HIRSCHMANN
A BELDEN BRAND

User Manual

Network Management System
Industrial HiVision 8.4

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.

© 2023 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

Contents

1 The Management Tool 13

1.1 Integration of third-party devices 14

1.2 Enhanced auto-topology discovery 15

1.3 MultiConfig™ for network installation 16

1.4 MultiConfig™ for live operation 17

1.5 Engineered through experience 18

1.6 30 days free trial 19

1.7 Third Party Libraries 20

2 Software Overview 23

2.1 System Requirements 24

2.2 Installation 25

2.2.1 Downloading the Industrial HiVision software 27

2.2.2 Installation under Windows 28

2.2.3 Installation under Linux 29

2.3 Update 33

2.3.1 Updating under Windows 33

2.3.2 Updating under Linux 34

2.4 Maintenance 35

2.5 Starting 36

2.5.1 Starting under Windows 36

2.5.2 Starting under Linux 37

2.6 Deinstallation 39

2.6.1 Deinstallation under Windows 39

2.6.2 Deinstallation under Linux 39

3 Preparation 41

3.1 Improving the security of Industrial HiVision 42
3.1.1 Physical protection 43
3.1.2 Measures before and during the installation of Industrial HiVision 43
3.1.3 Industrial HiVision configuration actions 46
3.1.4 Restrict File Access 51

3.2 Outside the program 52

3.3 Network structure 53
3.3.1 Advantages of the hierarchical network structure 53
3.3.2 Application Example 54
3.3.3 Configuration of the application example 56
3.3.4 Status display of the subdomains 58

3.4 Program default settings 59

3.5 Using Industrial HiVision with Firewalls 62

3.6 Fingerprint verification 65

4 Interface of the program 71

4.1 Main window of Industrial HiVision 72

4.2 Menu bar 74
4.2.1 File 75
4.2.2 Edit 76
4.2.3 View 77
4.2.4 Configuration 78
4.2.5 Tools 81
4.2.6 Help 82

4.3 Tool bar 83
4.3.1 Edit Mode 84
4.3.2 Preferences 88

4.4 Event line 89
4.4.1 Number of events 90
4.4.2 Types of events 91
4.4.3 Acknowledge events 92
4.4.4 Properties of an event 93

4.5 Folder frame 94
4.6 Navigation field 96
4.7 Detail display 97
4.7.1 Map 97
4.7.2 List 98
4.7.3 Devices 100
4.7.4 Ports 102
4.7.5 Connections 104
4.7.6 Properties 106
4.7.7 Security Status 107
4.7.8 PoE 108
4.8 Event list 112
4.8.1 Event History 115
4.9 To navigate with the Keyboard 119
4.9.1 Navigating in a table 119
4.9.2 Changing the frame 119

5 Creating a network plan 121

5.1 Device detection 122
5.1.1 Device Icons 125
5.1.2 TXCare 125
5.2 Assigning device icons 128
5.3 Device arrangement 130
5.3.1 Creating a network plan 130
5.3.2 Moving devices into the network plan 131
5.3.3 Creating new devices 132
5.3.4 Arrange devices in the detail display 133
5.3.5 Naming devices and ports 134
5.3.6 Copying devices 134
5.3.7 Paste as new Network 135
5.3.8 Devices with multiple IP addresses 138
5.3.9 Creating a link 139
5.4 Device connection 140
5.4.1 Automatically displaying the topology 140
5.4.2 Connecting devices manually 141

5.4.3 Reshaping a connection line 141
5.4.4 Specifying the line thickness 142
5.4.5 Other connections 143
5.4.6 Detecting a link to another folder 143
5.4.7 Specifying connection properties 144
5.4.8 Link types 145
5.4.9 Representation of the connection medium 146

5.5 The Network changing over time 147
5.5.1 Adding devices with HiDiscovery V1 147
5.5.2 Adding devices with network scan 148
5.5.3 Adding devices manually 148
5.5.4 Startup procedure for Hirschmann devices 149
5.5.5 Interrupting device monitoring 150
5.5.6 Removing devices 150
5.5.7 Exchanging devices 150

5.6 Network Documentation 152
5.6.1 Saving Industrial HiVision projects 152
5.6.2 Saving reporting data 152
5.6.3 Exporting the content of the detail display 153
5.6.4 Printing the content of the detail display 153
5.6.5 Exporting the event list 153
5.6.6 Printing the event list 154
5.6.7 Creating device documentation 154
5.6.8 Printing or exporting the status configuration 155
5.6.9 Agent 155

6 Configuring the network 157

6.1 Using the dialog box 159
6.1.1 Description of the menu tree 160
6.1.2 Description of the object frame 160
6.1.3 Description of the function frame 161
6.1.4 Description of the control elements 163

6.2 Examples for using the MultiConfig™ 164
6.2.1 Same contact person on multiple devices 164
6.2.2 Software update on similar devices 166
6.2.3 Restarting multiple devices 167

6.2.4 Loading/saving the configuration for multiple devices 168
6.2.5 Configuring an SNMPv1 trap destination on multiple devices 170
6.2.6 Configuring SNMPv3 traps 171
6.2.7 Make firewall rules on multiple devices 173
6.2.8 Configuring the Industrial HiVision property 176
6.2.9 Saving reference values for each device 177
6.2.10 Password synchronization 177
6.2.11 MultiConfig™ Search Function 178
6.2.12 MultiConfig™User Management 179
6.2.13 MultiConfig™ Time Sensitive Networking 183
6.2.14 Configure polling of device properties 192
6.2.15 Zero Touch Device Replacement 194

7 Monitoring the network 199

7.1 Improving security on the network 200
7.1.1 Password-protecting devices on your network 200
7.1.2 Password change during first time log on 201
7.1.3 Security status view and configuration 204
7.1.4 Security-related settings of devices on the network 208
7.1.5 Configuring security-relevant settings on the network 210

7.2 Status configuration 214

7.3 Status determination 215
7.3.1 Trap destination address 216
7.3.2 Updating device status 216

7.4 Status propagation 217

7.5 Management actions 219
7.5.1 Event actions 219
7.5.2 Time-linked actions 220
7.5.3 Industrial HiVision “I'm alive” event 220

7.6 Time-related recordings 221
7.6.1 History 221
7.6.2 Reports 222

7.7 User-defined properties 225
7.7.1 Description of user-defined properties 225
7.7.2 Application example for user-defined properties 225
7.8 Effect on system resources 228
7.8.1 Detecting utilization of system resources 229
7.8.2 Influencing utilization of system resources 230
7.8.3 Minimizing polling 231
7.8.4 Minimizing network load 232
7.9 Process visualization systems 233
7.9.1 Link to process visualization system 233
7.9.2 Structure of the transfer data for OPC 235
7.9.3 Supported applications OPC DA 237
7.9.4 Supported applications OPC UA 238
7.9.5 OPC UA Connection Example 239
7.9.6 OPC UA Server Custom Certificates 241
7.10 Remote access to Industrial HiVision 244
7.10.1 Web access to Industrial HiVision 244
7.10.2 Certificate for the HTTPS connection 247
7.11 Interface to InfluxDB® and Grafana® 250
7.11.1 Configure InfluxDB® and Grafana® 250
7.11.2 Import the Grafana® dashboard templates 253
7.11.3 Security 254

8 References 255

8.1 File 256
8.1.1 New Project 257
8.1.2 New 257
8.1.3 Login 259
8.1.4 Open... 259
8.1.5 Save 259
8.1.6 Save as... 260
8.1.7 Save Backup 260
8.1.8 Load Backup 261
8.1.9 Export... 262
8.1.10 Export Events... 262

8.1.11 Print 263
8.1.12 Print Events 263
8.1.13 Exit and Stop Service 263
8.1.14 Exit 264
8.2 Edit 265
8.2.1 Undo 265
8.2.2 Redo 265
8.2.3 Edit Mode 265
8.2.4 Switch to the free version 266
8.2.5 Cut 266
8.2.6 Copy 267
8.2.7 Paste 267
8.2.8 Paste as Link 267
8.2.9 Delete 268
8.2.10 Rename 268
8.2.11 Select All 268
8.2.12 Acknowledge Status Change 268
8.2.13 Manage 269
8.2.14 Unmanage 269
8.2.15 Set Device and Port Names 269
8.2.16 Set Default Device Icon 270
8.2.17 Device Documentation 270
8.2.18 Drawing Size 270
8.2.19 Background Image 271
8.2.20 Find... 272
8.2.21 Auto Topology... 273
8.2.22 Auto Layout 277
8.2.23 Properties of a folder/device 278
8.2.24 Properties of a component detail 285
8.2.25 Properties of a connection 292
8.2.26 Adding a component detail to a port 294
8.2.27 Add to reporting 295
8.2.28 Device and Port Signaling 297
8.3 View 299
8.3.1 Select VLAN 299
8.3.2 Refresh VLANs 299

8.3.3 Protocol Statistics 300
8.3.4 Filter Events for Object 301
8.3.5 Back 302
8.3.6 Forward 303
8.3.7 Up 303
8.3.8 Home View 303
8.3.9 Set Home View Settings 304
8.3.10 Geographical Location View 304
8.3.11 Zoom 305
8.4 Configuration 306
8.4.1 Monitor 306
8.4.2 PSM Manager 308
8.4.3 Reporting 309
8.4.4 Export to InfluxDB® 313
8.4.5 Scheduler 314
8.4.6 Preferences 321
8.5 Status Configuration 404
8.6 Scan Ranges 406
8.7 User defined Properties 408
8.7.1 Creating a new user-defined property 408
8.8 MultiConfig™ 410
8.8.1 Power Limit 410
8.9 MAC/IP List 412
8.9.1 MAC/IP Addresses 412
8.9.2 MAC/IP Address Pair Security 413
8.10 Refresh 414
8.11 IP Configuration 415
8.12 SNMP V1 Trap Destination 417
8.13 Tools 419
8.13.1 Dashboard 419
8.13.2 Web Interface 436
8.13.3 Device Configuration 437
8.13.4 CLI 438
8.13.5 SNMP Browser 439
8.13.6 Ping 439

8.13.7 HiDiscovery Scan 439
8.13.8 Scan Network 440
8.13.9 Demo Network 441
8.13.10Calculate Availability 442
8.14 Help 448
8.14.1 Online Help F1 448
8.14.2 Tutorial 448
8.14.3 Online 449
8.14.4 Kernel Info 449
8.14.5 About 450

A Appendix 453

A.1 FAQ 454
A.2 Monitored properties 455
A.2.1 Monitored properties in the basic setting 455
A.3 CSV export 457
A.3.1 Microsoft Excel before 2010 457
A.3.2 Microsoft Excel 2010 458
A.4 Language support 459
A.5 Ports used 460
A.6 Maintenance 461
A.7 Literature references 462
A.8 Copyright of Integrated Software 463

B Index 464

C Further support 469

D Readers' Comments 470

1 The Management Tool

Wherever individual network components are to be combined to create an overall system, Industrial HiVision 8.4 is the ideal solution for configuring and monitoring the administrable Hirschmann devices, including switches, routers, and EAGLE 20/30/40 firewalls, wireless BAT units and products from various manufacturers.

Designed for effective industrial supervision, Industrial HiVision can be easily integrated into SCADA applications. It offers a built-in SNMP to OPC server.

1.1 Integration of third-party devices

Of course, network management software from a specific manufacturer of network components is optimized for operating these components. In comparison, a generic, manufacturer-independent network monitoring system will only provide superficial product integration.
However, in the real world, networks are usually a heterogeneous environment with devices from multiple manufacturers.

Industrial HiVision makes it easier for the network administrator to also integrate non-Hirschmann products, as long as they are administrable. This applies to components of the network infrastructure as well as field devices. Managed products have a range of standard characteristics that can be monitored, such as the device status. In addition, the direct standard interface can be used to enter further device-specific information, such as the long-term history and status messages. You decide for yourself how detailed the monitoring of your application is to be.

Advantages:
- Monitoring and trend mapping for administrable devices from any manufacturer
- Status display for your entire system
- Comprehensive network monitoring using a single network management system.

1.2 Enhanced auto-topology discovery

To monitor an industrial network reliably, precise knowledge of the network topology is essential. The network administrator should know how and where which devices are linked to each other in order to manage a complex network efficiently and perform any maintenance measures that are required.

Existing customers are already familiar with the intuitive Industrial HiVision user interface.
This allows rapid visualization of the network topology. The standardized LLDP protocol is used to scan network infrastructure components and the received information allows Industrial HiVision to build a representation of the network connectivity. End devices such as PLCs, I/O, and HMIs are also detected and their location is accurately depicted on the graphical topology map.

Industrial HiVision software enables you to detect unmanaged switches and hubs and display their position within your network diagram. The software is also able to determine the network topology of devices which are located behind a router. This results in an increased level of topology detail.

Because industrial networks evolve over time, documentation can easily become out of date. The auto-topology discovery function assists you to know what is connected where in your network.

Key benefits:
- Network maps are created automatically, without manual intervention
- Topology maps are very accurate
- Network documentation is up to date

1.3 MultiConfig™ for network installation

Many network infrastructure devices require identical configuration parameters. But those parameters will differ from one network to the next.
Which redundancy protocol is required?
What is the temperature threshold of the devices?
Where is the time server located?
Should the web interface be disabled for live operation?
To which management station should alarms be sent?
Should unused ports be disabled?
The list goes on and on.

Configuring devices individually is a tedious task. A misconfiguration on a single device can be very difficult to find. As a result, Site Acceptance Tests will be prolonged or the network may be inoperable. MultiConfig™ helps prevent these issues from happening.
The configuration tool allows you to configure the same parameters across multiple devices simultaneously and it also shows you where there is an inconsistency between parameter configurations. It works across different types of devices, where those devices have parameters in common.
MultiConfig™ allows you to save multiple device configurations, both locally and to a server, without touching each device individually.

Key benefits:
- Reduced network installation time
- Network infrastructure configuration consistency

1.4 MultiConfig™ for live operation

Throughout a network's lifetime operation, it is necessary to carry out repetitive but essential maintenance tasks. The threat of cyber attacks means that responsible network administrators will change device passwords regularly. Technology innovations can have great benefits for your network and your company, but to take advantage of them you will need to update your device firmware. And in the worst case scenario, if your network breaks down, your support organization will need immediate access to the current configuration files and event logs of your network devices.

Of course, for a small network, the above can be done by accessing each device individually. But for both small and large industrial networks, network security and availability are the ultimate goals. MultiConfig™ can fulfill the above requirements with a few clicks of a mouse. As a result, network administrators can meet their daily objectives with less effort and minimal disruption.

Key benefits:
- Highest network availability.
- Least effort required for network administration and maintenance.
- Minimized operational disruption.

Note: If you change user access parameters on a device that contains identical SNMP, WEB- and CLI access parameters, then the changes are applied simultaneously to the 3 access modes.

