20 numeric characters grouped in 4, and separated with spaces:

```
HDD CHALLENGE FORMAT = 9999 9999 9999 9999 9999
```

An accepted challenge code would be:

```
2356 7217 2340 3992 6671
```

2. To limit user input to 10-20 alphanumeric characters:

```
HDD CHALLENGE FORMAT = *{10,20}
```

An accepted challenge code would be:

```
a6S8k7H6f1J1b2
```

3. To provide additional input for an optional 5 characters to a fixed string format for challenge codes, consisting of 20 alphanumeric characters with alphabetic characters converted to upper case, grouped in 5 and separated with spaces:

```
HDD CHALLENGE FORMAT = &&&&& &&&&& &&&&& &&&&& [&&&&&]
```

Accepted challenge codes would be:

```
6S9C1 7N6K2 T0I4W 9M3Q1 2Y6C5
```

or

```
7H2H5 J1R2I 2G2AI 6H4CS
```

4. To set a fixed string format for response codes, consisting of 30 alphanumeric characters with alphabetic characters converted to upper case, grouped in 5, and separated with spaces:

```
HDD RESPONSE FORMAT = &&&&& &&&&& &&&&& &&&&& &&&&& &&&&&
```

An accepted response code would be presented as:

```
A6S8S 9S7U6 Y6C4U 5H7Y7 T5S6G 3Z2SB
```

5. To add a line to a response code, using the previous example:

```
HDD RESPONSE FORMAT = &&&&& &&&&& &&&&&n &&&&& &&&&& &&&&&
```

An accepted response code would be presented as:

```
A6S8S 9S7U6 Y6C4U
5H7Y7 T5S6G 3Z2SB
```

6. To provision between 1-5 numeric characters at the end of a response code:

```
HDD RESPONSE FORMAT = 99999 99999 99999{1,5}
```

Accepted response codes would be:

```
23499 63724 60761
```

or

```
45789 23476 98892342
```

See also:

- For information about integrating with hard drive encryption systems, see the Connector Pack Integration Guide.

Appendices

Installing Add-on Software

A

This chapter describes Hitachi ID Systems add-on software that can be installed on external servers or client workstations. Files for add-on software are loaded onto the *Hitachi ID Bravura Pass* server, in the `addon` directory, when you install the core software.

In some cases the software is installed using an MSI installer. This chapter also provides general instructions for using the installers manually, or by setting a global policy for unattended installation.

Note: All of Hitachi ID Systems's *.exe, *.ocx, *.dll, and *.msi files are digitally signed.

A.1 Using MSI installers

This section provides general information about using MSI installers to install Hitachi ID Systems add-on software:

- [Manually](#) (p74)
- [Automatically, using a group policy](#) (p74).

A.1.1 Requirements

In order to create required accounts and install software on Windows workstations, you must launch the MSI installer using elevated privileges. The client workstation must have Windows Server 2008/Windows 7 or later installed.

Note: Support for earlier operating systems is available upon request. Contact support@Hitachi-ID.com for additional assistance.

To enable the MSI installer to run with elevated privileges, create a local computer policy with the following privileges enabled:

- Computer Configuration → Administrative Templates → Windows Components → Windows Installer → **Always install with elevated privileges**
- User Configuration → Administrative Templates → Windows Components → Windows Installer → **Always install with elevated privileges**

If you want the installer package to install automatically, with no end-user interaction, you must set installation options by applying a Windows Installer Transform file (.mst), or by editing the installer package directly. If you are not sure how to do this, contact support@Hitachi-ID.com.

A.1.2 Manual installation

To manually install add-on software, you can launch the appropriate MSI installer either by double-clicking the file or by using the Windows `msiexec.exe` command-line utility. You then proceed through a series of graphical user interface (GUI) pages to specify options for installation. An easier way to record installer choices that you provide in the GUI, and even some settings not available in the GUI, is to run the MSI from the command line, with the options described in [Add-on Installers](#) in the *Reference Manual*. See your Windows help for more information about Windows Installer technologies.

A.1.3 Customizing an MSI

You can customize an add-on MSI installer by modifying it with an MSI editor such as Orca. Orca is a table editing tool that can be used to edit .msi files. Information on how to use Orca and where to download it can be found at <https://docs.microsoft.com/en-us/windows/desktop/msi/orca-exe>. Properties can also be specified on the command-line or in a Windows Installer Transform file.

A.1.4 Automatic installation using a group policy

With a Windows group policy, you can easily deploy a Hitachi ID Systems MSI to a group of users or computers. If you set options for installation, such as the URL to the *Bravura Pass* server, before deploying the software, no end-user input is required.

Note: Contact your Windows system administrator or Windows documentation for more information about using Windows Installer technologies.

For information about installer command-line options, visit:

```
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/  
command\_line\_options.asp
```

The following steps outline the general procedure for configuring a group policy to deploy an installer package to computers in a domain (see your Windows help for more information). You must perform these steps using administrator privileges:

Note: The following steps are for Active Directory 2012R2, installed on Windows Server 2012R2. Details may vary depending on your version of Windows.

1. Log into a domain controller.

2. Copy the installer package and any transform files you have created to a shared folder with access granted to all target machines.
3. Launch Server Manager.
4. Click **Tools** → **Group Policy Management**.
5. If necessary, create a new group policy. To do this, right click on the container where you wish to create the group policy; for example, the container in which the computers reside.
6. Select **Create a GPO in this domain, and Link it here...**, and type a unique name for the policy. For example, `IDM Suite software policy`.
7. Click **OK**.
8. Ensure the group policy is applied only to the appropriate users, computers, or groups:
 - (a) On the left hand side, select the policy you just created. You may need to expand the tree before you can view the new policy.
 - (b) Select the **Delegation** tab.
 - (c) Click the **Advanced...** button.
 - (d) Select the Authenticated Users group.

