User Manual

GUI Application
HiView 4.2

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2021 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at:
https://www.doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

User Manual – Rel. 4.2 – 09/2021

Contents

1 Introduction 5

1.1 Password change during first time log on 6

2 Starting the application 7

2.1 System Requirements 8
2.1.1 Hardware 8
2.1.2 Operating system 8

2.2 Installation 10
2.2.1 Installation under Windows 10
2.2.2 Installation under Linux 11

2.3 Deinstallation 12
2.3.1 Deinstallation under Windows 12
2.3.2 Deinstallation under Linux 12

3 Using HiView 13

3.1 Devices Tab 14
3.1.1 Adding a device 15
3.1.2 TLSv1 and TLSv1.1 algorithm handling 15
3.1.3 Tile view 16
3.1.4 Table view 18
3.1.5 Removing a device 19
3.1.6 Device access 19
3.1.7 Connecting to Industrial HiVision 23

3.2 Discovery Tab 25
3.2.1 Discovery Tab Visibility 25
3.2.2 HiDiscovery v2 25
3.2.3 Network Adapter 26
3.2.4 Signaling a Device 27
3.2.5 First time log on (Password change) 27
3.2.6 IP address management 28
3.2.7 Device access 28

4 HiView Applet Launcher 31

4.1 Starting the Applet Launcher 32

4.1.1 Open a device with the Applet Launcher 34

4.1.2 Auto-Login 34

5 Saving an individual configuration 35

6 Delete cache directory 37

7 Devices in the Hirschmann Application Lab 39

8 Maintenance 41

A Tested products and software versions 43

B Index 48

C Further support 49

1 Introduction

HiView is a stand-alone application. HiView thus allows you to use the graphic user interface of Hirschmann Ethernet devices with management independently of other applications, such as a browser.
HiView is convenient in that it allows you to store HiView on a portable storage medium and start it on other computers in your data network.
HiView also supports your security efforts, as accessing Hirschmann devices with a product certificate is possible only with a valid product certificate.

Application Example

As the administrator of a large data network, you sometimes have to visit sites within your data network.
With a USB stick in your pocket, on which you have previously copied HiView with your settings, you have barrier-free access to the graphical user interface of Hirschmann Ethernet devices.
Forget difficulties such as the incompatibility of browsers, Java versions or Java plug-ins, installation with entries in the registry or the changing cache content of browsers on different computers.

1.1 Password change during first time log on

To help prevent undesired access to the devices, it is imperative that you change the default password during initial setup.

Starting with the following software releases, it is necessary to change the default password during the initial setup:

- HiOS
  08.1.00
  07.1.00
- Classic Switch
  09.1.00
  09.0.17
- RSB
  05.3.09
- GECKO
  02.2.00
- Eagle 20/30/40
  03.3.00
- EagleOne
  05.4.00

You can find detailed information about changing the password in “First time log on (Password change)” on page 27.

2 Starting the application

HiView is a stand-alone, portable application. This section describes the prerequisites and preparations for starting the HiView application.

2.1 System Requirements

2.1.1 Hardware

- Processor
  x86 compatible CPU, min. 1 GHz
- RAM
  at least 1 GB, 2 GB recommended
  HiView requires approx. 200 MB free RAM.
  For every open window, HiView requires an additional 500 MB RAM
  To start Industrial HiVision, HiView requires an additional 2 GB RAM
- Disk space
  1 GB free.
- Monitor resolution
  at least 1024x768 pixels.

2.1.2 Operating system

- Windows 7 (64 Bit)
- Windows 8.1 (64 Bit)
- Windows 10, Version 1803 (64 Bit)
- Windows Server 2019

- PC Linux (64 Bit: Kernel 3.10, libc 6):
  Debian 8
  Debian 9
  Debian 10
  Red Hat 7
  Red Hat 8

Note: Install the `libgtk2.0-0` packages for Debian.

2.2 Installation

2.2.1 Installation under Windows

If you use the installation wizard proceed as follows:
- ☐ Download the `hiview04200_windows.exe` file.
- ☐ To install HiView, double click on the program file.
- ☐ Answer the questions of the installation script and follow its instructions. If you do not answer a question of the installation script, then the installation script selects the default answer.