1.5 Engineered through experience

Industrial HiVision 8.4 is the fourth generation network management software from Hirschmann. We have built on our experience with previous releases to evolve a product which is unique in the industrial space. Industrial HiVision 8.4 encompasses the features and benefits of earlier versions. These include:

Key benefits:
- Client/Server architecture
- Web browser client
- Edit and Run modes
- Network hierarchy display
- Global and individual status display and propagation
- Flexible event handling
- Customizable data acquisition
- Long-term trending
- Comprehensive export functions
- Asset Management

1.6 30 days free trial

As a network administrator, you need cutting edge tools to help you meet your targets. Hirschmann is famous for innovation. We are committed to evolving Industrial HiVision to match our new hardware functionality, meet the requirements of our customers, and exceed the demands of the Industrial Ethernet marketplace.
Everybody knows, seeing is believing. Words cannot do justice to network management software. Download Industrial HiVision, and test it free of charge for 30 days at your convenience. Longer evaluation periods are available on request.
The current version 8.4 of Industrial HiVision is available for download at www.belden-solutions.com.

1.7 Third Party Libraries

Copyright (c) 2007-2008 Trilead AG (http://www.trilead.com)

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a.) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b.) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

c.) Neither the name of Trilead nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trilead SSH-2 for Java includes code that was written by Dr. Christian Plattner during his PhD at ETH Zurich. The license states the following:

Copyright (c) 2005 - 2006 Swiss Federal Institute of Technology (ETH Zurich), Department of Computer Science (http://www.inf.ethz.ch), Christian Plattner.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a.) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b.) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

c.) Neither the name of ETH Zurich nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Java implementations of the AES, Blowfish and 3DES ciphers have been taken (and slightly modified) from the cryptography package released by “The Legion Of The Bouncy Castle”.

Their license states the following:

Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle (http:// www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal In the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

2 Software Overview

This chapter describes the following topics:

- The prerequisites for installing and operating the software
- Installing the software
- Updating the software
- Maintaining the software
- Starting the program
- Deinstalling the software

You will find requirements for operating the software in the appendix (see on page 24 “System Requirements”).

Note: Regarding security:
Industrial HiVision helps to protect the edit mode of the user interface by requesting a password.
When you login to your network management station as an administrator and start the user interface of Industrial HiVision, then Industrial HiVision allows you to switch directly to the “Edit Mode“. You can thus avoid having to enter a password.

Note: Regarding security:
The Industrial HiVision database contains the information for your Industrial HiVision project.
Hinder the access to this file by means of selected access rights for the directory `<installation directory>\database`.

2.1 System Requirements

You can find a detailed description of the system requirements in the readme file.

License

License keys for Industrial HiVision depend on the number of devices you want to monitor.
You can get license keys for 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096 devices.

2.2 Installation

Industrial HiVision consists of a number of components. A service performs a large part of the work in the background.

This service has a close connection to a database containing the relevant data for the settings of Industrial HiVision and the devices to be monitored. When you reboot Industrial HiVision, Industrial HiVision gets the configuration data from the database which were current when you last quit the program.

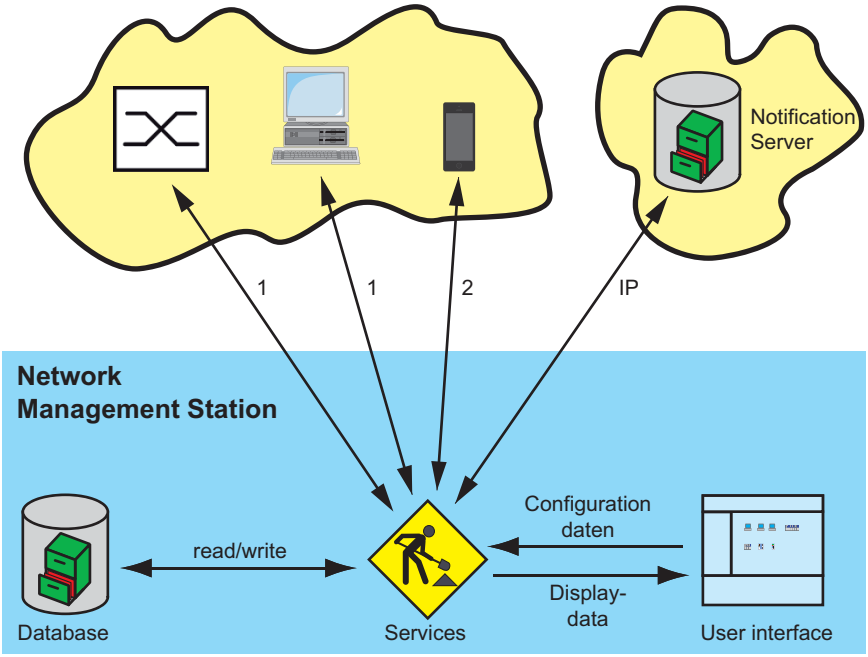


Figure 1: Architecture
1 - SNMP Get/Set/Trap, HiDiscovery V1, Ethernet/IP, Modbus/TCP, Ping, HTTP, HTTPS,
2 - HTTP, HTTPS

The program Industrial HiVision, which you call up directly on the screen, maintains a connection with the background service, from which it gets the required data.

You can install Industrial HiVision additionally to a former release of Industrial HiVision. If you start different releases simultaneously each release maintains a connection to its own background service.

Industrial HiVision enables you to install the following features on different computers:

- the user interface (Industrial HiVision Client)

  Note: For Windows 10 users. If you install Industrial HiVision as a client, then it is possible that client access is denied. To correct this, give the user read permission to the <Installation directory>\lib folder.

- the service with the database (Industrial HiVision Server)

You can thus access a central network management station from different locations with multiple user interfaces. The number of user interfaces that can access a central network management station depends on the capacity of the network management station. To avoid access conflicts, only one user interface can access a network management station in the “Edit Mode“ (see on page 370 “Program Access”).

However, you can access multiple decentralized Industrial HiVision servers with one user interface.

Note: Installing an external firewall with NAT between the service and the user interface:
In the external firewall you activate port forwarding for the connection port in the service direction for the following ports:

- 11209, Industrial HiVision proxy server for the communication between the service and the user interface.
- 11208, Industrial HiVision Web server to also open the user interface in the browser.

(see on page 374 “Services Access”)

Note: Industrial HiVision writes events (see on page 112 “Event list”) with dates and times in the database. The time written refers to the time in the system on which the service is running. When you start the user interface on a computer in a different time zone, Industrial HiVision displays the event times in the time zone of the computer on which the service is running.

2.2.1 Downloading the Industrial HiVision software

To install Industrial HiVision on your computer, perform the following steps:

- ☐ Open the website: hirschmann-support.belden.com/en/login
- ☐ When you have an account, login to your account. To make an account, click the `Register` button.
- ☐ Select the software link that best suits your needs.
- ☐ Click the `Download` button.
- ☐ After you read the End User License Agreement (EULA), click the `I Agree` button.
- ☐ Extract the files located in the downloaded ZIP file to a temporary folder.

Note: Before you install the software, compare the sha256 hash on the web page with the sha256 hash calculated from the zip file. Use the Windows utility "certutil" to calculate the sha256 hash. In the cmd window navigate to the file location, then enter the following command:

```
CertUtil -hashfile path\file_name.ext SHA256
Example: CertUtil -hashfile C:\Industrial_HiVision.zip SHA256
```

2.2.2 Installation under Windows

- ☐ Download and extract the Industrial HiVision files as described in “Downloading the Industrial HiVision software” on page 27.
- ☐ Navigate to the location of the extracted Industrial HiVision files.
- ☐ For Windows computers, double click the ihivision8.4_windows.exe file.
- ☐ In the `Open File - Security Warning` dialog, click the `Run` button.
- ☐ 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.

Note: If you get the message `Error during installation of ikernel.exe`, this means that the user does not have any administration rights.

Depending on your selection, the installation assistant installs the following items:

- ▶ the Hirschmann Industrial HiVision 8.4 Service with integrated database (= Industrial HiVision Server)
- ▶ OPC services
- ▶ the Industrial HiVision Client (= user interface) program

If you want to connect to a SCADA system, you need the OPC services on the Industrial HiVision server installed.
OPC services function as the data source for SCADA systems.

To perform a HiDiscovery V1 scan, Industrial HiVision requires the WinPcap program.
During the installation of Industrial HiVision, Industrial HiVision checks whether the version of WinPcap installed on your PC fulfills the requirements of Industrial HiVision. If not, you agree to the installation of WinPcap using the installation wizard.

During the installation, you can select how the Hirschmann Industrial HiVision 8.4 Service starts from the following options:

- ▶ start automatically each time the computer is rebooted
- ▶ start manually when the program starts

Note: You will find the status of the service in Windows 2008 R2, Windows Server 2012 R2, under `Start:Control Panel:Administration Tools:Computer Management:Services and Applications:Services.` Here you can also terminate the service and restart it.
If you are running other resource-intensive programs on the computer, then close the Industrial HiVision program and the “Hirschmann Industrial HiVision 8.4 Service”. This service requires considerable computer resources. When it starts, the Industrial HiVision program asks you whether you want to start the service. When you select `File > Exit and Stop Service` to leave the program, the Industrial HiVision program asks you whether you want to close the service.
Note that when the service is switched off, there is no network monitoring, which means that no events are recorded.

Note: In the default setting of the service properties on the “Logon” tab, no data exchange between the service and the GUI is permitted for the local system account (`Start:Control Panel:Administration Tools:Computer Management:Services and Applications:Services`, right-click on the “Hirschmann Industrial HiVision 8.4 Service” and select `Properties`). This means that you can start a program from Industrial HiVision (see on page 335 “Event Actions”) and that the process runs in the background, but that the program is not visible on the monitor. Permitting the data exchange between the service and the GUI is a security risk, because this program can then be started independently of the user who is logged on. So-called Trojan horse attacks use this security gap. To automatically send a Short Message Service (SMS) or an e-mail when an event occurs, you do not need a data exchange between the service and the GUI.

2.2.3 Installation under Linux

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

☐ Quit the current kernel.

- ☐ Start the installation script with the command
  `sh /mnt/cdrom/Software/IndustrialHivision/linux/install.sh`
- ☐ 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.

Example of a run of the installation script:

```
Welcome to Industrial HiVision

This script will install Industrial HiVision on your system.
You can abort the setup process anytime by pressing ctrl-c.

Do you wish to continue? [y]es, [n]o (default=no)
y

Please specify a destination directory for the installation
(default=/opt/ihivision8.4)

The directory /opt/ihivision8.4 does not exist.
Do you wish to create it? [y]es, [n]o (default=no)
y

Unpacking Industrial HiVision...

Running setup script...
*** Checking database user ***
*** Initialising installation directory ***
*** Initialising log directory ***
*** Configuring Services ***
*** Configuring Executables ***
*** Preparing Init Script ***
*** Industrial HiVision successfully installed ***

Industrial HiVision is now installed and ready for use.
```

- ☐ Start the Industrial HiVision service with the following command:`/etc/init.d/ihivision8.4 start`
  Industrial HiVision requires that you have logged on with `su`.
- ☐ You can quit the service with the following command: `/etc/init.d/ihivision8.4 stop`

☐ You can restart the service with the following command: `/etc/init.d/ihivision8.4 restart`

☐ You can check whether the service is running with the command: `/etc/init.d/ihivision8.4 status`

To start the service when starting the operating system, you include the service start in the init sequence of your system.
The various Linux distributions provide you with a whole range of options for this.
For some start sequences compatible with Sys V, the installation copies the start script `ihivision8.4` into the `init.d` directory of the system.
Depending on your requirements the following options are available:
- integrate this script into the various run levels
- start it manually with the above command

The Init script was developed and tested under Red Hat, Ubuntu/Kubuntu and Mandriva Linux. Other distributions (such as Gentoo) use a different script format and thus require different scripts.

Syslog Server Configuration

Linux applications save generated events in log files. The system utility Rsyslogd provides support to log events in a Linux system. You configure the Rsyslogd utility with the rsyslog.conf file. You can configure the rsyslog.conf file to save the Industrial HiVision events on a Syslog server.

The Linux Syslog includes the following events:
- Log in and out of the Industrial HiVision application,
- Actions which result in an SNMP Set Request being sent to a device, this includes the MIB variable that was set, and the new value,
- Actions from HiDiscovery V1 within Industrial HiVision,
- Start of external applications,
- Actions for which the “Edit Mode“ is needed.

To configure the rsyslog.conf file to save events on a Syslog server, proceed as follows:
☐ Navigate to the /etc folder in the installation directory.
☐ Open the rsyslog.conf file.
☐ Uncomment the following lines:
  – $ModLoad imudp,
  – $UDPServerRun 514.

Example of the rsyslog.conf file:

```
#/etc/rsyslog.conf     Configuration file for rsyslog
#                      For more information see
#                      /user/share/doc/rsyslog-doc/html
                       /rsyslog_conf.html


#################
#### MODULES ####
#################

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
$ModLoad immark   # provides --MARK-- message capability
|
# provides UDP syslog reception
|$ModLoad imudp
|$UDPServerRun 514
|
|
|# provides TCP syslog reception
|$ModLoad imudp
|$UDPServerRun 514
|
|
|"/ect/rsyslog.conf" 121 lines, 2630 characters
|
```

2.3 Update

2.3.1 Updating under Windows

To update a version of Industrial HiVision already installed, you install the new version as described on “Installation under Windows” on page 28.

During the installation, you can choose whether the installation routine transfers the database contents from a previous installation into the new installation.

If you want to transfer the database contents from an earlier version, you only uninstall the earlier version after the update. Industrial HiVision permits the installation of different versions on a PC.

Note: In the “Event History“ tab, Industrial HiVision notifies you when a new version of Industrial HiVision is available.

Note: In order to correctly transfer the data from the previous version, the installation routine terminates the previous version of the service, with your permission, if it is still active. Therefore, there is no network monitoring during the update procedure.

Note: The Industrial HiVision backup is version dependent. Make a backup file after every software update (see on page 260 “Save Backup”).

2.3.2 Updating under Linux

To update a version of Industrial HiVision already installed, you install the new version as described on “Installation under Linux” on page 29.

During the installation, you can choose whether the installation routine transfers the database contents from a previous installation into the new installation.

If you want to transfer the database contents from an earlier version, you only uninstall the earlier version after the update. Industrial HiVision permits the installation of different versions on a PC.

Note: In order to correctly transfer the data from the previous version, terminate the previous version before the installation, if it is still active. Therefore, there is no network monitoring during the update procedure.
If multiple previous versions are installed, Industrial HiVision takes the data from the latest previous version.

Note: During an update, Industrial HiVision can transfer the data from the database of the previous version if the previous version is in the specified installation directory.
Otherwise, you can use the interface functions “Save” on page 259 and “Open...” on page 259 to transfer the data.

Note: The Industrial HiVision backup is version dependent. Make a backup file after every software update (see on page 260 “Save Backup”).

2.4 Maintenance

Hirschmann are continually working on improving and developing their 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.hivision.de

2.5 Starting

2.5.1 Starting under Windows

During the installation, the program installation routine installs a program symbol for the link to the program Industrial HiVision in the following locations:

- on the desktop and
- in `Start:Programs:Hirschmann:Industrial HiVision` 8.4

☐ Start Industrial HiVision with a double-click on the program symbol on your desktop, or by selecting the program symbol in your start directory.

When starting, Industrial HiVision looks for the server. If Industrial HiVision does not find the server, Industrial HiVision opens a dialog for entering the server IP address or the server name. If the server is located on your local computer, you enter the name `localhost`.

Note: To be able to connect to the Industrial HiVision server from another computer, you first permit remote access in the server settings (see on page 374 “Services Access”).