Under the permissions for this group, clear the **Allow** checkbox for the **Apply Group Policy** permission.
 - (e) Click **Add**, type name of the users, computers, or groups to add, then click **OK**.
 - (f) Select each user, computer, or group for which you want to apply the group policy. Under the permissions for this object, select the **Allow** checkbox for the **Apply Group Policy** permission.
 - (g) Click **OK** to return to the **Group Policy Management** snap-in.
9. Select the group policy you want to modify, then click **Edit...**

The **Group Policy Management Editor** snap-in displays.
10. Expand **Computer Configuration** → **Policies** → **Software Settings**.
11. Right-click **Software installation** and select **New** → **Package...**

The **Open** dialog box appears.
12. Browse to the shared folder (UNC path) where you copied the MSI, select the file, then click **Open**.

The **Deploy Software** dialog appears.
13. Choose **Advanced**, then click **OK**.

The properties dialog for the package appears.
14. Select the **Modifications** tab. Click **Add**. In the Open dialog box, browse to the transform file (`.mst`), then click **Open**.

15. Click **OK**.

The package is assigned immediately. The installation is performed when it is safe to do so, typically when the computer starts up.

16. Close the **Group Policy Management Editor** and the **Group Policy Management** snap-in.

A.2 Enabling logging

You can use the `logutil` program to enable logging, for debugging purposes, for add-on software. To do so:

1. Copy the `logutil` program, located in the `util` directory on the *Hitachi ID Bravura Pass* server, to the server hosting the add-on tools. It can be placed anywhere on the server.
2. Open a command prompt and invoke `logutil` with:

```
logutil -makekey -instance <instance> -level <loglevel>
```

Note: The `-makekey` option needs to be run once only, to generate an instance name and required registry entries.

A.3 Configuring ActiveX security

For an ActiveX control to be downloaded and executed by a Internet Explorer or Edge Legacy, the browser must identify and authenticate the ActiveX control, or be configured with a lower security setting to accept unsigned controls (not recommended).

Note: These settings are not required for Edge Chromium, Google Chrome or Firefox.

To allow *Bravura Pass* users' web browsers to safely accept trusted ActiveX controls, your company can obtain and implement a Certificate that enables web servers and users to establish your identity before making a sensitive transaction. Alternatively, you may choose to have the ActiveX control "signed" by a trusted third-party organization. For more information on Certificates and ActiveX registration, consult your web server documentation, web browser documentation, or on-line authority.

It is recommended that the website for the *Hitachi ID Bravura Pass* server be added to the Trusted Site or Local Intranet zone in Internet Explorer.

A.3.1 Configuring internet options on a workstation

To configure internet options on a workstation:

1. Open Internet Explorer.
2. From the **Tools** → **Internet Options** → **Security** tab, choose the **Trusted sites** or **Local intranet** zone.
3. Click **Custom level**.
4. Ensure that the following ActiveX controls are *enabled*:
 - **Download signed ActiveX controls**
 - **Automatic prompting for ActiveX controls**
 - **Run ActiveX controls and plugins**
 - **Script ActiveX controls marked safe for scripting**
5. Click **Sites** to add the web site for the *Bravura Pass* web server as a trusted site or local intranet site.

A.3.1.1 Troubleshooting

- If you are prompted with a message to allow/disallow an add-on, try resetting your Internet Explorer security options to default before re-configuring your internet options. Alternatively, selecting allow will refresh the page and require you to login again, but this is only required once for each add-on/plugin.

A.3.2 Using GPOs to globally configure Internet Explorer/ActiveX security settings

You can use Group Policy Objects (GPOs) to globally configure Internet Explorer/ActiveX security settings. To do this:

1. Put the *Hitachi ID Bravura Pass* server in the approved installation sites list, and allow sites to run ActiveX controls.
See [Allowing approved installation sites to run ActiveX controls](#).
2. Put the *Bravura Pass* server in the trusted security zone, and allow trusted sites to run ActiveX controls.
See [Allowing trusted sites to run ActiveX controls](#).
3. Enable automatic download and installation of ActiveX controls provided by trusted sites.
See [Enabling automatic download and installation](#).

A.3.2.1 Allowing approved installation sites to run ActiveX controls

The following are instructions for Windows 8:

1. Open *Microsoft Management Console* by running `mmc.exe`.
2. Select **File** → **Add/Remove Snap-in...**
3. Select **Group Policy Object...**
4. Click **Add**.
5. In the **Select Group Policy Object** window, browse for a **Group Policy Object** or click **Finish** to accept the default.
6. Click **OK**.
7. In the tree, navigate to **Console Root** → **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **ActiveX Installer Service**.
8. In the right panel, right-click on **Approved Installation Sites for ActiveX Controls** and select **Edit**.
9. Select **Enabled**.
10. Under **Options**, click **Show...**
11. Under **Value name**, enter the server IP address.
12. Under **Value**, enter custom settings or leave blank for default.
13. Click **OK**.
14. Click **OK**.
15. Close *Microsoft Management Console*.

A.3.2.2 Allowing trusted sites to run ActiveX controls

The following are instructions for Active Directory 2008:

1. Open *Microsoft Management Console* by running `mmc.exe`.
2. Select **File** → **Add/Remove Snap-in...**
3. Select **Group Policy Management Editor** for AD 2008.
4. Click **Add**.
5. In the **Select Group Policy Object** window, browse for a **Group Policy Object** or click **Finish** to accept the default.
6. Click **OK**.
7. In the tree, navigate to **Console Root** → **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Internet Explorer** → **Internet Control Panel** → **Security Page**.