If you wish to use HiView as a portable application, then proceed as follows:
- ☐ Download the `hiview04200_windows.zip` file.
- ☐ Verify that authentication is available for data read-write access.
- ☐ Extract the files onto your portable medium for example, SD card, USB stick or onto the hard drive of your computer.

- ☐ To start the HiView application, double click the `HiView` program symbol.

Note: If you get the message `Error during installation of ikernel.exe`, then the current user account does not have administration rights.

The first time you start the HiView application, HiView asks you to accept the license conditions.
After you have accepted the license conditions, HiView creates the configuration file `HiView[2.0].cfg`.
Among other things, the configuration file also contains the languages of the application interface that you can select.

Note: When you restart the application, HiView opens the last saved configuration.

2.2.2 Installation under Linux

☐ Download the `hiview04200_linux.tar.gz` file.
☐ Extract the archive file into a file system that supports “Execute” rights. Depending on the Linux derivative, the file system can be stored onto a portable medium for example, SD card, USB stick or onto the hard drive of your computer.
☐ Provide “Execute” rights to every HiView application, (*.sh) in the HiView root directory with the chmod command. For example, run the command, `chmod +x HiView.sh.`

☐ Start the HiView application `HiView.sh`.
The first time you start the HiView application, HiView asks you to accept the license conditions.
After you have accepted the license conditions, HiView creates the configuration file `HiView[2.0].cfg`.
Among other things, the configuration file also contains the languages of the application interface that you can select.
You will find details on the different Linux derivatives on the product pages of Belden.
www.beldensolutions.com

Note: When you restart the application, HiView opens the last saved configuration.

2.3 Deinstallation

2.3.1 Deinstallation under Windows

☐ Quit the program HiView before you start the deinstallation.

☐ To uninstall HiView, select:
`Start:Control Panel:Software`

☐ Select the program HiView.

☐ Click on Change/Remove and follow the instructions of the deinstallation routine.

If you installed HiView as a portable application, then proceed as follows:
☐ Navigate to the extracted files on your portable medium for example, SD card, USB stick or on the hard drive of your computer. Verify that authentication is available for data read-write access.
☐ Delete the directory where you extracted the application files.

2.3.2 Deinstallation under Linux

☐ Log on with the `su` command so that you have root access rights.

☐ Delete the directory where you extracted the application files with the command `rm -rf`

3 Using HiView

After you start it the first time, HiView displays the following program window:

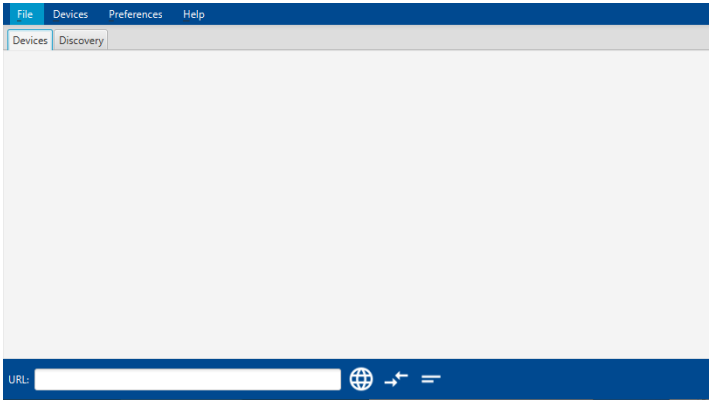

Figure 1: HiView program window after you start it the first time

The dialog contains the following tabs:

- Devices Tab
- Discovery Tab

3.1 Devices Tab

The Devices tab displays your devices as either a tile or a list item. You can verify the reachability and configure the devices displayed in the dialog. The dialog allows you to configure the devices using a web browser, telnet or SSH.

If you use HTTPS to connect to a device and get the message, “`Secure connection failed, please try again using a URL prefix and port.`”, then update the device software.

After you update the device software, proceed as follows:

☐ Make a new certificate.
Use an up-to-date hash algorithm to make the new certificate.

☐ Upload the new certificate on the device.

If you can not use HTTPS to connect to your device, then you can try to access the device with HTTP.

Note: HTTP and Telnet are unsecure connections. Hirschmann recommends that you use only secure methods, such as HTTPS or SSH to access your device.

☐ To use HTTP to access your device, enter `http://<IP address>` in the URL field.