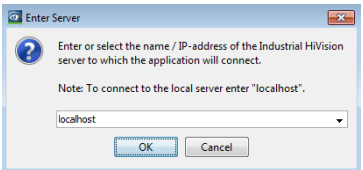


Figure 2: “Enter server address” window

If Industrial HiVision finds the server to which Industrial HiVision was last connected, Industrial HiVision connects to it again. If you want to connect to a different server, you click on “Cancel” in the “Connecting to server...” window. With `File > Login` you open the dialog for entering the server IP address.

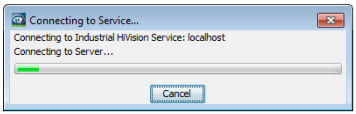


Figure 3: “Connecting to server...” window

Connecting to multiple servers

- ☐ To connect to multiple servers, you copy the program symbol and add it again as a connection.
- ☐ Open the properties of the new program icon by right-clicking on the icon and selecting `Properties`.
- ☐ In the `Destination` row, you enter a blank after “`C:\Programs\Hirschmann\Industrial HiVision 8.4\bin\HiVision.exe`”, then the command line parameter `-kernelHost <server name>`. For `<server name>` you enter the IP address or the name of your server.

Repeat these steps for every server you want to make a connection to.

2.5.2 Starting under Linux

- ☐ Start the service before you start the graphic interface (see on page 29 “Installation under Linux”).

To be able to start Industrial HiVision from the graphic interface, you put an icon on the desktop you are using (KDE, Gnome, etc.).

You will find a suitable image (`ihivision_op32x32.png`) in `/opt/ihivision8.4/lib`.

By double-clicking on the icon, or with the following command `/opt/ihivision8.4/bin/HiVision`, any user can start Industrial HiVision.

2.6 Deinstallation

2.6.1 Deinstallation under Windows

☐ Quit the program Industrial HiVision before you start the deinstallation.

☐ To deinstall Industrial HiVision, select:
`Start:Control Panel:Software`

☐ Select the program Industrial HiVision.

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

2.6.2 Deinstallation under Linux

☐ Quit the Industrial HiVision program before you start the deinstallation.

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

☐ Quit the Industrial HiVision service with the following command: `/etc/init.d/ihivision8.4 stop`

☐ Delete the `/opt/ihivision8.4` directory with the command `rm -rf /opt/ihivision8.4`

☐ Remove the ihivision start script from the run levels of your init sequence (see on page 29 “Installation under Linux”).

Note: The database content and the licenses are lost during the deinstallation.

3 Preparation

Before you start entering and monitoring your network, set up the necessary or useful conditions.

- ▶ One prerequisite to be emphasized here is protecting your network management station.
- ▶ The necessary conditions include the accessibility of the devices to be monitored and the related access authorization.
- ▶ The useful conditions are the settings related to the presentation, such as color and font size.
- ☐ Create a data backup plan. Regularly export the data of your project. You can thus recreate your project at any time, should adverse circumstances damage the data stock.

The “Demo Network“ program supplied allows you to simulate a network on your computer in order to familiarize yourself with Industrial HiVision without being connected to a network.

3.1 Improving the security of Industrial HiVision

Increasingly frequent attacks on IT systems, sabotage and espionage require in-depth knowledge of the targets for attacks on the part of the operator. The following list provides a selection of potential attack targets in the environment managed by a network management system:

- physical access to the network management station
- physical access to the managed devices
- manipulated installation files
- Ethernet access to the network management station
- Ethernet access to the managed devices
- Access to configuration and log files

This chapter provides guidelines to help you make it more difficult for unauthorized persons to access Industrial HiVision and the managed devices.

The term 'Security' in this manual, means everything related to the security and protection of your data network infrastructure.

Note: For security reasons, we recommend the use of secure protocols instead of unsecure protocols:

- HTTPS instead of HTTP
- SSH instead of Telnet
- SNMPv3 instead of SNMPv1

You can configure these protocols in the following “Preferences“ dialogs:

- “User Management“
- “Services Access“
- “Device Credentials“
- “Export to InfluxDB®“

3.1.1 Physical protection

Even the best IT security system and matching software security strategies are useless if an attacker has physical access to a device that you need to protect. The attacker can, for example, disconnect the device from the power supply, unplug data lines, sniff data lines, or destroy the device mechanically.

☐ Install devices that need protection in a locked cabinet or room.

3.1.2 Measures before and during the installation of Industrial HiVision

Take the first steps to help improve the security of your network management system before and during installation.

■ **Check the installation scope**

The more programs there are installed on your system, the more potential attack vectors for your system the attackers will find. The Industrial HiVision installation routines offer you several installation program extensions:

– OPC DA service
– OPC UA service
– GUI installation

☐ Check which products and program extensions you need to meet your needs.

☐ Remove any programs from your system that do not play a direct role in meeting your requirements.

☐ Only install the programs and program extensions, which you need to meet your requirements.

Note: Even if you do not install the OPC UA service, the communication port is open. This is a security risk.

To eliminate the security risk of the open communication port use the following work steps:

- ☐ If you have the Industrial HiVision program open, then close the program and stop the processes.
- ☐ Click `File > Exit and Stop Service`.
- ☐ Open the service.xml file in a text editor for example, Notepad ++. The service.xml file is in `C:\Program Files\Hirschmann\Industrial HiVision8.4\config`.
- ☐ Search for the OPC service line, `<Service Name="OpcUaServer" Enabled="yes" Path="..." Foreign="yes"`. This line is located near the bottom of the file.
- ☐ Change “`yes`” to “`no`” for the OPC UA server for example, `<Service Name="OpcUaServer" Enabled="no" Path="..." Foreign="yes"`.
- ☐ Save and close the service.xml file.
- ☐ Restart the Industrial HiVision program.

Verify the signature of the installation files

One option for attacking IT systems is to contaminate the installation files with malware. Hirschmann signs the *.exe-, *.ocx-, *.dll- and *.jar files in Industrial HiVision. The signature allows you to check whether you have original installation files from Hirschmann.

Check the signature of the *.exe-, *.ocx- and *.dll files in Windows:

The files in the installation path contain a signature.

- ☐ In the file explorer, open the `Properties` dialog of the file you want to check.
- ☐ In the `Properties` dialog, switch to the `Digital Signatures` tab.
- ☐ Mark the row with the signature and click the `Details` button.
- ☐ In the `Details` dialog, click `View Certificate`.

Verify that the certificate is issued for “Hirschmann Automation and Control GmbH.

Verify that the certificate is issued by a trusted authority, and is a Class 3 Code Signing CA.

Verify the signature of *.jar files in Windows and Linux:

The user interface is a Java application.

If you start the user interface in a web browser, the web browser organizes the display of the signature for the *.jar file. The web browser also gives you the option to trust the signature or prohibit the execution of the *.jar file.

See “Web access to Industrial HiVision” on page 244.

Restrict access authorizations to the installation files

Anyone who has write permissions for the installed files on a system can manipulate these files.

☐ Make it more difficult to access the Industrial HiVision installation directory by only giving people you can trust access to the directory.

Note: Regarding security:
Anyone who has write permissions to the registry on a system can manipulate the registry entries. Help protect the registry by assigning write permission only to people you trust.

Installing a redundant network management system

For high-availability network management, the Industrial HiVision network management system gives you the option of installing the software in different locations. The installations access a common database.
This gives you the following redundant design options:

- the network management station itself
- the connection between the two network management stations

The benefit of redundant availability is offset by additional attack vectors.
These additional attack vectors are as follows:

- the redundant network management station itself
- the redundant connection between the two network management stations

☐ Take the same security provisions for the redundant components as for the main components.

The “Redundant Network Management System Industrial HiVision” user manual provides details on installing the redundant system.

Web server certificate

Industrial HiVision lets you use a web browser to encrypt communications with the Industrial HiVision web server. For encrypted communication, select the HTTPS transmission protocol. Industrial HiVision uses a self-signed certificate for HTTPS. Trust this certificate only if you are sure that you addressed the real Industrial HiVision web server with your connection request.

3.1.3 Industrial HiVision configuration actions

After installing Industrial HiVision, anyone can launch the program without restriction. The security-specific configuration starts with restricting access authorizations.

Change login name and password for Edit Mode

You can access Industrial HiVision freely in the newly installed condition. Industrial HiVision gives you the option of requesting a login when starting the program interface initially.
After starting the program interface, Industrial HiVision has an “Edit Mode“ and a run mode. See “Edit Mode” on page 84.

- ☐ Setup the login request.
- ☐ Set up a password for access to the “Edit Mode“. See “User Management” on page 329.

Specifying user authorizations

Limiting access with user rights in connection with passwords is a crucial part of protecting IT systems.
You can define appropriate authorization roles and users with the matching authorization roles.

- ☐ In order to limit access to Industrial HiVision, set up a user under “Local Users“ and/or activate an authorization “Policy“. See “User Management” on page 329.

Setting up an LDAP

The Lightweight Directory Access Protocol (LDAP) is an application, whose tasks include authentication (verifying passwords) and authorization (verifying rights) in a data network. For example, Microsoft uses LDAP to perform user management in an Active Directory service. A central server or several distributed servers manage functions including user names and user roles.
If LDAP is activated, Industrial HiVision sends an inquiry to the LDAP server, as soon as a user logs on.

Industrial HiVision adopts the user names and authorization roles from the LDAP server and enters these into the local user directory.

☐ Ask the administrator of your LDAP server, which configuration data you should enter into the Industrial HiVision LDAP dialog.

☐ Give your LDAP server administrator the following user data to enter into the LDAP server:
- “User Name“
- “Password“
- “Access Roles“

See “User Management” on page 329.

Radius Authentication

The Remote Authentication Dial-In User Service (RADIUS) is a service for authentication (verifying passwords) and authorization (verifying rights) in a data network.
RADIUS is based on a client/server protocol.
If RADIUS is activated, Industrial HiVision sends an inquiry to the RADIUS server, as soon as a user logs on.
Industrial HiVision adopts the user names and authorization roles from the RADIUS server and enters these into the local user directory.

☐ Ask the administrator of your RADIUS server, which configuration data you should enter into the Industrial HiVision RADIUS dialog.

☐ Give your RADIUS server administrator the following user data to enter into the RADIUS server:
- “User Name“
- “Password“
- “Access Roles“

See “User Management” on page 329.

Monitoring the device configuration settings

The device configuration is an attack target. An attacker who gains access to the management system can manipulate the device configuration for example, by disabling a port.

Industrial HiVision gives you the ability to save the configuration of devices as a reference configuration, and to regularly compare this with the actual configuration of the device.

☐ Click on the “Properties“ tab in the detail display.

☐ Select the “Configuration File“ property in the “Property:“ drop-down list.

Industrial HiVision lists the devices on your network that have the property “Configuration File“.

☐ Select the devices whose configuration you want to monitor.

☐ Right click a selected device and select MultiConfig™.

Industrial HiVision opens the MultiConfig™ dialog.

☐ In the MultiConfig™ menu tree, click on the “Status Config“ dialog.

☐ To download the reference configurations of the devices, select the function framework of the “Status Config“ dialog “Set current to reference“.

☐ Select the status for “Value is Reference Value“ for example, “OK“.

☐ Select the status for “Other Value“ for example, “Warning“.

☐ Click “Write“.

☐ To configure polling and status forwarding, select “Property Properties“ in the menu tree of the MultiConfig™ dialog. Note the network load caused by this function when setting the polling interval. One option for being able to react to current events despite large polling intervals is to send traps using the devices in the network. Enter the network management station into the devices as a trap target.

If the configuration of the device to be monitored changes, Industrial HiVision gives you the ability to compare the configuration saved in Industrial HiVision with the current configuration on the device.

☐ To access the “Configuration File“ device property, double-click the detail display of the device in question in the list view.

☐ To display the differences, right click the “Configuration File“ device property and select “Display differences“.

The highlighted sections in the comparison have the following meanings:

▶ Green text on light gray background: Change

▶ Red text on light gray background: Deleted

▶ Blue text on light gray background: Added

Tracking changes to program settings and device configurations

"Audit Trail" or "Audit Log" is the name for a chronological record of changes to a system and its environment.

These records give you the opportunity to verify, for example, who made a configuration change and when.
Audit Trail uses the Windows Event Viewer or Linux syslog function.
Audit Trail runs automatically without any user intervention.
Industrial HiVision logs information for the following events:

- MultiConfig™
  - Write operations with MultiConfig™ that completed successfully or did not complete.
- Properties dialog
  - Write operations in the Properties dialog of a property
- Domains
  - Issue licenses
  - Revoke issued licenses
  - Add subdomain
  - Remove subdomains
- Scheduled actions
  - Execution of a task
  - Add tasks
- Device management
  - Set device to "Managed"
  - Set device to "Unmanaged"
  - Delete device
  - Set trap target address
- Change IP configuration
- Perform actions that require "Edit Mode"
  - "Audit Trail" records actions for which Industrial HiVision prompts the user to enter the "Edit Mode" password before completing the action.
- External programs
  - Open or close the web interface of managed devices
  - Open or close the device configuration of managed devices
  - Open or close the command line interface of managed devices
  - Open or close the SNMP browser for querying SNMP MIB variables of managed devices

  Logging of actions carried out by external programs is the responsibility of those external programs. Industrial HiVision logs the launch and termination of these external programs.
- User-defined actions
  - Add user-defined action
  - Run user-defined action

Restricting remote GUI access rights

Industrial HiVision gives you the ability to connect with the Industrial HiVision server remotely from another computer.

☐ Disable remote access if you want to prohibit remote access to the Industrial HiVision server.
See “Services Access” on page 374.

Restricting web server access rights

Industrial HiVision gives you the ability to use a browser to access the Industrial HiVision web server using the HTTP or HTTPS protocol. You can thus monitor your network from anywhere in the world.

☐ To enhance the protection for web server access, assign user authorizations.
See “User Management” on page 329.

☐ Disable the web server if you want to prohibit browser-based access to Industrial HiVision.
See “Services Access” on page 374.

Restricting OPC server usage

Industrial HiVision enables you to activate/deactivate the OPC server or to activate/deactivate the writing of object values in Industrial HiVision using an OPC write command. Both are deactivated on delivery.

☐ Only activate what you really need.
See “Services Access” on page 374.

☐ Disable the function in the service.xml.
See “Services Access” on page 374.

3.1.4 Restrict File Access

You can help protect your management system by limiting the number of Industrial HiVision users and by restricting user permissions. To further deny unauthorized user access, restrict access to the Industrial HiVision “`config`”, “`var\script`”, and “`var\report_files`” folders.

The Industrial HiVision “`config`” folder contains the security related files `usermanagement.xml` and `service.xml`.

Industrial HiVision saves script files in the “`var\script`” folder. If you use scripts with unencrypted passwords, then a user can open the script file and see the passwords. The “`var\report_files`” folder contains the script results. The results of a script can also contain unencrypted passwords.

The default path to the folders is as follows: “`C:\Program Files\Hirschmann\Industrial HiVision <version number>`”

Note: The Industrial HiVision “`config`” folder contains the `usermanagement.xml` file only after you have added users to the `Configuration > Preferences > User Management` dialog.