8. In the right panel, double-click to view **Site to Zone Assignment List** properties.
9. Select **Enabled**.
10. Under **Options**, click **Show...**
11. Click **Add ...**
12. Enter a name of the item to be added that matches what was specified as the server address for the *Hitachi ID Bravura Pass* server when the add-on software was installed on workstations; for example, an IP address or DNS name for the server.
13. Enter a value of the item to be added.
This can vary depending on your organization. There are four zones that may be specified:
 - 1 – Intranet zone – sites on your local network
 - 2 – Trusted Sites zone – sites that have been added to your trusted sites
 - 3 – Internet zone – sites that are on the Internet
 - 4 – Restricted Sites zone – sites that have been specifically added to your restricted sites.
 The recommended zone to specify is 2 for the Trusted Sites zone.
14. Click **OK**.
15. Click **Apply**.
16. In the tree, navigate to **Security Page → Trusted Sites Zone**.
17. Enable the following, by double-clicking in the right panel to open their respective properties page:
 - **Download signed ActiveX controls**
 - **Automatic prompting for ActiveX controls**
 - **Run ActiveX controls and plugins**
 - **Script ActiveX controls marked safe for scripting**

A.3.2.3 Enabling automatic download and installation

Windows Server 2008

When using a Windows Server 2008 Active Directory, you can use the ActiveX Installer Service to enable automatic download and installation of ActiveX controls for workstations running Windows Vista and newer.

To enable automatic download and installation of ActiveX controls from Windows Server 2008:

1. In the Group Policy Management Editor expand the domain policy → **Computer Configuration** → **Policies** → **Administrative Templates** → **Windows Components** → **ActiveX Installer Service**

2. Double-click to view Approved Installation Sites for ActiveX Controls

- (a) Select the **Enable** radio button
- (b) Click **Show** to enter the approved sites.
- (c) Click **Add...**
- (d) Enter the DNS or IP address of the *Hitachi ID Bravura Pass* server exactly as it will be entered into the address bar of Internet Explorer by users, or the Credential Provider (including the http:// or https:// prefix in this case).

- (e) Enter the value of the item to be added, in the format N,N,N,N where N is 0, 1 or 2 as defined below.

The value for each Host URL is four settings in CSV format. For maximum security, we recommend a value of 1,1,0,0 (prompt user for initial installation) or 2,2,0,0 (silently install), which represents:

"TPSSignedControl,SignedControl,UnsignedControl,ServerCertificatePolicy".

The three left most values in the policy control the installation of ActiveX controls based on their signature, and can be one of the following values:

0 – ActiveX control will not be installed

1 – Prompt the user to install ActiveX control

2 – ActiveX control will be silently installed Controls signed by certificates in trusted publisher store will be silently installed Silent installation for unsigned controls is not supported

The right most value in the policy is a bitmasked flag The flags are used for ignoring https certificate errors. The default value is 0, which means that the https connections must pass all security checks.

Use the combination of the following values to ignore invalid certificate errors

0x00000100 Ignore Unknown CA

0x00001000 Ignore invalid CN

0x00002000 Ignore invalid certificate date

0x00000200 Ignore wrong certificate usage

- (f) Click **OK** when setup finished

3. Double-click to view ActiveX installation policy for sites in Trusted zones

- (a) Select the **Enable** radio button
- (b) The following values are the recommended settings for maximum security:

Setting	Recommended value
Installation Policy for ActiveX control signed by trusted publisher	Prompt the user or Silently install
Installation Policy for signed ActiveX control	Prompt the user or Silently install
Installation Policy for unsigned ActiveX control	Don't install
Unknown certification authority (CA)	Disabled
Invalid certificate name (CN)	Disabled
Expired certificate validation date	Disabled
Wrong certificate usage	Disabled

Customizing installer (MSI) options

B

Hitachi ID Systems add-on software can be installed manually, from the command-line, or automatically using a group policy. If you want the installer package to install automatically, with no end-user interaction, you must set installation options by applying a Windows Installer Transform file (**.mst**), or by editing the installer package directly. If you are not sure how to do this, contact support@Hitachi-ID.com.

This chapter describes syntax requirements, and MSI features and property options for installing add-on software from the command line or using a Windows Installer Transform file.

For more information on running `msiexec` at the command line, see <https://docs.microsoft.com/en-gb/windows/desktop/Msi/command-line-options>.

Selecting features

You use the `ADDLOCAL` parameter to set which features you want installed. The format for the `ADDLOCAL` parameter on the command line is:

```
ADDLOCAL=<feature>,<feature>,...
```

Selecting a sub-component selects the parent component as well.

Setting parameters

If using the command line, you can specify parameters for non-interactive installation, or preset values for interactive installation. The syntax for setting parameters on the command line is:

```
<addon>.msi <parameter>=<value> <parameter>=<value>
```

Key-value pairs must be separated by spaces. If a value contains spaces, the value must be enclosed in double quotes.

For details on individual installers, see:

- Password Manager Local Reset Extension options in [Section B.1](#)
- *Login Assistant* options in [Section B.2](#)

B.1 pslocalr.msi / pslocalr-x64.msi

B.1.1 Features

Table B.1: pslocalr.msi / pslocalr-x64.msi ADDLOCAL installation options

Feature	Description
PSLOCALR	Parent component – Installs the Password Manager Local Reset Extension. Note: when installing Local Reset Extension through command line, EXCLUDED_GROUPS must have a value and ADMINACCOUNT must be valid in order for an admin account to be successfully created.

B.1.2 Properties

Table B.2: pslocalr.msi / pslocalr-x64.msi properties

Property	Description
INSTALLDIR	The directory in which the local reset extension will be installed. The default is C:\Program Files\Hitachi ID\Local Reset Extension\.
INSTALLLEVEL	This parameter is used in a silent installation and is mutually exclusive with ADDLOCAL. Set to a value from 1 to 100 for a typical installation: PSLOCALR. Set to a value greater than 100 (up to 32767) for complete installation. The default is 1.
EXCLUDED_GROUPS	If a user is a member of an excluded group, then a local reset will <i>not</i> be performed. You specify the groups to exclude in a comma-delimited list.
EXCLUDED_USERS	Used by the Local Reset Extension. If a user is in this list, then a local reset will <i>not</i> be performed. You specify the users to exclude in a comma-delimited list.
ADMINACCOUNT	When EXCLUDED_GROUPS is given a value, specify the account, in domain\user or user@domain form, with authority to validate AD group membership.
ADMINPASSWORD	The password for the administrator account indicated by ADMINACCOUNT.