3.1.1 Adding a device

To add a device to the `Devices` tab, proceed as follows:

- ☐ In the URL field at the bottom of the dialog, enter the path with the IP address of your device or its domain name.
- ☐ Click the `Open GUI` button.
  HiView establishes a connection to the device, opens the graphical user interface of the device and adds the device to the dialog. HiView copies the program file of the device to the cache directory of the HiView installation directory.

The HiOS devices, with software version 7.0 and higher, have an HTML5 based Graphical User Interface (GUI). When you enter an IP address of a device with an HTML5 based GUI, HiView connects to the device with your default browser. After accessing the device, HiView adds the device to the dialog.

The BAT devices also have HTML dialogs. When you enter an IP address of a BAT device, HiView connects to the device with your default browser.

Note: HiView does not support BAT-C nor BAT-C2 devices.

Note: To help provide secure communications, use HTTPS or SSH to connect to a device. Disable the HTTP and Telnet functions in the Web Server dialog of the device.

3.1.2 TLSv1 and TLSv1.1 algorithm handling

The TLSv1 and TLSv1.1 algorithms are deprecated and have been succeeded by the TLSv1.2 algorithm. Some older devices, or servers with older software, still use the TLSv1 or TLSv1.1 algorithm. In the default setting, the HiView application supports the TLSv1 and TLSv1.1 algorithms.

To disable the TLSv1 and TLSV1.1 algorithms, perform the following steps:

- ☐ Close the HiView application.
- ☐ Using a text editor, save a text file as `security.properties` to your installation directory:
- ☐ Enter the following text into the `security.properties` file:
  `reenableUnsecureTLSAlgorithms=false`
- ☐ Save the `security.properties` file.
- ☐ Restart the HiView application.

3.1.3 Tile view

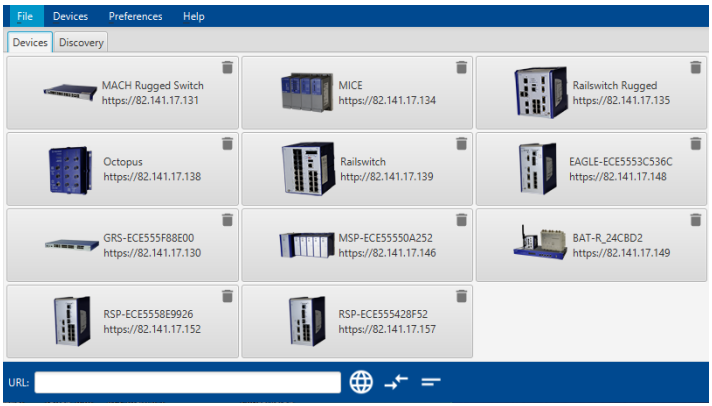

Figure 2: Tile view

The Tile view is the HiView default setting. If you want to switch from Tile View to Table view, proceed as follows:

- ☐ To display the Table view, select `Preferences > View > Table view`.

Every tile represents one device and displays the device symbol, the device name and the device address.
The more often you establish a connection to the device, the further forward HiView places the device in the Tile view.

3.1.4 Table view

HiView provides a Table view as an alternative to the Tile view:

	MACH 4002	http://82.141.17.131		
	Power MICE	http://82.141.17.133		
	MICE	http://82.141.17.134		
	Railswitch Rugged	http://82.141.17.135		
	Octopus	http://82.141.17.138		

Figure 3: Table view

☐ To display the Tile view, select `Preferences > View > Tile view`.

Every table row represents one device and displays the device symbol, the device name and the device address. Furthermore, HiView indicates with a check mark in the “Open” column if the graphical user interface of the device is open.
The more often you establish a connection to the device, the further up the list HiView places the device in the Table view.

3.1.5 Removing a device

To remove a device from the `Devices` tab, proceed as follows:

- Tile view
  - ☐ Select the tile of the device you want to delete.
  - ☐ Click the “Delete“ button.
- Table view
  - ☐ Select the table row with the device you want to delete:
  - ☐ Select `Devices > Delete Selected Devices`.

3.1.6 Device access

Certificate Fingerprints

If HiView does not have an HTTPS certificate fingerprint on record for a device, then HiView displays the “Confirm HTTPS Certificate“ dialog. The dialog contains the fingerprint of the HTTPS certificate. HiView also displays the “Confirm Applet Signature Certificate“ dialog when a fingerprint for an applet signing certificate is not on record. To help prevent a man-in-the-middle attack, verify that the dialog contains the correct fingerprint.