3.2 Outside the program

Industrial HiVision requires access to the devices to be monitored. Therefore keep the following in mind:

- Your network management station has access rights to every device to be monitored. This is the case if the IP address of your network management station is entered as an IP address with access rights on the device to be monitored.
  Devices with any IP address have access to Hirschmann devices whose configuration is set to the factory default.
- Your network management station is physically connected to every device to be monitored, directly or indirectly through hubs and switches or routers.

3.3 Network structure

Large data networks have hierarchical network structures. Industrial HiVision is scalable and can be adapted to the hierarchical network structure. Adapting to the hierarchical network structure means that you can set up a network management station for each subdomain of your data network (see figure 55 “Domains”).
A superdomain can attach several subdomains, but a subdomain can only be attached to a single superdomain. Domain interaction is a host-client type of relationship. A superdomain as a host can have several subdomains as clients, but a subdomain can only have a single superdomain.The superdomain kernel contains a host infrastructure to connect to other subdomain kernels and can connect several instances of this client. But a kernel has only one subdomain interface that allows a single superdomain to be connected to it. In addition, a kernel can be a host for its clients and a client to its host at the same time.

3.3.1 Advantages of the hierarchical network structure

This hierarchical adaptation offers the following advantages to you:

- Load distribution
  In very large data networks with extensive monitoring, you can easily reach the limits of your system resources (see on page 228 “Effect on system resources”). Through the use of multiple network management stations, you can restrict the utilization of the data network and the network management station to the domain limits. This significantly increases the performance.
- Smaller projects
  Smaller projects make it easier to get an overview.
- Organizational structure
  Adapting your network management projects to your organizational structure enables you to create and copy relevant projects individually.

- Central administration of Industrial HiVision licenses
- Concentrated display of the statuses of the subdomains

Note: A superdomain requires its own license. The free-of-charge 16 nodes license cannot be assigned to the superdomain. If you plan to use subdomains, then you require a license other than the free-of-charge 16 nodes license. This is because, the free-of-charge 16 nodes license does not let you lease licenses to subdomains. Furthermore, if you have sub-subdomains, then the free-of-charge 16 nodes license on a subdomain device blocks previously leased licenses.

3.3.2 Application Example

The following figure shows an application example of a hierarchical network structure.
The network consists of the IT domain, with lower-level domains A1, A11, and B1.
The IT network management station is in the IT network.
The A1 network management station is in production network 1.
The A11 network management station is in production subnetwork 11. In this case, the A1 network management station is the superdomain of the A11 domain.
The B1 network management station is in distribution network 1.
The domains A1 and B1 are subdomains of the IT domain.
Industrial HiVision allows a nesting depth of 4 layers and 5 subdomains per domain.

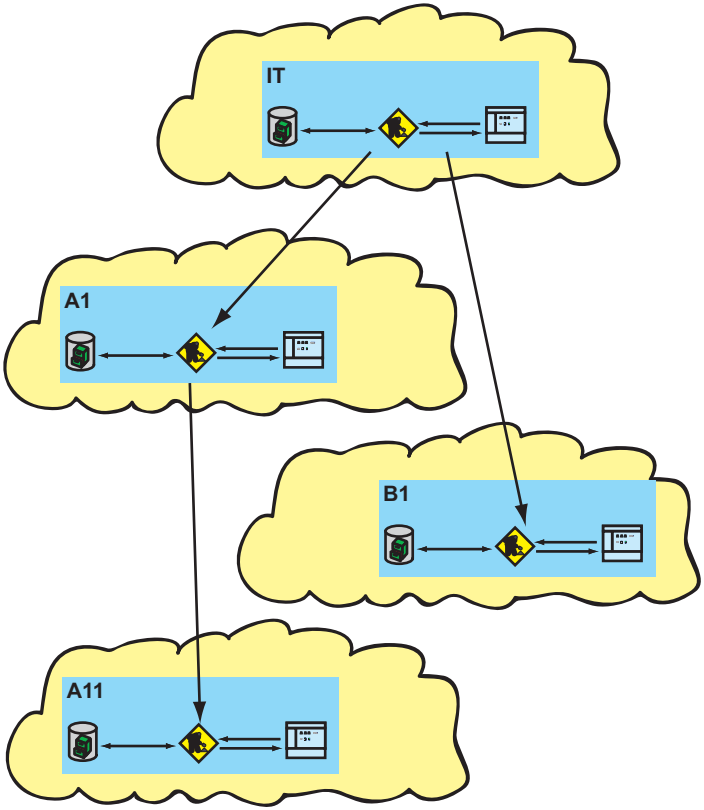


Figure 4: Domains

3.3.3 Configuration of the application example

The configuration of hierarchically arranged network management stations comprises the following steps:

- Release subdomains
- Connect subdomains to superdomains
- Assign licenses from top to bottom

Release subdomains

First you go into the hierarchical levels from bottom to top. In Industrial HiVision, go into the subdomain interface and release access for the superdomain on the next higher level.

The following instructions describe this process for the A11 subdomain:

- ☐ In the “Preferences“ menu tree, open the `Advanced > Services Access` dialog.
- ☐ To allow remote access mark the `Project Data Server > Remote Access` checkbox.
- ☐ To allow the subdomain interface mark the `Project Data Server >` Subdomain interface checkbox.
- ☐ Under `Project Data Server > Password`, enter a password with which the superdomain can access this subdomain.
  Requirement for the password: 8 to 16 characters.
- ☐ Repeat these steps for the subdomains A1 and B1.

Connect subdomains to superdomains

- ☐ To connect the A11 subdomain to the A1 superdomain, on the superdomain A1 open the “Add New Subdomain“ dialog with `File >` New `> Subdomain`.
- ☐ Enter the IP address of the subdomain.
- ☐ Enter a name for the subdomain under which Industrial HiVision displays the subdomain in the folder frame.
- ☐ Enter and repeat the subdomain password with which the superdomain can access the subdomain.
  Industrial HiVision shows the subdomain in the upper part of the folder frame.
- ☐ Repeat these steps for the IT superdomain with the superdomains A1 and B1.

You can delete a subdomain from the folder frame by selecting the subdomain and pressing the `Del` button.

Assign licenses from top to bottom

Now you assign the Industrial HiVision licenses in the levels of the hierarchy from top to bottom.

Note: A superdomain requires its own license. The free-of-charge 16 nodes license cannot be assigned to the superdomain(see on page 53 “Advantages of the hierarchical network structure”).

- ☐ In the IT superdomain, enter your license key (see on page 348 “License”).
- ☐ To assign licenses to the subdomain A1, right-click the subdomain A1 in the folder frame of the IT superdomain.
  In the “Lease license nodes“ dialog, enter the number of licenses you are leasing to subdomain A1.
  The number of licenses for the subdomain A1 includes the number of licenses that you further assign from superdomain A1 to subdomain A11 in the next step.
- ☐ To assign licenses to the subdomain A11, right-click subdomain A11 in the folder frame of the A1 superdomain.
  In the “Lease license nodes“ dialog, enter the number of licenses you are leasing to subdomain A11.
  Superdomain A1 requires a separate license so that it can issue licenses to subdomains.

As an alternative, Industrial HiVision offers you the option to enter a license key directly in the subdomain.

Note: A subdomain maintains the validity of its borrowed licenses using periodic communication with the superdomain. If this communication is interrupted for more than 48 hours, the validity of the subdomains borrowed licenses lapses. The lapsed licenses are then available again in the superdomain. If the connection is restored, the licenses are leased back to the subdomain automatically. The lapsed licenses are available again in the superdomain only after the user disables the leasing of the licenses. IHV does not disable the leasing automatically.

You will find an overview of the licenses assigned to subdomains in the `Basics > License` dialog in the configuration settings (see on page 348 “License”).

3.3.4 Status display of the subdomains

The superdomain determines the status of its subdomains and indicates this status with color.

Color	Meaning
Dark gray	Subdomain cannot be reached
Gray	Status determination not available
Green can be configured in the initial settings	OK
Yellow can be configured in the initial settings	Warning
Red can be configured in the initial settings	Error

Table 1: Meaning of the status colors of the subdomains

3.4 Program default settings

To take into account the individuality of every user, Industrial HiVision gives you the option of entering settings relating to the presentation, the function and the device detection.

IP parameters

Enter the IP parameters of your network management station under `Configuration > Preferences > Advanced > Management Station` (see on page 385 “Management Station”).

Device access

Industrial HiVision independently detects the delivery settings of Hirschmann devices for the SNMP access.
If for security reasons you have already made changes to the SNMP settings for the devices to be monitored, then enter the user names and the passwords under `Configuration > Preferences > Advanced >` Device Credentials (see on page 377 “Device Credentials”).

Discover Devices

Industrial HiVision gives you the following options for detecting devices in the connected network:

- Traps: Detecting devices using the alarm messages (traps) sent by them. Keep in mind that your network management station is entered as the trap destination address in every device to be monitored (see on page 216 “Trap destination address”).
- HiDiscovery V1: Detecting devices by means of a query using the HiDiscovery V1 protocol. Select the relevant network card of the network management station (see on page 385 “Management Station”).
  On delivery, the HiDiscovery V1 protocol on a new Hirschmann device is active.
- Network scan: Discovering devices by means of an IP query for an entered IP address range (see on page 122 “Device detection”).

Select the required method for device detection under `Configuration > Preferences > Basics > Discover Devices` (see on page 324 “[Basics]”).

License

To be able to utilize the entire scope of the functions of Industrial HiVision, enter your license key under `Configuration > Preferences > Basics > License` (see on page 348 “License”).
After a new installation or after an update, Industrial HiVision starts fully functional for the duration of the free 30-day trial period.
After the free 30-day trial period, Industrial HiVision runs as a free version (see on page 266 “Switch to the free version”).
After you enter a license key, Industrial HiVision runs as the licensed version.

Font size

Depending on the setting of your screen resolution, some of the text displayed is too small or incomplete. Adapt the font size under `Configuration > Preferences > Display > Device`, `Configuration > Preferences > Display > Device Appearance` (see “Appearance” on page 363 and “Device” on page 360).

Colors

The optimal signal effect of the display depends on your color sensitivity. Select your color display under `Configuration > Preferences > Display > Status Colors` (see on page 365 “Status Colors”).

Devices and port names

Industrial HiVision enables you to select the name of the device/port that appears in the interface. Select the name of the device/port under `Configuration > Preferences > Advanced > Device/Port Names` (see on page 395 “Device/Port Names”).

Default device icons

Industrial HiVision enables you to assign defined default icons to different device types. Select device icons under `Configuration` > Preferences > `Display > Device Icon` (see on page 366 “Device Icon”).

3.5 Using Industrial HiVision with Firewalls

Industrial HiVision is a management system that allows you to connect multiple clients to the Industrial HiVision services. You can install the management station which provides the Industrial HiVision services in the same network as the clients or in a remote network. You can separate the networks with a firewall. When a firewall separates the Industrial HiVision services from the clients, add rules to the firewall to forward the required Industrial HiVision service data.

Note: Limit “Project Data Server“ access to local users only. To limit access to the “Project Data Server“, deactivate the “Remote Access“ function.

The following list contains the various types of clients:

- Application GUI
  The Application GUI client uses the Industrial HiVision executable file to connect to the Industrial HiVision services.
- Industrial HiVision Super Domain Client
  This client is the Industrial HiVision service were you add an Industrial HiVision Subdomain.

  Note: Activate the “Subdomain interface“ and set the password on the Industrial HiVision subdomain.

- Web GUI
  The Web GUI client is available using any web browser.
  To access the Industrial HiVision services using a web browser, enter the IP address of the management station and the “Port“ number. For example:
  `https://[IP address of the network management station]:11165`

Note: Regarding security:
An attacker can spoof the Industrial HiVision Web GUI client, also known as the browser client, which can lead to unauthorized access to the Industrial HiVision kernel/web server. To help protect your network against attack, verify that every user requiring access has proper credentials. Limit the number of administrators and users (see on page 329 “User Management”).

- HTML GUI
  The HTML GUI client is available using any web browser.
  To access the Industrial HiVision index using a web browser, enter the IP address of the management station, the “Port“ number, and idx. For example:
  `https://[IP address of the network management station]:11208/idx`
  To access the Industrial HiVision events using a web browser, enter the IP address of the management station, the “Port“ number, and events. For example:
  `https://[IP address of the network management station]:11208/events`
- OPC UA HTTP/HTTPS
  You can configure any suitable OPC UA client to access the Industrial HiVision OPC UA server through the corresponding port.

For entries marked with an “X”, activate the service in Industrial HiVision. To forward the port data add a rule to the firewall. To activate a service, mark the checkbox for the required service in the `Preferences > Advanced >` Services Access dialog.

Note: For the “Project Data Server“ entries, verify that the Industrial HiVision service is running and accessible (see on page 374 “Services Access”).

Type of Industrial HiVision Service /Client	Web Server	Project Data Server	OPC UA Server (HTTP)	OPC UA Server (HTTPS)
Ports used to connect to the services	11208 (Configurable)	11209	11210	11211
Application GUI	–	X	–	–

Table 2: Service-Client settings

Type of Industrial HiVision Service /Client	Web Server	Project Data Server	OPC UA Server (HTTP)	OPC UA Server (HTTPS)
Industrial HiVision Super Domain Client	–	X	–	–
Web GUI	X	X	–	–
HTML GUI	X	–	–	–
OPC UA HTTP	–	–	X	–
OPC UA HTTPS	–	–	–	X

Table 2: Service-Client settings

3.6 Fingerprint verification

As described in “Physical protection” on page 43, secure the physical access to the kernel host against unauthorized access. The remote GUI client also requires protection against connecting to a fraudulent kernel host. To verify that the remote GUI client is connecting to the correct kernel host server, use the fingerprint verification function.

During the initial installation, Industrial HiVision creates a certificate and saves it in the key store. Industrial HiVision generates an SHA-256 fingerprint from the certificate. The fingerprint used for verification is unique for every Industrial HiVision application.

You can find the fingerprint in the `Help > About > Fingerprint > SHA-256 Fingerprint` text field. The “Fingerprint“ dialog also displays additional certificate information. For example, who created the certificate, the creation date, and the expiration date.

Note: The management stations located in the subdomains accept the fingerprint of the kernel host without notification.

To verify that the remote GUI client is connecting to the correct kernel host, proceed as follows:

☐ The remote user requests the fingerprint of the kernel host server from the administrator. To find and send the fingerprint, the administrator proceeds as follows:
- Open the `Help > About > Fingerprint` tab.
- Copy the fingerprint from the “SHA-256 Fingerprint“ field.
- Pastes the fingerprint into a text file.
- Using a secure communications channel, send the text file to the remote user.

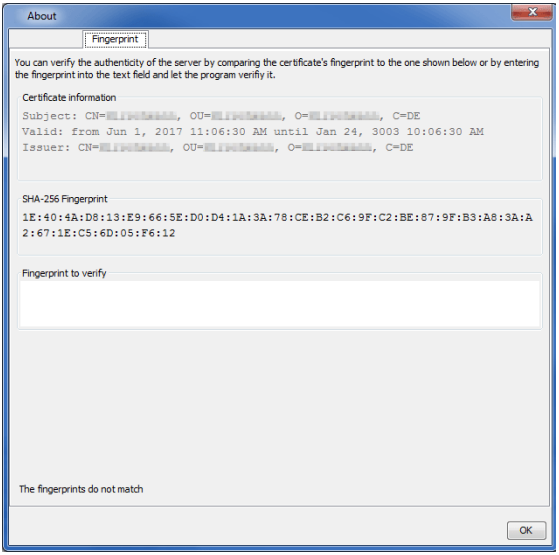


Figure 5: `Help > About > Fingerprint` *tab*

☐ To connect the remote GUI client to the kernel host server, proceed as follows:
- Click the “File“ option on the toolbar.
- Select the “Login“ option from the drop-down list.
- In the “Enter Server“ dialog, enter the IP address of the server containing the kernel host.
- Click the “OK“ button.