B.2 ska.msi / ska-x64.msi

Note: The ska.msi and ska-x64.msi installers require Windows Installer 4.5.

B.2.1 Features

Table B.3: ska.msi / ska-x64.msi ADDLOCAL installation features

Feature	Description
SKA	Parent component, installs the <i>Login Assistant</i> SKA (secure kiosk account).
CREDPROV	Installs the <i>Bravura Pass</i> Credential Provider for Windows clients.

B.2.2 Properties

Table B.4: ska.msi / ska-x64.msi generic properties

Property	Description
INSTALLDIR	The directory in which <i>Login Assistant</i> will be installed. The default is C:\Program Files\Hitachi ID\Login Assistant\.
INSTALLLEVEL	This parameter is used in a silent installation and is mutually exclusive with ADDLOCAL. Set to a value of 1 or more (up to 32767) for a complete install: SKA+CREDPROV.
ADMIN_USERNAME	Specify the username of a privileged administrator. When you need to launch the installer from an account with insufficient privileges, use this and ADMIN_PASSWORD to specify a more privileged account to perform the installation.
ADMIN_PASSWORD	Specify the password of a privileged administrator. When you need to launch the installer from an account with insufficient privileges, use this and ADMIN_USERNAME to specify a more privileged account to perform the installation.

Table B.5: ska.msi / ska-x64.msi SKA properties

Property	Description
SKATIMEOUT	The maximum amount of minutes the <i>Login Assistant</i> secure kiosk account will stay open before it automatically closes. Default is 15 minutes.
URL	The full path to the Front-end (PSF) on the <i>Bravura Pass</i> server; for example, https://server:443/instance/ .
USEVPN	0 1 If set to 1, use a VPN connect program.
HELPADMINENABLED	0 1 No longer used.
HELPAccount	The name of the <i>Login Assistant</i> “help” account (default is <code>help</code>).
HELPPASSWORD	The password for the help account specified by HELPAccount. If this option is <i>not</i> set, you must set RANDOM_HELPPASSWORD to generate a random password. If neither option is set, a blank password is created.

... continued on next page

Table B.5: ska.msi / ska-x64.msi SKA properties (Continued)

Property	Description
RANDOM_HELPPASSWORD	<p>0 1 Set to 1 to create a random password for HELPPASSWORD. This setting is off by default.</p> <p>This setting defaults to 0 for <i>Login Assistant</i> SKA-only installations and to 1 for CREDPROV installs – it is not recommended to use a random password in <i>Login Assistant</i> SKA-only installations.</p> <p>Note that when HELPPASSWORD and RANDOM_HELPPASSWORD are both specified, the RANDOM_HELPPASSWORD setting is ignored.</p>
IMAGEFILE	<p>Fully-qualified file name for the bitmap file used to replace the the Credential Provider tile for CREDPROV installations.</p> <p>The MSI can also be modified, using an MSI editing tool, to add an "ImgFile" entry into the Binary table, where the binary file is the bitmap to use.</p>
LANGUAGEFILES	<p>Specifies a pipe-separated list of gina.z files to use as additional languages for the secure kiosk account and Credential Provider. These must be fully-qualified file names. The gina.z files are generated in the 12.2.4 language packs. The list must be enclosed in double quotes.</p> <p>The MSI can also be modified, using an MSI editing tool, to add an entry into the Binary table, of the form Lang_<language>-<country>, where the binary file is the gina.z file for the corresponding language. For example, Lang_fr-ca can be added with the contents of the gina.z file from the fr-ca skin.</p>
EN_US, <LANGUAGE>_<COUNTRY>	0 1 Indicates whether the specified language is enabled for use. EN_US is installed by default. Additional languages are specified with the LANGUAGEFILES setting.
SHELLOPTIONS	Command-line options for the runurl command, used when invoking the web browser. The default is " -kiosk -no_icw -logoff -trapsesslock ".
RUNURLCFG	Provide any additional options that may be required for runurl . This replaces the shell options with " -cfg runurl.cfg ", and generates a runurl.cfg file that includes the shell options and any additional options specified by this property. The default is no value.
HIDEERRORS	0 1 Set to 1 to suppress warnings when the SKA displays a page that contains JavaScript errors. This setting is off by default.

Table B.6: ska.msi / ska-x64.msi VPN properties

Property	Description
REMOTESKAACCESSEENABLED	0 1 Enable or disable remote access to the SKA.
VPN_CONNECT_PROGRAM	Name and full path of the VPN connect program to run in order to establish a VPN connection.
VPN_CONNECT_CMDLINE	Command-line arguments for VPN connect program; for example -u %userid% -p %password% . This value cannot be blank.
VPN_DISCONNECT_PROGRAM	Name of the VPN disconnect program to run to disconnect from the VPN.

... continued on next page

Table B.6: ska.msi / ska-x64.msi VPN properties (Continued)

Property	Description
VPN_DISCONNECT_CMDLINE	Command-line arguments for VPN disconnect program; for example <code>-u %userid% -p %password%</code> .
VPN_USER	VPN user ID to be used with the VPN connect and disconnect programs.
VPN_PASSWORD	Password to be used with the VPN user ID.
VPN_TIMEOUT	The number of seconds to wait between retries. The default is 30.
VPN_RETRIES	The number of VPN retries to test for connectivity. If this value is blank, there will only be one retry attempt. The default is 3.
VPN_CONNECT_STDINPUT	Standard input lines for Cisco anyConnect connections. See Command-line Cisco anyConnect VPN parameters for details.
VPN_CONNECT_TERMINATE	For Cisco anyConnect, terminate any running programs before trying to launch the VPN client. See Command-line Cisco anyConnect VPN parameters for details.
VPN_HIDE_WINDOW	For Cisco anyConnect, hide the pop-up console window that <code>vpncli.exe</code> starts. See Command-line Cisco anyConnect VPN parameters for details.