If you do not know the fingerprint of the HTTPS certificate, then you can use HiView to get the fingerprint. To get the fingerprint of the HTTPS certificate, perform the following steps:

- ☐ In a controlled environment, connect the isolated device, for which you wish to get the fingerprint, directly to your PC.
- ☐ Open the GUI of the device.
- ☐ When the fingerprint of the certificate is not recorded in the `ssl_known_hosts` file, HiView displays the “Confirm HTTPS Certificate“ dialog.
- ☐ Copy the fingerprint to a secure location.

If you do not know the fingerprint of the applet signing certificate, then you can use HiView to get the fingerprint. To get the fingerprint of the applet signing certificate, perform the following steps:

- ☐ In a controlled environment, connect the device, for which you wish to get the fingerprint, directly to your PC.
- ☐ Open the GUI of the device.
- ☐ In the “Confirm HTTPS Certificate“ dialog, click either the “Accept“ or the “Accept Permanently“ button. The “Confirm Applet Signature Certificate“ dialog opens.
- ☐ Copy the fingerprint to a secure location.

If HiView does not display the “Confirm HTTPS Certificate“ dialog, then HiView accepted the fingerprint permanently in a previous session. To display the “Confirm HTTPS Certificate“ dialog again, perform the following steps:

- ☐ Close the GUI of the device.
- ☐ Open the `<Installation directory>/ssl_known_hosts` text file.
- ☐ Comment out the line that contains the IP address and fingerprint of the device.
- ☐ In HiView, reopen the GUI of the device. The “Confirm HTTPS Certificate“ dialog opens.

If HiView does not display the “Confirm Applet Signature Certificate“ dialog, then HiView accepted the fingerprint permanently in a previous session. To display the “Confirm Applet Signature Certificate“ dialog again, perform the following steps:

- ☐ Close the GUI of the device.
- ☐ Open the `<Installation directory>/known_applet_signatures` text file.
- ☐ Comment out the fingerprint lines.
- ☐ In HiView, reopen the GUI of the device.When HiView did not record the fingerprint of the HTTPS certificate in a previous session the “Confirm HTTPS Certificate“ dialog opens.
- ☐ In the “Confirm HTTPS Certificate“ dialog, click either the “Accept“ or the “Accept Permanently“ button. The “Confirm Applet Signature Certificate“ dialog opens.

Note: HiView displays the “Confirm Applet Signature Certificate“ dialog for certificates issued around the release date of HiView 4.2, and later.

After the network administrator gets the fingerprint of the certificate, the network administrator uses a secure channel to send the fingerprint to the remote client. The remote client compares the fingerprint received from the network administrator to the fingerprint in the dialog. To help you verify the fingerprint, HiView lets you copy and paste the fingerprint in the “Fingerprint to verify“ field.

The buttons in the dialog let you perform the following actions:

- “Accept“
  HiView accepts the certificate, but does not record the fingerprint for future reference. HiView opens the dialog for confirmation each time you access the device.
- “Accept Permanently“
  HiView records the fingerprint for future reference.
- “Cancel“
  The dialog closes without making a connection to the device. The fingerprint is not recorded for future reference.

Graphical user interface (GUI)

To access a device through the graphical user interface, proceed as follows:

- Tile view
  - ☐ Select the tile of the desired device.
- Table view
  - ☐ To view the context menu, right-click the table row of the desired device.
  - ☐ Click the “Open GUI“ button.

Note: If you use your computer to connect to the device through a firewall, enter a rule in the firewall that allows the data traffic through port `161`.

Command Line Interface (CLI)

HiView lets you connect to a device using SSH or Telnet. HiView attempts to connect to a device using SSH first. When HiView cannot connect to a device using SSH, HiView attempts to connect to the device using Telnet. To access a device using the Command Line Interface (CLI), perform the following steps:

▶ Tile view
- ☐ To view the context menu, right-click the tile with the desired device.
- ☐ Click the “Open CLI connection“ button.

▶ Table view
- ☐ To view the context menu, right-click the table row of the desired device.
- ☐ Click the “Open CLI connection“ button.