Industrial HiVision opens the “Confirm Server Certificate for Industrial HiVision Server“ dialog.

Note: If the kernel host and remote GUI client are both located in the same private network, then leave the text field empty. Click either the “Accept“ or “Accept Permanently“ button.

☐ Enter the fingerprint received from the administrator in the “Fingerprint to verify“ text field.
- If the fingerprint is a mismatch, then the text field displays red characters. The dialog also displays the message, “The fingerprints do not match“. Click the “Cancel“ button and contact your administrator.
- If the fingerprints match, then the “Accept“ and “Accept Permanently“ buttons are active. The dialog also displays the message, “The fingerprint matches this server's fingerprint“.
- When you click the “Accept“ button, the remote GUI client connects to the kernel host. If the connection to the server terminates, then Industrial HiVision requires that you reverify the fingerprint in order to re-establish the connection.
- When you click the “Accept Permanently“ button, Industrial HiVision saves the fingerprint with the associated IP address. If the connection terminates, then Industrial HiVision re-establishes the connection without fingerprint verification.

Note: Whenever the fingerprint is accepted, Industrial HiVision makes an entry in the log file.

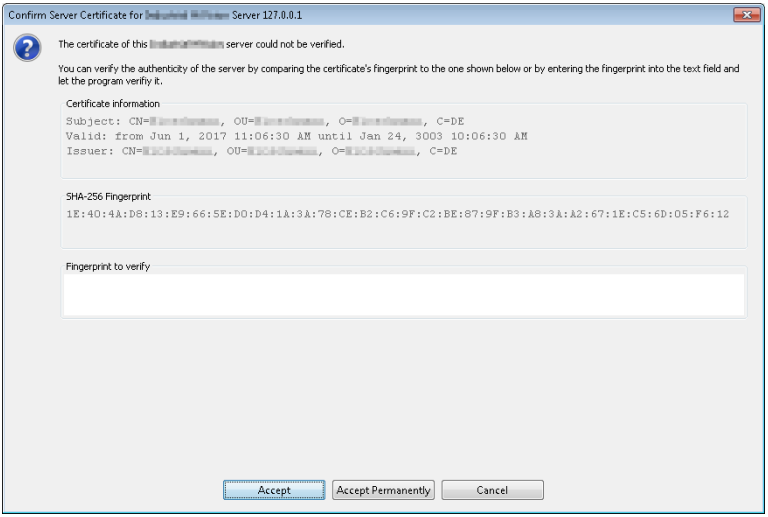


Figure 6: “Confirm Server Certificate for Industrial HiVision Server“ dialog

Industrial HiVision allows you to connect the remote GUI client to different kernel host servers. If the fingerprint for a previously trusted server has changed or is no longer trustworthy, then “distrust” the certificate.

Industrial HiVision allows you to distrust a certificate on the kernel host or on the remote GUI client.

- When you delete the “corbas.jks” file on the kernel host server, after a restart Industrial HiVision creates a new “corbas.jks” file containing a new certificate. Every remote GUI client is required to accept the fingerprint of the new certificate.
- When you delete the “corbas.jks” file on the remote GUI client, you delete the fingerprints of every trusted server. After you restart Industrial HiVision, Industrial HiVision creates a new “corbas.jks” file. To rebuild the “corbas.jks” file, accept the fingerprints of the trusted servers again.

To distrust a server either on the kernel host or the remote GUI client, proceed as follows:

☐ Verify that you have administrator rights.
☐ Navigate to the "config" folder in the installation directory.
☐ Delete the “corbas.jks” key store file
☐ Restart the Industrial HiVision application.

To rebuild the “corbas.jks” key store file on the remote GUI client, perform the following work steps for every required kernel host server:

☐ Reconnect to a kernel host server.

☐ Verify that the fingerprint displayed in the dialog matches the fingerprint received from the administrator.

4 Interface of the program

This chapter describes the structure of the program interface. It provides you with an overview to help you find your way in the graphic interface. You will find a detailed description in the chapter “References” on page 255.

Expert knowledge of networks is not required to use Industrial HiVision. The interface enables you to operate the program intuitively. It contains elements of standard user interfaces, so you will be able to get started after a brief familiarization phase.

4.1 Main window of Industrial HiVision

When you start Industrial HiVision, the main window appears on the screen. It consists of the following parts:

- Menu bar
- Tool bar
- Event line
- Folder frame
- Navigation field
- Detail display
- Event list

By positioning the mouse on a screen position in Industrial HiVision for a short time, you open an information window with a small help text.

In the event list area, Industrial HiVision shows the time that is synchronized with the system time of the computer. Industrial HiVision updates this time every second.
If the time displayed matches the system time of the computer, you can assume that the displayed content of Industrial HiVision is up to date.

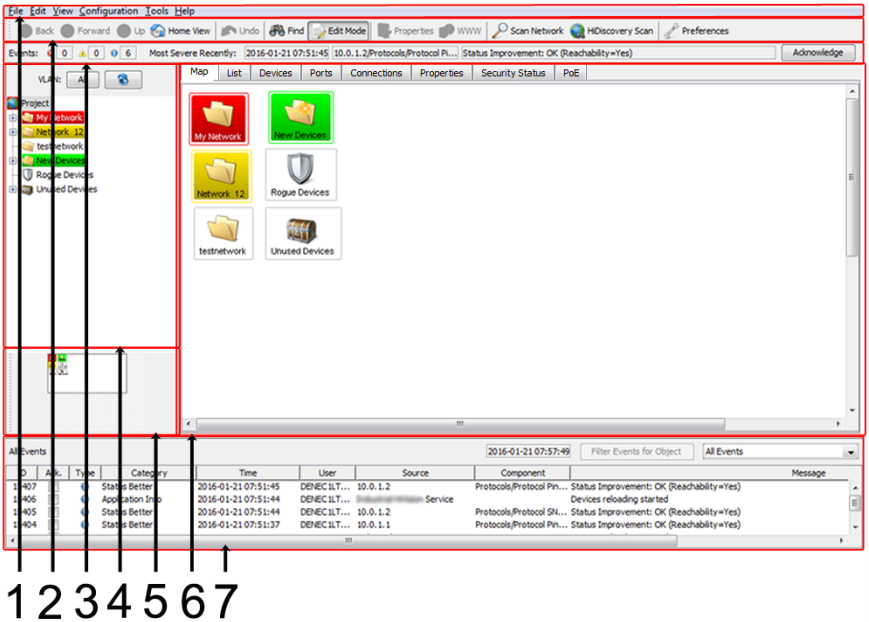


Figure 7: Main window
1 - Menu bar
2 - Tool bar
3 - Event line
4 - Folder frame
5 - Navigation field
6 - Detail display
7 - Event list

4.2 Menu bar

The menu bar is right at the top of the main window of the program. It gives you support in importing, exporting, and creating new projects, in copying, adding, and deleting data, and in changing the view and configuration. A help menu is also provided. See “Main window of Industrial HiVision” on page 72.

The menu bar contains the following selection items:

- “File“
- “Edit“
- “View“
- “Configuration“
- “Tools“
- “Help“

Note: When you start Industrial HiVision from HiView some options are missing from the selection items.

4.2.1 File

The “File“ menu item in the menu bar contains the following selection fields:

- “New Project“
- “Run Setup Wizard“
- “New“
- “Login“
- “Logout“
- “Open...“ (Ctrl+O)
- “Save“ (Ctrl+S)
- “Save as...“
- “Save Backup“
- “Load Backup“
- “Export...“
- “Export Events...“
- “Print“ (Ctrl+P)
- “Print Events“
- “Exit and Stop Service“
- “Exit“ (Ctrl+Q)

The key combinations in brackets allow you to start the selection items without using the mouse.

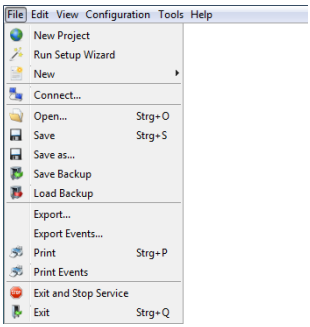


Figure 8: Menu bar – file

4.2.2 Edit

The “Edit“ menu item in the menu bar contains the following selection fields:

- “Undo“ (Ctrl+Z)
- “Redo“ (Ctrl+Y)
- “Edit Mode“
- Switch to the Free Version (available during the 30-day trial period)
- “Cut“ (Ctrl+X)
- “Copy“ (Ctrl+C)
- “Paste“ (Ctrl+V)
- “Paste as Link“
- “Delete“ (Del)
- “Rename“ (F2)
- “Select All“ (Ctrl+A)
- “Acknowledge Status Change“
- “Manage“
- “Unmanage“
- “Set Device and Port Names“
- “Set Default Device Icon“
- “Device Documentation“
- “Drawing Size“
- “Background Image“
- “Find...“ (Ctrl+F)
- “Auto Topology...“
- “Auto Layout“
- “Properties...“ (Alt+Enter)

The key combinations in brackets allow you to start the selection items without using the mouse.

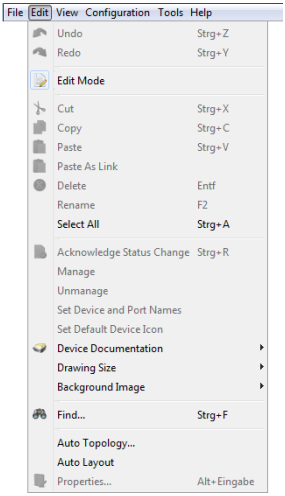


Figure 9: Menu bar – edit

4.2.3 View

The “View“ menu item in the menu bar contains the following selection fields:

- “Select VLAN“
- “Refresh VLANs“
- “Protocol Statistics“
- “Filter Events for Object“
- “Back“
- “Forward“
- “Up“
- “Home View“
- “Set Home View Settings“
- “Geographical Location View“
- “Zoom“

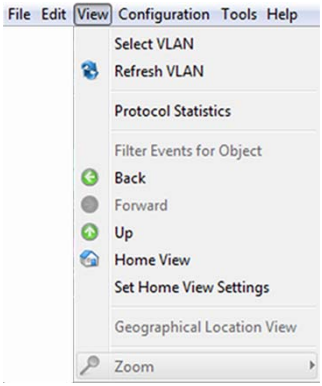


Figure 10: menu - View

4.2.4 Configuration

The “Configuration“ menu item in the menu bar contains the following selection fields:

- “Monitor“
  This dialog gives you an overview of the setting of the monitored components. (see on page 306 “Monitor”).
- “PSM Manager“
  Product-Specific Modules (PSMs) describe the properties of a device which Industrial HiVision can read for monitoring or write to for configuration.
  The PSM Manager gives you the opportunity to update PSMs or import additional PSMs beyond the ones included with delivery and remove them again.
  See “PSM Manager” on page 308.
- “Reporting“
  The reporting function allows you to manage long-term statistics outside the database of the network management system program.
  See “Reports” on page 222.

- “Scheduler“
  Scheduler offers the possibility of having repeating tasks of Industrial HiVision carried out automatically.
  See “Scheduling” on page 310.
- “Preferences“ (Ctrl+E)
  You use this selection field to enter settings for the configuration of Industrial HiVision(see on page 321 “Preferences”).
- “Change Password...“
- “Status Configuration“
  With this dialog you can perform the status configuration of component details for the devices in a device class, or for all devices.
- “Scan Ranges“
  With this dialog you can enter the scan ranges for the device discovery.
- “User defined Properties“:
  With the “User defined Properties“ function, Industrial HiVision allows you to include additional properties from the MIB of SNMP-capable devices in the management (see on page 225 “User-defined properties”).
- MultiConfig™
  The multi-configuration function (MultiConfig™) allows you to perform configurations on the device and in Industrial HiVision for:
  – one or more devices
  – one or more device properties, also for all the devices
  – one or more device details, also for all the devices
- “MAC/IP List“
  MAC/IP list of the discovered devices.
- “Refresh“ (F5)
  The “Refresh“ option allows you to update the properties or refresh selected devices.
- “IP Configuration“
  This dialog lets you configure the IP parameters of a device detected by HiDiscovery V1 without an IP address, or to change IP parameters already configured.
- “SNMP V1 Trap Destination“
  This dialog lets you configure the destination address, for SNMP V1 traps, to one of the IP addresses of your Network management station.

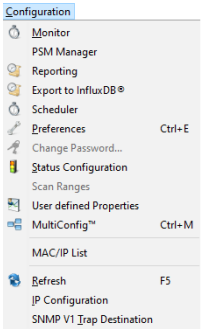


Figure 11: Menu bar – configuration

4.2.5 Tools

The “Tools“ menu item in the menu bar contains the following selection fields:

- “Dashboard“
- “Web Interface“
- “Device Configuration“
- “CLI“
- “TXCare“
- “Actions“
- “SNMP Browser“
- “Ping“
- “HiDiscovery Scan“
- “Scan Network“
- “Demo Network“
- “Calculate Availability“

You can activate menu items displayed in gray by selecting a device or property that supports this function.

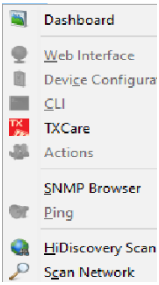


Figure 12: Menu bar – tools

4.2.6 Help

The “Help“ menu item in the menu bar contains the following selection fields:

- “Online Help“, (F1)
- “Tutorial“
- “Online“
- “Kernel Info“
- “About“

You can use the F1 key to start the online help without using the mouse.

Online Help (F1)
You select his field to start the online help of the program.

About
You select this field to open a window with information on the program.

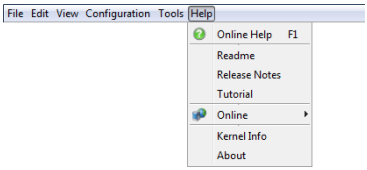


Figure 13: Menu bar – Help

4.3 Tool bar

In the tool bar you can quickly access frequently used functions by clicking on the relevant button. See “Main window of Industrial HiVision” on page 72. The tool bar contains the following selection fields:

- “Back“
- “Forward“
- “Up“
- “Home View“
- “Undo“
- “Find“
- “Edit Mode“
- “Properties“
- “WWW“
- “Scan Network“
- “HiDiscovery Scan“
- “Preferences“

Grayed-out selection fields cannot be used at the present time. This is the case, for example, if you want to use “Up“ to reach a higher level when you are already on the highest level.

4.3.1 Edit Mode

Industrial HiVision provides two operating modes. You use the “Edit Mode“ button to switch between these two operating modes. You can password protect the “Edit Mode“ button. You can use either the “Edit Mode“ password or the password from active administrators to password protect the “Edit Mode“ button.

Another way to restrict the “Edit Mode“ access, is to use the time of expiry. Here you can specify how long the edit mode is allowed to be active (see on page 370 “Program Access”).