Table B.7: ska.msi / ska-x64.msi remote access properties

Property	Description
RUNURL_EXTERNAL_URL	<p>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 <code>http://www.msftncsi.com/ncsi.txt</code>.</p> <p>Other options for the external url are <code>http://detectportal.firefox.com/success.txt</code> with <code>RUNURL_EXTERNAL_URL_EXPECTED_DATA</code> set to <code>success</code></p> <p>Or <code>http://captive.apple.com/hotspot-detect.html</code> with <code>RUNURL_EXTERNAL_URL_EXPECTED_DATA</code> set to <code>Success</code></p>
RUNURL_EXTERNAL_URL_EXPECTED_	<p>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 <code>Microsoft NCSE</code>.</p>
RUNURL_EXTERNAL_CONNECT_PROG	<p>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 SKA to allow the user to connect.</p>
RUNURL_EXTERNAL_CONNECT_PROG	

... continued on next page

Table B.7: ska.msi / ska-x64.msi remote access properties (Continued)

Property	Description
	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.
RUNURL_PORTAL_TIMEOUT	The number of seconds to wait for a captive portal connection. The default is 300.
RUNURL_REMOTE_HOST	The address of the VPN server to test if the server is reachable.
RUNURL_REMOTE_PORT	The port that the VPN server is listening on to test if the server is reachable.

Table B.8: ska.msi / ska-x64.msi proxy properties

Property	Description
PROXY_ENABLE	0 1 Enable or disable the installer to modify Internet Explorer proxy configuration.
PROXY_AUTODETECT	0 1 Enable or disable Internet Explorer proxy to use "Automatically detect settings".
PROXY_AUTOCONFIGURATION_ENABLE	0 1 Enable or disable Internet Explorer proxy to use "Use automatically configuration script".
PROXY_AUTOCONFIGURATION_URL	Use this to set the URL of an automatic configuration script.
PROXY_URL	Use this to set the proxy server's address.
PROXY_PORT	Use this to set the proxy server's port number.

The following parameters are available with ADDLOCAL=CREDPROV for Windows:

Table B.9: ska.msi / ska-x64.msi CREDPROV properties

Property	Description
HIDEFASTUSERSWITCHING	0 1 Hides Fast User Switching on this machine, preventing multiple concurrent logins. The default is 1. This property is no longer used and will be removed in future releases. Fast User Switching must be enabled.
USECLASSICLOGON	0 1 Provides a more traditional interface for login (rather than individual tiles) for users. It prompts for a user ID and a password. The default is 1.

SKA client: runurl

C

Description

The **runurl** program launches a web browser on a Windows workstation and opens it to a specified URL. When configured to launch in kiosk mode the browser window fills the screen, removes all window borders and decorations, disables navigation, and disables all function keys, the **[Alt]** and **[Ctrl]** keys, the Windows logo key, and any combination of keys that you specify.

A major use for the **runurl** program is to enable users to reset their own passwords using a SKA.

C.1 Requirements

When invoked by a local SKA or Credential Provider, **runurl** is launched from the Login Assistant\ directory on the user's workstation.

The following files must be located in the share or directory from which **runurl** is launched:

- **msgmap.txt** – used to disable Windows message events on Windows workstations.
- **webbrowser.dll** – used to block the **[Ctrl]**, **[Alt]**, and the right mouse button, and to run the web browser. It is also used by the Credential Provider.
- **pscredprov.dll** – used to block the **[Ctrl]**, **[Alt]**, and the right mouse button, and to run the web browser. It is used by the Credential Provider.
- **launch_ska.exe** – used to launch the SKA and invoke the **runurl** command.

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.

C.2 Usage

```
runurl.exe -url <URL> [<options>]
```

```
runurl.exe -cfg <filename>
```

The **runurl** program works with the following command-line arguments:

Table C.1: runurl options

Option / Argument	Description
-url <URL>	Specify the URL that will be displayed in the web browser.
-userid <userID>	<i>Bravura Pass</i> user ID to pass through the URL.
-ntkeymap <args>	Enable or disable a key or combinations of keys on a Windows workstation. See Enabling or disabling key combinations for details.
-msgmap <filename>	Specify a file containing Windows message events to block. Do <i>not</i> modify this file unless you are sure of what you are doing.
-reg <filename>.reg	Load the named registry file into the registry before terminating runurl . This is used to restore standard registry entries in case runurl was launched during the first login of the help account, using a restrictive security policy, and the user elected to not save settings – which means that registry changes were applied to the default user rather than help.
-kiosk	Start the web browser in kiosk mode.
-keylock	Disable [Ctrl] , [Alt] , and the right mouse button. This is implied by -kiosk .
-no_icw	Do not pop up Internet Connection Wizard when the user starts up the browser the first time.
-logoff	Log off from the workstation after the web browser closes.
-run "<programname>,<args>"	Run this program with these parameters before exiting, and before logging off. The run option requires quotes around the external program name and param arguments. If you need quotes inside of this then use a \ to escape them. If both run and logoff are specified, run will execute first.
-cfg <filename>	If the command line is too long, use this option to read all arguments from this file. Write the file with the arguments separated by white space.
-trapsesslock	Trap the Windows workstation lock notification to ensure that runurl handles locked workstations correctly; for example a browser displaying a <i>User notifications</i> (PSN) module notification is returned to the state it was in before the lock.