As an alternative HiView lets you start the CLI using the “URL“ field, in both the Tile view and the Table view. To access a device using the “URL“ field, perform the following steps:
- ☐ Enter a device IP address in the “URL“ field.
- ☐ Click the “Open CLI connection“ button.

Note: To help provide secure communications, use SSH and disable Telnet on the device.

Note: If your computer is connected to the device through a firewall, enter a rule in the firewall that allows the data traffic through port 22 (SSH) or port 23 (Telnet).

Displaying a certificate

Hirschmann devices usually have certificates for the Web application (jar file). Depending on the device you access, the connection also has a certificate.
- ☐ To view the certificates of HiOS devices, with a software version lower than 7.0, select in the graphical user interface of the device `Tools >` Retrieve Product.
- ☐ To view the certificates of the HiOS devices, with software version 7.0 or higher, open the certificate in the web browser.

3.1.7 Connecting to Industrial HiVision

Using HiView, you can start the Industrial HiVision GUI without installing Industrial HiVision. You can use the URL connection to Industrial HiVision to monitor the status of your network. This function offers you a limited version of the Industrial HiVision GUI.

To establish a connection to the Industrial HiVision “Web server“, in the Industrial HiVision `Preferences > Advanced > Services (Access)` dialog, perform the following steps:

☐ Mark the `Web server > Web server` checkbox.
☐ Mark the `Project Data Server > Remote Access` checkbox.
☐ Record the following settings:
- `Web Server > Protocol`
- `Web Server > Port`
- `Project Data Server > Port`
  Starting with Industrial HiVision release 8.0, you can change the value of the `Project Data Server > Port`. Record this value if you changed the default port value. If you changed the `Project Data Server >` Port from the default port value, then it is necessary to connect to the configured port.

Note: You can find the default port values in the Industrial HiVision manual, chapter A.5 “Ports used“.

Perform the following steps in the HiView `Devices` tab.

In the following examples, these values are used:

▶ The `Web Server > Protocol` is `https`.
▶ The IP address of the network management station is `10.0.1.159`.
▶ The `Web Server > Port` is `11194`.
▶ For the second example, the `Project Data Server > Port` was changed to `10000`.

When the `Project Data Server > Port` is set to the default port value, perform the following steps:

☐ In the “URL“ field, enter the following information: `Web Server >` Protocol`://Management Station IP Address:Web Server > Port`.
For example, `https://10.0.1.159:11194`.
☐ Press the “Return“ key.

When you changed the `Project Data Server > Port` from the default port value, perform the following steps:

- ☐ In the “URL“ field, enter the following information: `Web Server > Protocol ://Management Station IP Address:Web Server > Port?project-data-port=Project Data Server > Port`.
  For example, `https://10.0.1.159:11194?project-data-port=10000`.
- ☐ Press the “Return“ key.

Note: The Web server port value that Industrial HiVision uses is version-dependent. You find the port that Industrial HiVision uses in the settings under `Preferences > Advanced > Services`.
Starting with Industrial HiVision version 7.0 you find the current port number in the `Preferences > Advanced > Services Access` dialog.

3.2 Discovery Tab

The Discovery tab allows you to search for devices in your network. The tab also allows you to specify the IP parameters for the devices. The tab also allows you to configure the devices using a web browser, Telnet or SSH.

The Discovery tab is compatible with devices that support HiDiscovery v2.
- Classic Switches since version 09.0.01
- HiOS since version 05.0.00
- HiSecOS since version 03.0.00

3.2.1 Discovery Tab Visibility

If you do not have devices in your network that support HiDiscovery v2 then HiView allows you to hide the Discovery tab.

To hide the Discovery tab proceed as follows:
- ☐ Start HiView.
- ☐ In the menu bar, click `Preferences > Options`.
- ☐ Unmark the `Display Discovery tab` checkbox.
- ☐ Click the `Close` button.
- ☐ In the menu bar, click `File > Exit`.
- ☐ Restart the HiView program.

3.2.2 HiDiscovery v2

HiDiscovery v2 is a primary setup tool based on the SNMPv2 protocol. After you select the network adapter and click the `Refresh` button, the `Discovery` tab displays a line for every device that responds to a HiDiscovery v2 inquiry.

Note: After you have assigned the IP parameters, it is recommended that you disable the HiDiscovery v2 function in the Network dialog of the device.