▶ “Edit Mode“
The “Edit Mode“ is the administrative mode. Verify that you have specified at least 1 user with administrator access. To specify a user as an administrator, mark the “Login“, “Edit Mode“, “User Management“, and “Web Access“ checkboxes in the “User Management“ dialog. See “User Management” on page 329.

The following list contains some of the parameters that you can configure in the “Edit Mode“:
– network display in the graphic user interface
– monitoring parameters
– configure security parameters
– copy a network for reuse, See “Paste as new Network” on page 135.
– user management and authorization roles, See “User Management” on page 329.
– signaling device ports, See “Device and Port Signaling” on page 297.
– configure the Home View parameters, See “Set Home View Settings” on page 304.
– scheduling tasks, See “Scheduler” on page 314.
– automatic device log on, See “Web Interface” on page 436.

– configure the “Dashboard“ function, See “Dashboard” on page 419.
– functions listed in the run mode section

▶ Run Mode
The run mode is used only to monitor the network. When you specify a role that only has the “Login“ authorization, the user can only operate Industrial HiVision in the run mode. See “User Management” on page 329.

The following list contains some of the functions that you can monitor in the run mode:
– open the various tabs to view the network statuses
– start the “Dashboard“ to monitor the network, See “Dashboard” on page 419.
– use the “Find“ button to look for devices, See “Find...” on page 272.
– use the “Home View“ button to revert back to the home settings, See “Home View” on page 303.
– use the “Forward“, “Back“ and “Up“ navigation buttons
– log out of Industrial HiVision

Note: The run mode is used to avoid unintentionally writing to the Industrial HiVision parameters. The run mode is also used to avoid a database access conflict. For example, the “Edit Mode“ allows only 1 user at a time to edit the parameters in Industrial HiVision. The run mode is not intended to protect the system against unauthorized user access.
To help prohibit unauthorized user access, it is recommended that you use 'User Management' with access role permissions.

Example configuration

This example describes how you can password protect the “Edit Mode“ button.You can password protect the “Edit Mode“ button with an “Edit Mode“ password or with “User Management“. When you protect the “Edit Mode“ button with “User Management“, only active administrators can access the “Edit Mode“ using their user password

To password protect the “Edit Mode“ button with an “Edit Mode“ password, verify that the “User Management“ function is deactivated.To verify that the “User Management“ function is deactivated, proceed as follows:

☐ Open the `Preferences > Basics > User Management` dialog
☐ Verify that the “Selected Order“ list is empty.

To password protect the “Edit Mode“ button with an “Edit Mode“ password proceed as follows:

☐ Verify that you have “Edit Mode“ access.
☐ Open the `Preferences > Advanced > Program Access` dialog.
☐ Type in `test1` as the password in the `Password for Edit Mode >` Password field.
☐ Verify your password in the `Password for Edit Mode > Retype Password` field.
☐ Click the “OK“ button.

The “Edit Mode“ button is now protected with the “Edit Mode“ password. To verify the password, click the “Edit Mode“button twice. To access the “Edit Mode“ it is now necessary to type in the “Edit Mode“ password.

User management has priority over the “Edit Mode“ password. When the user management function is active, the “Edit Mode“ frame is inactive.

To password protect the “Edit Mode“ button with the “User Management“ function, proceed as follows:

☐ Verify that you have “Edit Mode“ access.
☐ Open the `Preferences > Basics > User Management` dialog.
☐ To add a new role to the “Access Roles“ frame, click the “New“ button.
☐ In the “Role Name“ field, type in the value `Admin`.
☐ To give the `Admin` role administrator authorization, mark the “Login“, “Edit Mode“, “User Management“, and “Web Access“ checkboxes.
☐ To close the dialog and add the role to the “Access Roles“ list, click the “OK“ button.
☐ To give a local user the `Admin` role, click the `Local Users > Edit` button.
☐ In the “Local Users Configuration“ dialog, click the “New“ button. The “New Entry“ dialog opens.
☐ In the “User Name“ field, type in the value `AdminUser`.
☐ In the “Password“ field, type in the value `test2`.
☐ Verify the password in the “Confirm Password“ field.
☐ Mark the `Admin` checkbox.
☐ To close the dialog and add the user to the “New Entry“ dialog, click the “OK“ button.
☐ To close the “New Entry“ dialog, click the “OK“ button.

- ☐ To activate the “local“ policy, select the “local“option from the “Selectable Policies“ list.
- ☐ Click the left arrow button ▸. The “local“ policy moves to the “Selected Order“ list.
- ☐ Click the “OK“ button.

The “Edit Mode“ button is now protected with the `AdminUser` password. To verify the password, click the “Edit Mode“button twice. To access the “Edit Mode“ it is now necessary to type in the `AdminUser` password.

Note: When you password protect the “Edit Mode“ button with the “User Management“ function, the “Edit Mode“ password is deactivated.

4.3.2 Preferences

By selecting the “Preferences“ in the tool bar you open a window with the following selection items:

- “Basics“
  Using “Basics“
  - you specify how Industrial HiVision detects devices
  - you specify how Industrial HiVision reacts to events
  - you enter passwords for accessing devices
  - you manage your Industrial HiVision licenses
- “Display“
  The “Display“ selection field enables you to specify the mode of presentation for events, devices or text.

4.4 Event line

The event line gives you information on events which are saved in the event log (see on page 112 “Event list”) and which have not been acknowledged yet. The number of events that have occurred is displayed in three fields, sorted by type. You also get more detailed information on the events, which service logged them, and when the events occurred.See “Main window of Industrial HiVision” on page 72.
In the case of an event of the error type, for example, the relevant fields in the event line are colored. In the detail display, the device affected flashes red, and in the event window the relevant event line is highlighted in red.
The user can change the standard settings for the display with color and flashing by means of the “Preferences“ menu item in the tool bar (see on page 83 “Tool bar”).

Note: Regarding security:
An attacker can spoof the Industrial HiVision browser client which can lead to unauthorized access to the Industrial HiVision kernel/web server. If you suspect that an unauthorized person has tried to access Industrial HiVision, then examine the host computer event log entries.

4.4.1 Number of events

The event line contains the number of unacknowledged events in the 3 information fields after the item “Events“.
Industrial HiVision can assign one of the 3 evaluation types to an event:

- Error: (red symbol)
  Industrial HiVision evaluates the event that has occurred as a severe error.
- Warning: (yellow symbol)
  Industrial HiVision evaluates the event that has occurred as an error that can lead indirectly to a problem in your network.
- Info: (blue symbol)
  Industrial HiVision evaluates the event that has occurred as a normal operating condition.

Figure 14: Event line – events

For every new event that occurs, Industrial HiVision increases the relevant counter by 1. When an event is acknowledged by the user, Industrial HiVision reduces the relevant counter by 1.

4.4.2 Types of events

In the three information fields after the item “Most Severe Recently“, the event line contains more detailed information on the respective event.

Designation	Meaning
Time	Date and time of the event
Source	Service for example, Industrial HiVision service
Message	Type of event for example, “New device detected by ping”

Table 3: Information on the event line

The last, most significant event is always displayed. If there is only information, then the latest information for the relevant event is displayed. If there are warnings too, then the latest warning for the relevant event is displayed. If there are also errors, then the latest message for the relevant event is displayed.

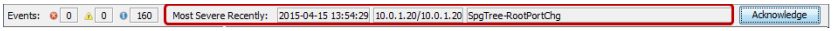


Figure 15: Event line – events – last most significant

For each new event occurring, the following is displayed:

- In the “Time“ field, the related date and the time
- In the “Source“ field, the name of the service which logged the event
- In the “Message“ field, a detailed description of the event type

You get the full listing of every event in the “Event list” on page 112. You will find the data from the event line in the columns of the event frame.

4.4.3 Acknowledge events

Use the “Acknowledge“ button in the event line to acknowledge the displayed event after you have noted it. The “Ack.“ field in the event list provides you with another option for acknowledging events.

Figure 16: Event line – events – acknowledge

After the acknowledgment, the event line (see on page 91 “Types of events”) displays the next event from the event log. You get the full listing of every event in the (see on page 91 “Types of events”). Here you can also acknowledge the relevant events in the “Ack.“ (acknowledge) column.

When an event is acknowledged by the user, the relevant counter is decreased by 1 (see on page 90 “Number of events”).

In the “Ack.“ (acknowledge) column in the “Event list” on page 112, a green check is set or the event is hidden after you acknowledge it, depending on the event filter selected.

4.4.4 Properties of an event

By clicking with the right mouse button on the event line and selecting “Properties“, you open an information window with a text on the event currently displayed.

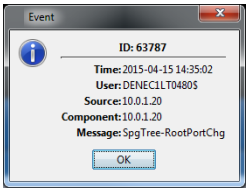


Figure 17: Event line – Events – Properties

4.5 Folder frame

In the folder frame of the Industrial HiVision program interface, you can move around like in other standard user interfaces. See “Main window of Industrial HiVision” on page 72. You can create new folders and move up and down within the hierarchy using the “Back“, “Forward“ or “Up“ buttons in the tool bar (see on page 83 “Tool bar”).

- “Back“: go back to the last position
- “Forward“: go forwards to the next position
- “Up“: go up one level

You can also access these functions under the “View“ menu item in the menu bar (see on page 77 “View”).

If you have divided your network into subdomains and configured them in Industrial HiVision (see on page 53 “Network structure”), then Industrial HiVision represents the domain structure in the top section of the folder frame.

The folders and elements listed in the folder frame are indicated by a “+” sign if they contain further subordinate elements or folders. To display them, you click on this plus sign. The subordinate elements/folders are indicated by a minus sign “-”.

To hide subordinate elements/folders again, you click on this minus sign.

In its state on delivery, Industrial HiVision contains three folders:

- “New Devices“
  In this folder, Industrial HiVision displays the newly-detected devices. This is part of the software and therefore cannot be deleted. Industrial HiVision does allow you to rename the folder.
- “Unused Devices“
  Industrial HiVision does not monitor the devices in this folder. This folder is part of the software and therefore cannot be deleted. Industrial HiVision does allow you to rename the folder. In order to decrease your network load, you can move devices which you do not need to monitor into this folder. Industrial HiVision assigns the device status "Unmanage" to devices in the “Unused Devices“ folder. To monitor a device again, move the device to the desired folder.
- “My Network“
  Industrial HiVision provides this folder for you to create your own network plan. You can rename or delete it and create new folders for your network plans.

4.6 Navigation field

You can use the navigation field to move around the topology display (see on page 97 “Detail display”).
Click the navigation rectangle and pull it to the position you want within the navigation field. Your position within the detail display changes accordingly.
See “Main window of Industrial HiVision” on page 72.
You can use the `View > Zoom` menu item in the menu bar, or right-click in the navigation field, to set the enlargement of the display in the detail frame by increments of 10%.

4.7 Detail display

In the detail display area of the Industrial HiVision user interface, you get a detail display of your network structure as a topology diagram, or in the form of a list. See “Main window of Industrial HiVision” on page 72.

Industrial HiVision allows you to move devices located in the “Map“, “List“, and “Devices“ tabs to other project folders using drag and drop. For example, after scanning your network, Industrial HiVision displays a device in the “New Devices“ folder. Using drag and drop you can move the device from the “New Devices“ folder to the “My Network“ folder. The drag and drop function allows you to move a single device or multiple devices at the same time.

4.7.1 Map

To access the topology view of the detail display, click on the “Map“ tab of the detail display.
The devices and connections in your network structure are displayed in the topology view in accordance with the presentation options you selected. By selecting and pulling while pressing the mouse button, you can move devices.

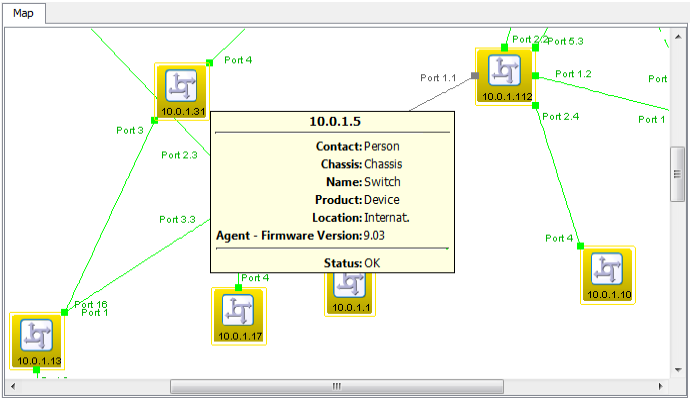


Figure 18: Detail display – “Map“

Double-click on a device/component to go down one level in the detail display (see figure 47).
The lowest level is the Component-detail-level. You recognize it by the diagram symbol.

Figure 19: Diagram symbol for a component detail

4.7.2 List

To access the list view of the detail display, click on the “List“ tab of the detail display.

The devices and connections in your network structure on this layer are displayed in a list in accordance with the presentation options you selected.

You double-click a device/component, you go down one level in the display.

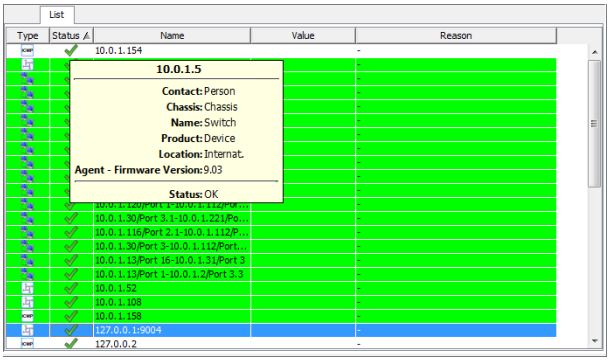


Figure 20: Detail display – “List“

4.7.3 Devices

To access the device view of the detailed display, click on the “Devices“ tab of the detailed display.
Industrial HiVision displays in a list the devices of the folder selected in the folder frame, and its subfolders. This list displays for each device:

Name	Meaning
Type	Symbol for the device
Status	Symbol for the device status
Name	Name you gave to the device in Industrial HiVision, otherwise the IP address of the device
IP Address	Management IP address
MAC Address	Management MAC address
Product	Name of the product family
Chassis	Product description
Serial Nr..	Serial number of the device
System Name	System name from the device MIB
Location	Location name that you entered in the device
Contact	Name of the contact person that you entered in the device
Firmware Version	The version of the firmware on the device
Chassis Name	Chassis name of a device with multiple management agents
Configuration Signature	Devices that support this function assign a signature to a stored configuration.
PSM up to date	This column indicates whether the data read from the device for the current PSM (Product-Specific Module) corresponds to the data in Industrial HiVision. If the data read from the device is from an earlier version of Industrial HiVision, then Industrial HiVision will re-read the data from the device in the next scan cycle.
Revision“EtherNet/IP“	If the property exist on the device, then column contains the revision number of the Ethernet/IP application.

Table 4: Meaning of the columns in the detail display of the “Devices“ tab

The selection of a class of devices offers the possibility of filtering devices of a class and tagging them at the same time. Using the MultiConfig™ function, you can configure the selected devices together.