C.3 Enabling or disabling key combinations

You can run **runur1** with the `-ntkeymap` option to enable or disable keys and combinations of keys on a Windows workstation (XP or higher). Write the arguments for `-ntkeymap` using the following syntax:

```
[ - ] [ ( ) [ <MOD>+ ] <KEY> [ ) ] [ , ... ]
```

Where:

– enables the keys that follow

() are optional brackets (these are for formatting only, they do not modify the meaning of the text)

<MOD> specifies one of **[Alt]**, **[Shift]**, **[Ctrl]**, or the Windows key

<KEY> specifies the name of the key to enable/disable

<KEY> can be any of the following:

'	A	F13	I	Num8
,	Alt	F15	J	Num9
-	B	F2	K	NumDel
.		F20	L	O
/	Backspace	F21	M	P
0	C	F22	N	Pause
1	CapsLock	F23	Num*	Q
2	Ctrl	F24	Num+	R
3	D	F3	Num-	RightShift
4	E	F4	Num0	S
5	Enter	F5	Num1	
6	Esc	F6	Num2	ScrollLock
7	F	F7	Num3	Shift
8	F1	F8	Num4	Space
9	F10	F9	Num5	SysReq
;	F11	G	Num6	T
=	F12	H	Num7	Tab

U	Win	Z]
V	X	[
W	Y	\	'

C.4 Examples

1. To launch a web browser in kiosk mode and open it to the *Change passwords* (PSS) module, open a command prompt, and type on one line:

```
runurl.exe -kiosk -logoff -no_icw -trapsesslock -url https://<server>/<instance>/
change-passwords
```

2. If **runurl** is run from a public share rather than your current workstation, specify the UNC path to **runurl** in your command. If the share is located on an Active Directory domain controller, open a command prompt, and type on one line:

```
\\MyADDC\SYSVOL\runurl.exe -kiosk -logoff -no_icw -trapsesslock -url https://<
server>/<instance>/change-passwords
```

3. To disable keys on a Windows workstation using the **-ntkeymap** option, open a command prompt, and type on one line:

```
runurl.exe -kiosk -logoff -no_icw -trapsesslock
-url https://<server>/<instance>/change-passwords
-ntkeymap Win+F1,-Shift+F1,Alt+Shift+F1,F1
```

This is the same as:

```
runurl.exe -kiosk -logoff -no_icw -trapsesslock
-url https://<server>/<instance>/change-passwords
-ntkeymap (Win+F1),(-Shift+F1),(Alt+Shift+F1),(F1)
```

4. To print a list of available key names for the **-ntkeymap** option on the command line, type the following in the Login Assistant\ directory:

```
runurl -ntkeymap ?
```

5. An example of a runurl.cfg file:

```
-kiosk -logoff -no_icw -trapsesslock -url http://<server>/<instance>/?
```

6. To run commands from a configuration file, type:

```
runurl -cfg runurl.cfg
```

Description

Use the **skautil** program to update cached registry values for VPN connection credentials or the local, secure kiosk account (LSKA) (help) userID and/or password used in the secure kiosk account. The program does *not* change the underlying password; only the cached registry values.

Usage

```
skautil.exe -vpnuser <vpnuser> | -vpnpass <vpnpass> | -helpuser  
<helpuser> | -helppass <helppass>
```

Table D.1: skautil arguments

Argument	Description
-vpnuser <vpnuser>	The new VPN user to write into the registry.
-vpnpass <vpnpass>	The new VPN user's password to write into the registry.
-helpuser <helpuser>	The new help account to write into the registry.
-helppass <helppass>	The new help account's password to write into the registry.

File Locations

E

This chapter provides details of the location and purpose of files installed by:

- *Hitachi ID Bravura Security Fabric* (p93)
- *Hitachi ID Connector Pack* (p98)

When you install any Hitachi ID Systems product, the default path for program files is:

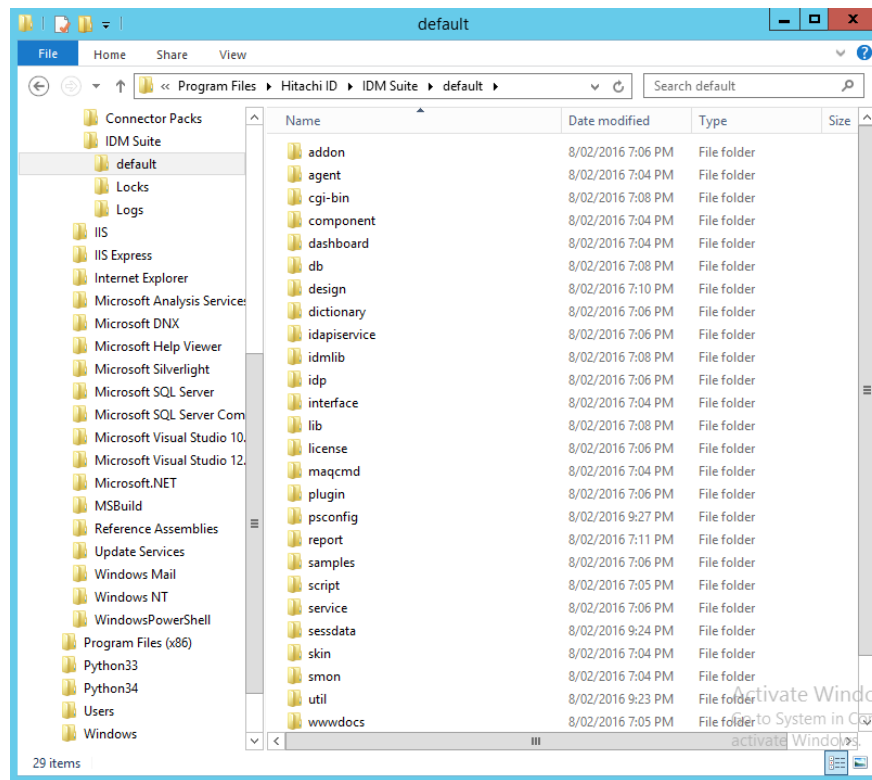
C:\Program Files\Hitachi ID\

E.1 *Bravura Security Fabric* directories and files

There are three main directories that are created when you install *Bravura Pass* instance:

- <Program Files path>\Hitachi ID\IDM Suite\<instance>\
- <Program Files path>\Hitachi ID\IDM Suite\Logs\<instance>\
- <Program Files path>\Hitachi ID\IDM Suite\Locks\

The contents of those directories are detailed in the following subsections.



It is recommended that you do *not* change these directory locations during the setup process. You cannot install any of the directories required for *Bravura Pass* on a mapped drive.