To disable the HiDiscovery v2 function, use the following work steps:
☐ Open the `Devices` tab.
☐ Log on to the device by double-clicking on the device entry.
☐ Open to the Networks dialog.
☐ In the HiDiscovery v2 frame, click the `Off` radio button.
☐ Save the configuration on the device.

Note: When using HiDiscovery v2 to search for devices behind a firewall, configure the firewall to forward UDP packets on port 51973.

3.2.3 Network Adapter

The `Discovery` tab uses the first network interface found for the computer. When your computer has several network cards, you can select the one you desire in the adapter field at the bottom of the tab. To scan your network with the available network cards, select “Every Network Interface“.

When the `Adapter` field does not display an adapter, verify that the IPv4 Ethernet Property in the network settings on the HiView host are enabled.

Note: If you change the network interface parameters of the computer, then restart HiView.

3.2.4 Signaling a Device

The `Discovery` tab allows you to identify the devices displayed in the list.

☐ To set the LEDs to flashing for the selected device, mark the `Signal` checkbox.
☐ To stop the flashing, unmark the `Signal` checkbox.

3.2.5 First time log on (Password change)

The `Discovery > Password Change` column displays devices for which it is necessary to change the default password. If the checkbox in the `Password Change` column contains a mark, then the device still has the default password configured. The Password change function is only available for devices that support the HiDiscovery v2 protocol, see "Password change during first time log on" on page 6.

Example configuration

To change the default password on a device proceed as follows:
☐ Open the `Discovery` tab.
☐ Select a device which has a marked checkbox in the `Password Change` column.
☐ Right-click on a selected device.
☐ In the context menu select the `Change Password` option.
☐ In the `Change Password > New password` field, type in the password that you want to use to access the device.
☐ You can use the following methods to verify your password:
  – Mark the `Show Password` checkbox. The `New password` field displays the password in plain text.
  – Type in the same password in the `Confirm password` field.
☐ Click the `OK` button.

Note: You can change the password on several devices at the same time. For security reasons, it is recommended that each device has a different password.

3.2.6 IP address management

The `Discovery` tab displays which IP addresses are configured on your devices. When a device has both an IPv4 and IPv6 address assigned to it, you can select which address HiView uses to connect to the device. The addresses displayed in the `IPv6 Address (Link Local)` column are local addresses. The devices use Link-local addresses only to communicate within the network segment or broadcast domain.

To select which IP address HiView uses to communicate with the device proceed as follows:

☐ Open the `Discovery` tab.
☐ In the tool bar, select `Preferences > Options`.
☐ In the `Options` dialog, activate the radio button for the preferred version.

3.2.7 Device access

When you access a device for the first time using HTTPS, HiView displays the Security Alert dialog containing the host key fingerprint. Verify that the dialog contains the correct key for the device which you are attempting to access.

Right-clicking on a device row in the table displays a drop-down list with the following functions:

Configure

The Configure function opens the Discovery Configuration dialog which allows you to specify the IP parameters and name of a device.

Note: After you make changes to the parameters in the Discovery Configuration dialog, the changes are only saved in the running configuration. To save the changes in the permanent memory, use the Load/Save function in the Graphical User Interface of the device.

GUI

The GUI function opens the graphical user interface of the device which allows you access to the device configuration.

Note: If you use your computer to connect to the device through a firewall, enter a rule in the firewall that allows the data traffic through port `161`.

GUI / Add to devices

The GUI / Add to devices function opens the graphical user interface of the device and adds the device to the Devices tab.

SSH/Telnet

The “SSH/Telnet“ function allows you to remotely login to the Command Line Interface (CLI) of the device using an encrypted network protocol. HiView attempts to connect to a device using SSH first. When HiView cannot connect to a device using SSH, HiView attempts to connect to the device using Telnet.

To help provide secure communications, use SSH and disable Telnet on the device.

The prerequisite for an SSH connection is that the SSH server using SSHv2 is enabled in the device.

Note: If your computer is connected to the device through a firewall, enter a rule in the firewall that allows the data traffic through port 22 (SSH) or port 23 (Telnet).

Note: To help provide secure communications, use SSH and disable Telnet on the device.

Ping

The Ping function allow you to test the reachability of a device in an IP network. The function also measures the round trip time of the ICMP echo request and reply.