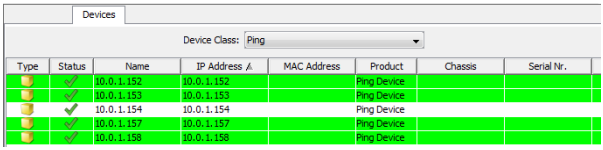


Figure 21: Detail display – “Devices“

Advanced EtherNet/IP Support

In the “Devices“ and “List“ tabs, Industrial HiVision displays additional information about the devices in your network that communicate using the EtherNet/IP protocol. Industrial HiVision displays the following EtherNet/IP devices:

- Switch
- PC
- Ping Device

The “List“ tab contains an “EtherNet/IP“ folder for the EtherNet/IP devices. When you open the folder, Industrial HiVision displays the following information:

- “Vendor ID“
- “Status“
- “State“
- “Serial Number“
- “Revision“
- “Product Name“
- “Product Code“
- “Device Type“

If the columns in the following list are empty or contain default values, then the “Devices“ tab maps the EtherNet/IP properties as described below:

- “MAC Address“ column
  Contains the MAC Address of the device.
- “Chassis“ column
  Contains the product name of the EtherNet/IP device.
- “Serial Nr.“ column
  Contains the serial number of the EtherNet/IP device.

4.7.4 Ports

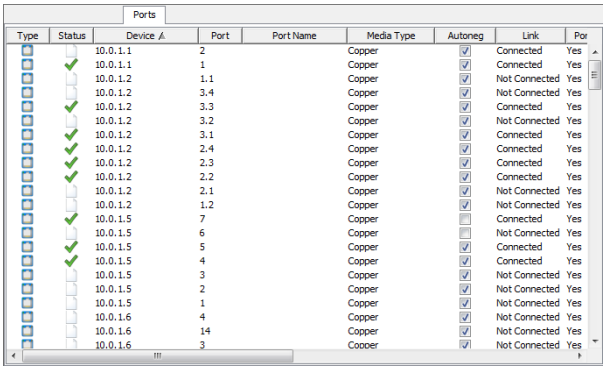
In the port view of the detail display, you click on the “Ports“ tab to go to the detail display.
Industrial HiVision displays in a list the ports of the folder/device selected in the folder frame and the subfolders in accordance with the presentation options you selected.

Name	Meaning
Type	Symbol for the port socket
Status	Symbol for the port status
Device	IP address of the device to which the port belongs
Port	Port number
Port Name	Name of the port as it is stored in the device
Media Type	Type of the connected transmission medium, for example, copper
Autoneg	Status of the autonegotiation function. A grayed-out display signifies that there is no autonegotiation function on this port.
Link	Link state of the device connected to this port
Port Enabled	Port setting: switched on or off.
Speed/Duplex	Speed and duplex transmission of the link connected to the port
User	MAC addresses of the device connected to the port. The cell displays the number of MAC addresses and multicast addresses connected to the port.
Load	Network load of the incoming data volume
SFP Power RX dBm	Displays the RX Power of the SFP transceiver, in dBm.
SFP Power TX dBm	Displays the TX Power of the SFP transceiver, in dBm.
PVID	Port VLAN ID of this port. A hyphen indicates that the device has no port VLAN function.
Ingress	Status of the ingress filter function. A grayed-out symbol indicates that the device has no ingress filter function.

Table 5: Meaning of the columns in the detail display of the ports

Name	Meaning
VLANs	The port's membership of VLANs. A number indicates the VLAN ID of the VLAN of which the port is a member. "U" stands for member of the VLAN; data packets without tag. "T" stands for member of the VLAN; data packets with tag.
VLAN Consistency Check	Industrial HiVision compares the PVID to the VLAN Egress Rules on the port. When the device does not support VLANs, Industrial HiVision displays the value "–" for the port. When the untagged VLAN Egress Rules contains the PVID and there is only one untagged entry, the port displays the value "`OK`". When there are only tagged VLAN Egress Rules, the port displays the value "`OK`". When the untagged VLAN Egress Rules do not contain the PVID, or the port has multiple untagged members, the port displays the value "`Error`". **Note:** Private VLANs erase the VLAN Egress Rules. Because the VLAN Egress Rules is empty, and therefore, the port displays the value "`Error`".

Table 5: Meaning of the columns in the detail display of the ports



Ports

Type	Status	Device	Port	Port Name	Media Type	Autoneg	Link	Por
		10.0.1.1	2		Copper	✓	Connected	Yes
	✓	10.0.1.1	1		Copper	✓	Connected	Yes
		10.0.1.2	1.1		Copper	✓	Not Connected	Yes
		10.0.1.2	3.4		Copper	✓	Not Connected	Yes
	✓	10.0.1.2	3.3		Copper	✓	Connected	Yes
		10.0.1.2	3.2		Copper	✓	Not Connected	Yes
	✓	10.0.1.2	3.1		Copper	✓	Connected	Yes
	✓	10.0.1.2	2.4		Copper	✓	Connected	Yes
	✓	10.0.1.2	2.3		Copper	✓	Connected	Yes
	✓	10.0.1.2	2.2		Copper	✓	Connected	Yes
		10.0.1.2	2.1		Copper	✓	Not Connected	Yes
		10.0.1.2	1.2		Copper	✓	Not Connected	Yes
	✓	10.0.1.5	7		Copper		Connected	Yes
		10.0.1.5	6		Copper		Not Connected	Yes
	✓	10.0.1.5	5		Copper	✓	Connected	Yes
	✓	10.0.1.5	4		Copper	✓	Connected	Yes
		10.0.1.5	3		Copper	✓	Not Connected	Yes
		10.0.1.5	2		Copper	✓	Not Connected	Yes
		10.0.1.5	1		Copper	✓	Not Connected	Yes
		10.0.1.6	4		Copper	✓	Not Connected	Yes
		10.0.1.6	14		Copper	✓	Not Connected	Yes
		10.0.1.6	3		Copper	✓	Not Connected	Yes

Figure 22: Detail display - "Ports"

4.7.5 Connections

To access the links view of the detailed display, click on the “Connections“ tab of the detailed display.
Industrial HiVision displays in a list the links of the folder selected in the folder frame and its subfolders. The list displays the following information for each link:

Name	Meaning
Status	Symbol for the link status according to the settings in the monitoring
Name	Name of the link - a name you entered for the link, or the IP address/ port number of the connected devices
Connection	Status of the link (active, inactive)
Device A	Name/IP address of device A, to which the link is connected
Port A	Port number of device A, to which the link is connected
Device B	Name/IP address of device B, to which the link is connected
Port B	Port number of device B, to which the link is connected
Load A-B	Network load of the data volume from device A to B
Load B-A	Network load of the data volume from device B to A
Speed/Duplex	Speed and duplex transmission of the link
Media Type	Type of the transmission medium of the link, for example, copper
Link Changed	Date of the last status change for the link
Config Check	Discrepancy in the settings of the ports to which the link is connected. Refer to table 7
SFP Power RX dBm A	Displays the RX Power of the SFP transceiver, in dBm, for port A
SFP Power RX dBm B	Displays the RX Power of the SFP transceiver, in dBm, for port B
SFP Power TX dBm A	Displays the TX Power of the SFP transceiver, in dBm, for port A
SFP Power TX dBm B	Displays the TX Power of the SFP transceiver, in dBm, for port B
PVID Port A	Port VLAN ID of port A. A hyphen indicates that device A has no port VLAN function.
PVID Port B	Port VLAN ID of port B. A hyphen indicates that device B has no port VLAN function.
VLANs A VLANs B	The link’s membership of VLANs. A number indicates the VLAN ID for the VLAN of which the link is a member. “U” stands for member of the VLAN; data packets without tag. A number alone stands for member of the VLAN; send data packets with tag.

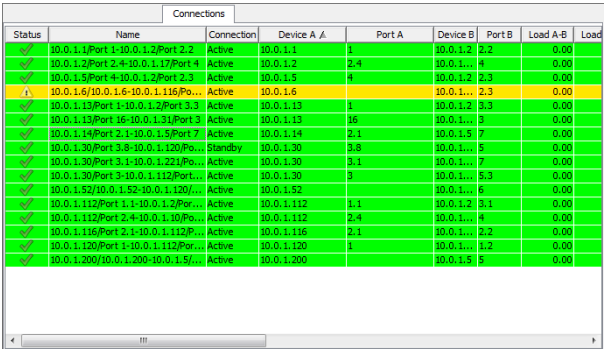
Table 6: Meaning of the columns in the detail display of the “Connections“ tab

Name	Meaning
VLAN Check	When one or both devices do not support VLANs, Industrial HiVision displays the value “-” for the connection. When the untagged VLAN Egress Rules contains the PVID and there is only one untagged entry, the port displays the value “OK”. When there are only tagged VLAN Egress Rules on both ports, and the VLAN Egress Rules are the same, the port displays the value “OK”. When the untagged VLAN Egress Rules does not contain the PVID, or the port has multiple untagged members, the port displays the value “Error”. When there are only tagged VLAN Egress Rules on both ports, and the VLAN Egress Rules are not the same, the port displays the value “Error”. When the untagged VLAN Egress Rules contains the PVID and there is only one untagged entry, but Port A and Port B have a different PVID, the ports display the value "Inconsistent"
MTBF	Mean Time Between Failure of the components participating in the link. (see on page 442 “Calculate Availability”).
MTTR	Mean Time to Repair of the components involved in the link (see on page 442 “Calculate Availability”).

Table 6: Meaning of the columns in the detail display of the “Connections“ tab

Value	Description
OK	Both of the ports connected to the link have duplex settings that match each other.
Duplex	The ports connected to the link have different duplex settings.
Empty field	Missing information

Table 7: Configuration check - meaning of the display



Connections

Status	Name	Connection	Device A	Port A	Device B	Port B	Load A-B	Load
✓	10.0.1.1/Port 1-10.0.1.2/Port 2.2	Active	10.0.1.1	1	10.0.1.2	2.2	0.00	
✓	10.0.1.2/Port 2.4-10.0.1.17/Port 4	Active	10.0.1.2	2.4	10.0.1....	4	0.00	
✓	10.0.1.5/Port 4-10.0.1.2/Port 2.3	Active	10.0.1.5	4	10.0.1.2	2.3	0.00	
!	10.0.1.6/10.0.1.6-10.0.1.116/Po...	Active	10.0.1.6		10.0.1....	2.3	0.00	
✓	10.0.1.13/Port 1-10.0.1.2/Port 3.3	Active	10.0.1.13	1	10.0.1.2	3.3	0.00	
✓	10.0.1.13/Port 16-10.0.1.31/Port 3	Active	10.0.1.13	16	10.0.1....	3	0.00	
✓	10.0.1.14/Port 2.1-10.0.1.5/Port 7	Active	10.0.1.14	2.1	10.0.1.5	7	0.00	
✓	10.0.1.30/Port 3.8-10.0.1.120/Po...	Standby	10.0.1.30	3.8	10.0.1....	5	0.00	
✓	10.0.1.30/Port 3.1-10.0.1.221/Po...	Active	10.0.1.30	3.1	10.0.1....	7	0.00	
✓	10.0.1.30/Port 3-10.0.1.112/Port...	Active	10.0.1.30	3	10.0.1....	5.3	0.00	
✓	10.0.1.52/10.0.1.52-10.0.1.120/...	Active	10.0.1.52		10.0.1....	6	0.00	
✓	10.0.1.112/Port 1.1-10.0.1.2/Por...	Active	10.0.1.112	1.1	10.0.1.2	3.1	0.00	
✓	10.0.1.112/Port 2.4-10.0.1.10/Po...	Active	10.0.1.112	2.4	10.0.1....	4	0.00	
✓	10.0.1.116/Port 2.1-10.0.1.112/P...	Active	10.0.1.116	2.1	10.0.1....	2.2	0.00	
✓	10.0.1.120/Port 1-10.0.1.112/Por...	Active	10.0.1.120	1	10.0.1....	1.2	0.00	
✓	10.0.1.200/10.0.1.200-10.0.1.5/...	Active	10.0.1.200		10.0.1.5	5	0.00	

Figure 23: Detail display – “Connections“

4.7.6 Properties

To access the properties view of the detail display, click on the “Properties“ tab of the detail display.
Industrial HiVision displays in a list a selected property of device classes for the folder/device selected in the folder frame, and its subfolders.

☐ Select a device class (e.g. Windows PC).
☐ Select a property which you want to see for the devices of the device class.

This list displays for each device in the device class:

- Status derived from the value in the right column
- Name/IP address of the device
- Device class
- Name of the queried property
- Value of the property

The “Properties“ view provides you with a quick overview -- for example, if you want to see the following:

- The software version of the devices of a device class
- The location of the devices of a device class
- The relay states
- The port properties of the Windows PCs
- etc.

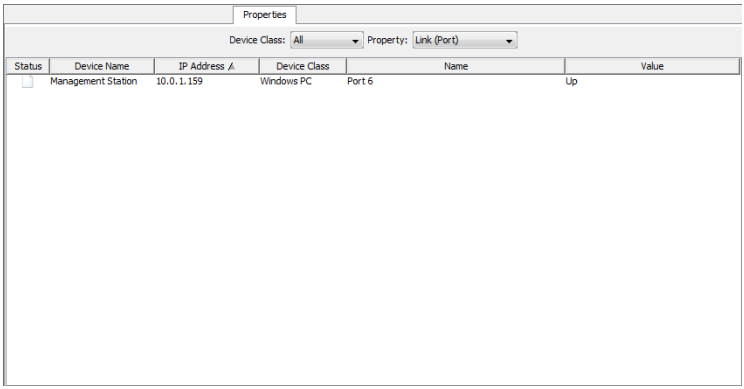


Figure 24: Detail display - “Properties“

4.7.7 Security Status

The “Security Status“ tab gives you an overview of the security properties of the devices in the selected folders.
See “Security Status” on page 204.

Figure 25: Detail display - “Security Status“

4.7.8 PoE

In the detailed view, the “PoE“ tab displays an overview of the PoE parameters for the Power over Ethernet (PoE) capable devices located in your network.

Note: The column definition in the “Device / Module“ and “Module / Port“ view depends on the PoE functions available for a particular device.

When you select a project in the folder frame, the “PoE“ tab displays the parameters of every PoE capable device located in the project. You can also filter your selection to include only the devices with the PoE function located in a specific network. To display the PoE parameters of individual devices, proceed as follows:

☐ In the folder frame, locate a device with the PoE function.
☐ Open the device to display the available properties.
☐ Click the “PoE“ property.

You can also find the PoE parameters for individual devices in the “List“ tab.

Assuming that the devices supports the various levels, you can use MultiConfig™ to specify the PoE parameters on the global, module, and port level.

▶ To access the PoE parameters on the global or module level, proceed as follows.
  ☐ Select the devices on which you wish to specify the parameters.
  ☐ Right click on a selected device.

- ☐ Select the MultiConfig™ option from the list.
- ☐ Open the `Basic Settings > PoE > Global` dialog.

▶ To specify the PoE parameters on the port level, proceed as follows.

- ☐ Select the devices on which you wish to specify the parameters.
- ☐ Open the “PoE“ tab.
- ☐ Select the ports on which you wish to specify the parameters.
- ☐ Right click on a selected port.
- ☐ Select the MultiConfig™ option.
- ☐ Open the `Basic Settings > PoE > Global` dialog.

The “Reload“ button allows you to refresh the parameters in the selected rows. When you click the “Reload“ button, Industrial HiVision triggers a polling task to retrieve the selected parameters. Depending on the network load, the reload operation can require a significant amount of time to complete the polling tasks.