E.1.1 Instance directory

[Instance directory files](#) describes the function of directories that are created when an instance of *Bravura Pass* is installed.

Note: Directories marked with ★ include files installed by *Connector Pack*.
Directories marked with ★★ include folders and files installed with the optional *Analytics* app.
Directories marked with † include optional files. They are only installed in a complete installation or if selected in a custom installation.

Table E.1: Instance directory files

Directory	Contains
† * addon	Files required for add-on software, such as Password Manager Local Reset Extension and SKA. Some files, required to target Netegrity SiteMinder, are installed by <i>Connector Pack</i> . If you installed a global <i>Connector Pack</i> , these files are contained in the <i>Connector Pack</i> global directory.
* agent	Instance-specific user management connectors (agents). If you installed a global <i>Connector Pack</i> , user management connectors are contained in the <i>Connector Pack</i> global directory.
** analytics	<i>Analytics</i> app specific folders
** analytics\DataSets	Contains *. rsd files which are Shared Dataset Definitions. These files are only used by SQL Server versions higher than Express. They contain datasets that are shared between reports.
** analytics\Hidden	Contains *. rdl files which are Report Definitions. These files are the drillthrough reports used by other reports. They are not visible to the end-user.
** analytics\ReportItems	This folder contains other folders. Each folder in this folder is a category in the <i>Analytics</i> app. Within these folders are *. rdl files which are Report Definitions. The folders need to be added to the CUSTOM ANALYTIC CATEGORIES system variable to be visible. These reports are then visible to the end-users in the <i>Analytics</i> app.
cgi-bin	The user web interface modules (*. exe CGI programs).
db	The <i>Bravura Pass</i> database SQL scripts.
db\cache	Search engine temporary search results. These files are cleaned up nightly by psupdate .
db\replication	Stored procedure replication queues, and temporary replicated batch data.
* design	Files necessary to make modifications to the GUI. Some files are installed by <i>Connector Pack</i> . If you install a global <i>Connector Pack</i> , files related to connectors are located in the global design directory. See the Bravura Security Fabric Documentation for details.
dictionary	A flat file, words.dat , that contains dictionary words. <i>Bravura Pass</i> uses this file to determine if new passwords fail dictionary-based password-policy rules.
idapiservice	Files required to use the SOAP API.
* interface	Instance-specific ticket management connectors (exit trap programs). If you installed a global <i>Connector Pack</i> , ticket management connectors are contained in the <i>Connector Pack</i> global directory.
lib	Contains the pslangapi.dll .
license	The license file for <i>Bravura Pass</i> .
plugin	Plugin programs executed by <i>Bravura Pass</i> .

... continued on next page

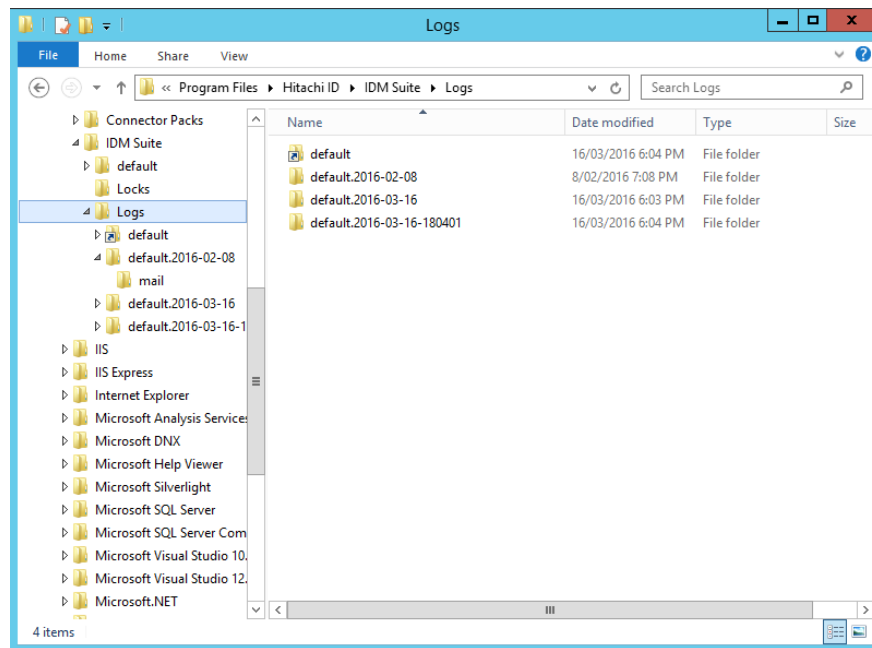
Table E.1: Instance directory files (Continued)

Directory	Contains
psconfig	List files produced by auto discovery and the <code>idmsetup.inf</code> file.
report	Files and programs for report generation.
† ★ samples	Instance-specific sample scripts and configuration files. If you installed a global <i>Connector Pack</i> , connector-related sample files are contained in the <i>Connector Pack</i> global directory.
script	Configuration files and scripts used by connectors, <code>psupdate</code> , plugins and interface programs.
service	Service programs.
sessdata	Session data. A scheduled program removed old data files nightly.
skin	Compiled GUI files used at run-time (HTML and *.z).
★ util	Command-line programs and utilities. If you install a global <i>Connector Pack</i> , tools related to connector configuration are located in the global util directory.
★ unix	The <code>psunix</code> archive, which is required to install the Unix Listener and supporting files on a Unix-based target system. If you installed a global <i>Connector Pack</i> , this directory is created in the <i>Connector Pack</i> global directory.
wwwdocs	Images and static HTML pages used by <i>Bravura Pass</i> .

E.1.2 Log directory

Any operation that is run by *Bravura Pass* is logged. Those logs are invaluable when debugging an issue. The log directory by default is `C:\Program Files\Hitachi ID\IDM Suite\Logs\`. Each instance of *Bravura Pass* that is installed will have at least one sub-directory within this directory.

The `rotatelog` scheduled job, which runs on a nightly basis, rotates the logs in to a new folder, to reduce disk space usage.