4 HiView Applet Launcher

When you install the HiView program, the Applet Launcher is added to the installation directory. You can find the Applet Launcher in the HiView installation directory.

You can use the Applet Launcher in conjunction with other external programs. Calling the Applet Launcher from an external program lets you open the Graphical User Interface (GUI) of a device.

HiView for example, uses the Applet Launcher to open the Graphical User Interface of a device. After you open a supported device with HiView, it stores the device information and displays the device.

4.1 Starting the Applet Launcher

To start the Applet Launcher, perform the following steps:

- ☐ Open a command window.
- ☐ Change the directory to the HiView installation directory.
  For example, if the installation directory is the default installation directory, then enter the following command:
  `cd/d C:\Program Files\Hirschmann\HiView 4.2`
- ☐ Enter `AppletLauncherCmd.exe` on the command line.
- ☐ Press the `Return` key.

Note: The Applet Launcher is also available for Linux users. To start the Applet Launcher with the Linux operating system, open the HiView root directory and start the `AppletLauncher.sh`.

After you press the `Return` key, the command window displays the `Usage` line and descriptions of the available arguments. On the `Usage` line the arguments in brackets, “`[]`” are optional.

The following list contains further description of the available arguments:

- `-address`
  - http[s]
    This argument is optional. Enter the protocol over which you wish to communicate with the device. If you do not specify a value for this argument, then the Applet Launcher attempts to communicate with the device over HTTPS. If the Applet Launcher cannot communicate with the device over HTTPS, then it attempts to communicate with the device over HTTP.

    Note: When the Applet Launcher uses HTTP, it transmits passwords in plain text.

  - IP address
    This is the only mandatory argument. This value is the IP address of the device.
  - Port
    The TCP web port of the device for example, 80 = HTTP, 443 = HTTPS. If you changed the web port of the device, then enter the web port in the command. Otherwise, this argument is optional.
  - ?Param=Value[&Param=Value]
    The URL query `project-data-port` parameter is used to connect to Industrial HiVision. See “Connecting to Industrial HiVision” on page 23.
- `-user`
  This argument is optional. Enter the login user name for the device. This argument is used for the auto-login function. Use this argument only in combination with the password argument.
- `-password`
  This argument is optional. Enter the login password for the device. This argument is used for the auto-login function. Use this argument only in combination with the user argument.
- `-locale`
  This argument is optional. This argument is used to specify the GUI language of the device. The possible values are `en` for English, and `de` for German.

4.1.1 Open a device with the Applet Launcher

The following example describes how to enter arguments in the command line to open the login dialog of a device.

In the following example, these values are used:
- The protocol is omitted from the command line. The Applet Launcher attempts to communicate with the device over HTTPS.
- The IP address is `123.45.67.89`.
- The desired GUI language is `English`.

To open the login dialog of a device, enter the values in the command line as follows:

```
AppletLauncherCmd.exe -address 123.45.67.89 -locale en
```

4.1.2 Auto-Login

You can use the Applet Launcher to automatically login to the device.

The following example describes how to enter arguments in the command line to automatically login to a device. The web port on the device was also changed.

In the following example, these values are used:
- The protocol with which the Applet Launcher communicates with the device is `https`.
- The IP address of the device is `123.456.78.90`.
- The web port was changed to `5000`.
- The user name is `admin`.
- The password is `private`.
- The desired GUI language is `English`.

To automatically login to a device, enter the values in the command line as follows:

```
AppletLauncherCmd.exe -address https://123.456.78.90:5000 -
user admin -password private -locale en
```

5 Saving an individual configuration

HiView allows you to create configurations for particular application cases in the `.hvw` format and to save them to a location of your choice. Thus, you determine which devices the `Devices` tab displays. Application examples are a network related device selection and a selection on the basis of device families.

☐ To save an individual configuration, select `File > Save as`.

☐ To open an individual configuration, select `File > Open`.

6 Delete cache directory

When establishing a connection to a device, HiView loads the device-specific application into the cache directory of your HiView folder.
When you are setting up the connection to this device again, the device-specific application saved in the cache directory keeps you from having to wait for a reload.
In order to free memory space on your storage medium, HiView allows you to delete the cache directory completely or in part.

☐ Select `Preferences > Cache`.
HiView displays the “HiView - Cache” dialog.

☐ Select the devices which you want to delete from the cache directory.

☐ Click the `Delete` button.

7 Devices in the Hirschmann Application Lab

HiView allows you to access a selection of devices in the Hirschmann Application Lab through the Internet. These devices allow you to familiarize yourself with the graphical user interface of the devices.

☐ Select `File > Hirschmann Application Lab`.

8 Maintenance

Hirschmann is continually working on improving and developing our software. You should regularly check whether there is a new version of the software that provides you with additional benefits.
You will find information about updates and upgrades on the Internet pages of Hirschmann Automation and Control GmbH.
www.beldensolutions.com

A Tested products and software versions

The HiView Devices tab has been tested and is compatible with the following devices and software versions:

Note: The * symbol entered next to the version means the software version, and later versions, support the HiDiscovery v2 protocol.

Products with “Classic Switch Software”

- EAGLE20
  05.4.00*
  05.3.02
- MACH100 L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MACH100GE L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MACH1000 L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11

- MACH1000GE
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MACH1000GE L3P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MACH3000
  3.46
- MACH4000 L2P/L3E
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MACH4000 L3P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MACH40XG L2P/L3E/L3P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MS20/30 L2E
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- MS20/30 L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11

- Octopus OM L2E
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- Octopus OM L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- Octopus OS L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- PowerMice L2P/L3E/L3P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- RS20/30/40 L2E/L2P
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11
- RSB
  05.3.09*
  05.3.03
- RSR
  09.1.00*
  09.0.16*
  09.0.04*
  08.0.11

Products with software “HiOS” / “HiSecOS”

- BRS
  08.1.00*
  07.4.01*
- EAGLE20 Ruggedized
  03.3.00*
  03.0.00*
  02.0.01
  01.0.00
- EES (EES-PRP)
  07.1.00*
  07.0.06*
  06.1.00*
  06.0.02*
  05.0.03
  04.0.04
  03.0.04
- EES-HSR, EES-MRP
  02.0.03
- GRS1020/30
  08.1.00*
  07.0.06*
  06.1.00*
  06.0.02*
  05.0.03
  04.0.04
- MSP30
  08.1.00*
  07.0.06*
  06.1.00*
  06.0.02*
  05.0.03
  04.0.04
  03.0.04
- MSP40
  08.1.00*
  07.0.06*
  06.1.00*

- RSP (RSP-MRP, RSP-PRP)
  08.1.00*
  07.0.06*
  06.1.00*
  06.0.02*
  05.0.03
  04.0.04
  03.0.04
- RSP-HSR
  08.1.00*
  05.0.03
  04.0.04
  03.0.04
- RSPL
  07.1.00*
  07.0.06*
  06.1.00*
  06.0.02*
  05.0.03
  04.0.04
  03.0.04
- RSPS (RSPS-HSR, RSPS-MRP, RSPS-PRP)
  07.1.00*
  07.0.06*
  06.1.00*
  06.0.02*
  05.0.03
  04.0.04
  03.0.04
- Octopus OS2-37
  07.1.00*
  04.1.02
- Octopus 3
  08.1.00*
- Dragon
  08.1.00*

B Index

A
Applet signature certificate 19

B
Barrier-free 5
BAT devices 15

C
Cache 15, 37
Certificate 22
Configuration file 10, 11

D
Device Password 27
Disk space 8

F
FAQ 49
Fingerprint Verification 19
Firewall 26

H
HTTPS certificate 19

I
IP Address 28

J
Java error 14

L
Language 10, 11
License conditions 10, 11
Linux 11

M
Memory space 37
Monitor resolution 8

P
Portable 5
Processor 8
Product certificate 22
Program window 15, 19

R
RAM 8

S
SD Card 10, 11, 12
Stand-alone 5
Storage medium 37
System requirements 8

T
Table view 18
Technical questions 49
Tile view 16
TLS Protocols 15
Training courses 49

U
UDP Port 26
Update 41
URL 15, 23
USB stick 5, 10, 11, 12

W
Windows 10, 12

Z
Zip file 10, 11, 12

C Further support

Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at http://www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at https://hirschmann-support.belden.com.

This site also includes a free of charge knowledge base and a software download section.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at https://www.belden.com/solutions/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against making any compromises in any case. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
https://www.belden.com/solutions/customer-innovation-center

HIRSCHMANN

A BELDEN BRAND