See the [Bravura Security Fabric Documentation](#) for more information.

E.1.3 Locks directory

Certain target systems can only be accessed serially, such as Lotus Notes. This is a limitation of the API used to access the target system. In these cases *Bravura Pass* drops a *lock file* in the locks directory when an operation is being performed that should only be performed serially. For this reason the locks directory *must* be the same for all instances of *Bravura Pass* that are installed on the same server.

See the [Bravura Security Fabric Documentation](#) for more information.

E.2 Connector pack directories and files

When you install *Hitachi ID Connector Pack*, files are placed in different locations depending on type of *Connector Pack*.

For an instance-specific connector pack, the installer, **connector-pack-x64.msi**, installs connectors and supporting files in:

<Program Files path>\Hitachi ID\IDM Suite\<instance>\

For a global connector pack, the installer, **connector-pack-x64.msi**, installs connectors and supporting files in:

<Program Files path>\Hitachi ID\Connector Packs\global\

[Connector Pack directory files](#) describes the function of directories that are created when a *Connector Pack* is installed:

Table E.2: Connector Pack directory files

Directory	Contains
addon	Files required to target Netegrity SiteMinder systems
agent	User management connectors (agents)
design	<i>Connector Pack</i> -related files necessary to make modifications to the GUI; for example target system address help pages. See the Bravura Security Fabric Documentation for details.
interface	Ticket management connectors (exit trap programs)
samples	Sample scripts and configuration files
unix	The psunix archive, which is required to install the Unix Listener and supporting files on a Unix-based target system
util	Tools to support the configuration of various target systems

Index

A

Active Directory

- 2008 group policy settings, 51
- 2012 group policy settings, 49
- secure kiosk account, 23, 46–53

ActiveX

- security, 76

add-on software

- installation using a group policy, 74

Analytics, 94, 95

authentication

- IVR, 56, 59
- voice, 56

C

cgilocalr, 18

cgilocalr.cfg, 18

Change passwords, 3, 4, 6, 11, 16–18, 91

Cisco anyConnect VPN parameters, 37

client tools

- local reset extension, 14

configuring

- ActiveX security, 76
- IVR registration, 62
- self-service hard drive unlock, 68

Credential Provider, Login Assistant, 24

customizing

- password reset, 18

D

digital signatures, 73

domain-level Login Assistant, 46–54

- Active Directory 2008 group policy, 51
- Active Directory 2012 group policy, 49
- advertising the account, 53
- configuring the runurl program, 47
- creating a help user, 47
- creating group policy, 48

domain-level secure kiosk account, 23

F

Front-end, 84

G

Generate voice print enrollment PIN, 61, 62, 65

gina.z, 47

global *Connector Pack*

- files, 98

group policy

- for domain-level Login Assistant, 48

H

hdd, 68, 69

- configuring, 68

hidgeneric.ocx, 18

HISCPINToolAX.ocx, 6

I

idapi, 65

idmsetup.inf, 96

installation directory path

- instance specific *Connector Pack*, 98

installing

- add-on software, using a group policy, 74
- local reset extension, 14
- Login Assistant, 30

instance-specific *Connector Pack*

- location, 98

interactive voice response system, 56, 61

IVR authentication

- architecture, 57
- integration, 56
- password resets, 65
- question sets, 60
- touch tone, 59
- voice print, 61

IVR registration, 61–62
 configuring, 62
 options, 62
 selecting an IVR ID source, 58

K

kiosk mode, 88–91

L

launch_ska.exe
 runurl, 88
 local password reset
 plugins, 18
 local reset extension, 14
 local secure kiosk account
 uninstalling, 38
 Login Assistant, 23, 30–38
 configuring language support, 36
 installing, 30
 installing help account, 33
 manual installation, 30
 msi properties, 83
 NETLOGON, 27
 Password Manager Credential Provider, 24
 proxy, 35
 remote access, 25
 remote connection, 34
 self service anywhere, 25
 SYSVOL, 27
 troubleshooting, Windows, 38
 vpn connection, 33

M

modifying
 msi properties, 74
msgmap.txt
 runurl, 88
 msi installers
 manual installation, 74
 using, 73
 msi properties
 modifying, 74

N

nplocalr.ocx, 12, 18

O

Orca, 74

P

Password Manager Credential Provider, 24
 Password Manager Remote API, 65
 password resets
 adding GUI functionality, 18
 IVR authentication, 65
 passwords
 reset by telephone, 56
 resetting locally on workstations, 10
 PGP Whole Disk Encryption
 resetting cached credentials, 10
 proxy, Login Assistant, 35
pscredprov.dll
 runurl, 88
 psf, 84
 psi, 62
 configuring, 61
pslangapi.dll, 95
pslocalr
 msi properties, 83
pslocalr-x64.msi, 13, 14
pslocalr.msi, 13, 14
pslocalr.ocx, 18
 pss, 18
psunix, 96, 98
psupdate, 96

R

remote connection, Login Assistant, 34
runurl, 27, 33, 47, 48, 85, 88–91
 configuring for secure kiosk account, 47
runurl.cfg, 48

S

scpinplugin, 6
 secure kiosk, 23–54
 secure kiosk account
 domain-level, 23, 46–54
 Login Assistant, 23
 NETLOGON, 27
 SYSVOL, 27, 47
 Windows workstations, 23
 selecting an IVR ID source, 58
 self-service anywhere, 68
 self-service hard drive unlock, 68
 configuring, 68
 options, 68

ska

msi properties, 83

ska-x64.msi, 30, 31

ska.msi, 30, 31

Login Assistant, 30

skautil, 92

synchronizing workstation cached credentials, 10

U

User notifications, 3, 89

V

VPN connection, Login Assistant, 33

W

web browser, launching, 88–91

webbrowser.dll

runurl, 88

Windows Installer, 74

Windows workstation

launching web browser, 88–91

resetting cached credentials, 10

Windows workstations

Login Assistant, 23

words.dat, 95