Using the “View:“ drop-down list, you can display either the “Device / Module“ or “Module / Port“ properties.

The “Device / Module“ view contains the module parameters in the following columns:

Name	Meaning
Name	Displays the IP address of the device.
Operation	Displays whether the PoE function is enabled/disabled on the device.
Budget	Displays the sum of the power available for the global budget.
Remaining	Displays the remaining power. Rem Pwr= “Budget“ - “Reserved“
Reserved	Displays the global reserved power.
Delivered	Displays the actual power delivered to the modules.
Global Threshold[%]	Displays the threshold value for the power consumption of the entire device, in percent
Device Limit	Displays a warning if the device consumption exceeds the configured threshold.
Module	Displays the module number of the device.
Nominal Pwr	Displays the power available on the modules for distribution to the ports.
Max Pwr	Displays the maximum power available for the module.
Del Pwr	Displays the actual power delivered to the powered devices connected to this port.
Res Pwr	Displays the power reserved for the module according to the detected classes of the connected powered devices.
Pwr Source	Displays the power sourcing equipment for the device.
Threshold[%]	Displays the threshold value for the power consumption of the module in percent.

Table 8: Meaning of the columns in the “Device / Module“ view

Name	Meaning
Module Limit	Displays a warning symbol if the module consumption exceeds the configured threshold.
Trap Notif	Displays whether the SNMP trap sending function is enabled/disabled. When enabled, and the threshold value for the power consumption is exceeded the device sends a trap.

Table 8: Meaning of the columns in the “Device / Module“ view

Figure 26: Detail display - “PoE“ tab, “Device / Module“ view

The “Module / Port“ view contains the port parameters in the following columns:

Name	Meaning
Name	Displays the IP address of the device.
Nominal Pwr	Displays the power available on the modules for distribution to the ports.
Rem Pwr	Displays the remaining power. Rem Pwr= “Budget“ - “Reserved“
Res Pwr	Displays the power reserved for the module according to the detected classes of the connected powered devices.
Del Pwr	Displays the actual power delivered to the powered devices connected to this port.
Module	Displays the module number on the device.
Port	Displays the number of the device port.
Operation	Displays whether the PoE function is enabled/disabled on the device.
Fast Start	Displays whether the PoE Fast Startup function is activated/deactivated on the port.
Prio	Displays the port priority.
Status	Displays the status of the port Powered Device (PD) detection.
Det. Cl.	Displays the power class of the powered device connected to the port.
C0 Det.	Displays a warning symbol for ports which do not declare their power class.
C0...“C4“	Displays the current status of the classes 0 through 4 on the port.
Cons	Displays the current power consumption of the port in watts.
Pwr Limit	Displays the maximum power in watts that the port outputs.
Port Limit	Displays a warning if the port consumption exceeds the configured threshold.

Table 9: Meaning of the columns in the “Module / Port“ view

Name	Meaning
Max Cons	Displays the maximum power that the device has consumed since the last start up in watts.
Enab ASDn	Displays whether the Auto Shutdown function is activated/deactivated on the port.
Start	Displays the time at which the device disables the power for the port upon activation of the Auto Shutdown function.
End	Displays the time at which the device enables the power for the port upon activation of the Auto Shutdown function.

Table 9: Meaning of the columns in the “Module / Port“ view

You can deactivate specific port parameters at “Device / Module“ level and at “Module / Port“ level.

☐ To enable the editing mode, click “Configure Monitoring“.

☐ Activate or deactivate the required parameters.

☐ To apply the change to all the “PoE“ capable devices, modules or ports, use the “Activate all“ and “Deactivate all“ buttons.

After the parameters are deactivated, the application stops displaying warning messages related to these parameters.

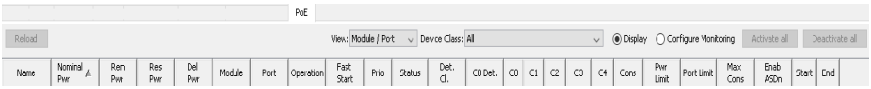


Figure 27: Detail display - “PoE“ tab, “Module / Port“ view

4.8 Event list

Industrial HiVision logs the events that relate to the program itself and to the monitored devices. (see on page 353 “Event”). There are the following main scenarios to select and display the events in the event list:

- object-based filter
- type of event/chronological filter for every object.

In the first scenario, select the number of required objects, on the map. Use the “Filter Events for Object“ button, at the top right of the event list. When you select at least one object on the map, the button becomes active. Then, to filter the events that you want Industrial HiVision to display, use the selection field at the top right of the event list. You can select from these filter options:

- “All Events“,
- “Last 24 Hours Events“,
- “Last 12 Hours Events“,
- “Unacknowledged Events“,
- “Warnings & Errors“,
- “Unacknowledged Warnings & Errors“,
- “Link Events“,
- “User Defined...“
  For user-defined events, Industrial HiVision opens the “User Defined...“ dialog, in which you can specify which events Industrial HiVision displays in the list.
  For help with the input format, hover the mouse pointer over an input field.

When you click the “Filter Events for Object“ button, Industrial HiVision displays the events of the selected object in the event list.

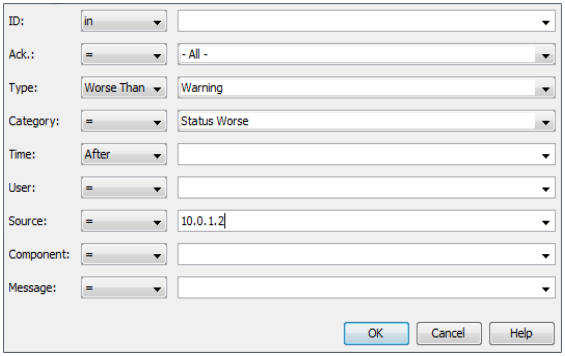


Figure 28: “User Defined...“ dialog

Note: When you enter the time, use the 24-hour clock format.

Examples of events are:
- “Application Info“,
- “Status Better“/“Status Worse“,
- “Event Acknowledge“,
- “SNMP Trap“,
- “Device Discovered“,
- and so on.

Industrial HiVision lets you write the events to an event log file. You can also display the events in the program interface.
For every event, Industrial HiVision logs the information as follows:

- An identification number,
- Whether the event was acknowledged by the user,
- The event type (Info, Warning, Error),
- The event category,
- The time the event occurred,
- The user responsible for the entry, for example, the user who acknowledged the event,
- The source that caused this entry, for example, the device that changed to a better status.

- The component that caused this entry, for example, the port for which the connection status changed back to “`Ok`” again,
- A message stating which event caused this entry.

Note: When a device changes to a better status, for example, from an `Error` type to a `Warning` type, the event list displays the `Warning` type with a yellow background.

The event list lets you acknowledge individual events, or every event at once. See figure 7 on page 73.

Right-click on a line in the event list and select an option:
☐ To acknowledge a single event, select the “Acknowledge“ item.
☐ To acknowledge every event, select the “Acknowledge All“ item.

If Industrial HiVision can relate the event to a device or a property, then double-click on a row in the event list to select the source of the event in the folder frame.

Note: The “User Intervention“ event related to, or which contains, the message “Device refresh (F5) complete” is now an “Application Info“ event with the same message. If you configured an event alarm for this “User Intervention“ event, then change the event alarm to match the new “Application Info“.

4.8.1 Event History

The “Event History“ dialog displays the same events as in the `Event List`, but in a Gantt chart. The Gantt chart has the following areas:

- a left tree,
  The left tree contains users, devices, connections and their subcomponents that enter any event in the chart.
- a right chart.
  The right chart contains a dedicated row for every subcomponent. The row is made of the events that belong to that subcomponent.

The “Event History“ dialog displays the following events:

- Status period
  Status period is a colored bar that displays the period in time during which a device property, device or connection has a specified status.
  The bar displays the status of the event with these colors:
  - Red
    A red bar displays events with the “Error” status.
  - Yellow
    A yellow bar displays events with the “Warning” status.
  - Green
    A green bar displays the time that the operated device error free.
  - Silver
    The silver bar is only available for users, devices and connections. The bar displays a summary of the subcomponents that belong to the same device or connection.

- Application events

  The “Event History“ dialog displays the application events in the application row. Application events are information about the Industrial HiVision application for example, the time that a user logged in.

- Trap events

  The “Event History“ dialog displays trap events in the component row. Trap events are information sent from a device to Industrial HiVision for example, an unreachable device, or a change in a protocol.

- User events

  The “Event History“ dialog displays events in the “User Intervention“ category, in a row related to a user.

The “Event History“ dialog displays the number of events that occurred at or around the same time on an icon. To display the text for the events, hover the mouse pointer over the icon. When the number of events displayed on an icon is more than 1, right-click on the icon and select the “Details“ option. The list also displays the time that the event occurred.

To display events in the “Event History“ dialog, proceed as follows:
- ☐ In the event filter drop-down list, select a filter for the events that you want to display.
- ☐ Click the “Event History“ button.

To display events in the “Event History“ dialog related only to a specified component, proceed as follows:
- ☐ Select the component in the “Map“ tab.
- ☐ Click the “Filter Events for Object“ button.
- ☐ Click the “Event History“ button.

If an event icon displays a number of events occurred at or around the same time, you can use the “Zoom Time Scale“ slider to stretch the time line. If you stretch the time line, then the “Event History“ dialog lists the events. The “Zoom Row Height“ slider increases and decreased the height of the row.

Note: When you delete a component from the “Map“ tab, the events that the component made stay in the event list. However, Industrial HiVision deletes the events from the “Event History“ dialog.

The list below contains a description of the checkbox and buttons in the “Event History“ dialog:
- ☐ “Fit all Events“
  The button reduces the width of the rows to display the start and end times of the events.
- ☐ “Export“
  The button allows you to export the“Export“ dialog as a PDF file.
- ☐ “Export all Pages“
  The checkbox allows you to decrease the export job to export only the components on the current screen.

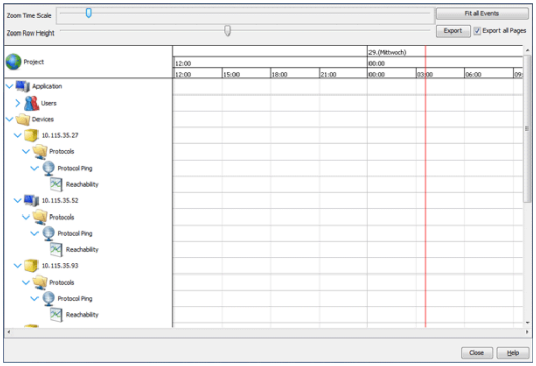


Figure 29: “Event History“ dialog

Example

You notice that the “Map“ tab displays some links down. To pinpoint the time that the status for the links changed, you can display the devices and connections in the “Event History“ dialog. To filter the “Event History“ for events related to the devices and connections proceed as follows:

☐ In the “Event History“ section, select the “User Defined...“ function from drop-down list. Industrial HiVision opens the “User Defined...“ dialog.

☐ Enter the device information in the “User Defined...“ dialog.

Note: For help with the input format, hover the mouse pointer over an input field.

– In the “ID“ row, select “in“ from the drop-down list, and enter an asterisk (`*`) in the text field.
– In the “Ack.“ row, select “in“ from the drop-down list, and enter an asterisk (`*`) in the text field.
– In the “Type“ row, select “=“ and “Warning“ from the drop-down lists.
– In the “Category“ row, select “=“ and “Status Worse“ from the drop-down lists.
– In the “Time“ row, select “Before“ from the drop-down list and enter the present time.
– In the “User“ row, select “=“ and “*” from the drop-down lists.

- In the “Source“ row, select “=“ and the IP address of the device from the drop-down list.
- In the “Component“ row, select “=“ and “*” from the drop-down lists.
- In the “Message“ row, select “=“ and “*” from the drop-down lists.

☐ To apply the filters to the “Event History“ log, click the “OK“ button. Industrial HiVision displays only the log entries that match the filter values.

☐ To open the “Event History“ dialog, click the “Event History“ button.

☐ The “Event History“ dialog displays the time that status worsened for the device.

Now that you know when the device links went down, you can find the root cause.

4.9 To navigate with the Keyboard

4.9.1 Navigating in a table

You can use the arrow keys to move up, down, right and left between the table fields in a table.
You use the tab key to move to the next table field.
With `Ctrl+Tab` you move to the next field outside the table.

4.9.2 Changing the frame

With `Tab` you move to the next frame in the program interface.

5 Creating a network plan

The monitoring of a network starts with the display of the network on the network management interface. Industrial HiVision allows you to view your network in different display variations at the same time, based on different criteria.

For example, you can set up a network plan on the following criteria:
- display the actual physical environment
- display the most important connection nodes
- is based on the topology of your network, and so on.

You can display a device in several network plans by means of copying or connections.

The network display is subdivided into the following items:

- Device detection
- Device arrangement
- Device mapping
- Device connections

Networks are generally undergoing constant modification. This involves the following activities:

- removing devices
- adding new devices, and thus
- rearranging connections.

5.1 Device detection

During the first step in setting up a network plan, Industrial HiVision supports you in discovering the following devices installed on the network (see on page 325 “Discovering devices”).

- Hirschmann BAT family
- Hirschmann OCTOPUS family
- Hirschmann GECKO family with Management
- Hirschmann Rail Switch with Management
- Hirschmann MICE family
- Hirschmann Power MICE family
- Hirschmann MACH family
- Hirschmann GREYHOUND family
- Hirschmann GES-24TP Plus
- Hirschmann EAGLE family
- Hirschmann Rail Router family
- Hirschmann Redundancy Switch family
- Hirschmann LioN-P family
- Hirschmann LioN-R family
- Hirschmann LION family
- Hirschmann Embedded Ethernet family
- Hirschmann OWL family
- Hirschmann Dragon PTN family
- Hirschmann Dragon MACH 4000 and 4500
- Hirschmann Bobcat family
- Hirschmann IT family
- Hirschmann LRS family
- Hi-SCOM-BN
- Hi-SCOM-IP66
- Magnum 5RX
- Magnum 6K
- Magnum 10KT
- Magnum DX line
- Magnum 10ETS
- Magnum 10RX
- Magnum 12KX
- Schneider Electric TCSESM, TCSESM-E, TCSESB families
- Schneider Electric TCSEFEC family

- Schneider Electric Nxx family
- Schneider Electric MCSESM, MCSESP families
- Selectron Systems ESM family
- Selectron Systems ERT family
- ABB AFF, AFS and AFR families
- INSYS MoRoS Modem, ISDN, HSPA, UMTS, GPRS, LAN, MI
- Meinberg LANTIME GPS, M300, M600
- Advantech SNMP-1000
- EPSON FX-2190, ACULASER C100N printers
- Devices with SNMP
- Windows PCs
- Devices with ICMP (Ping)

Note: Industrial HiVision detects SNMP based devices of a third party manufacturer based on the MIB II standard. As a result, Industrial HiVision represents existing interfaces of the `ifTable`, including VLAN or routing interfaces, as separate ports.

☐ Under `Configuration > Preferences > Basics > Discover Devices`, you select your preferred device discovering method.

Industrial HiVision provides 4 methods for discovering devices:

- Discovering devices using traps
  After they are switched on, the devices send a switched-on message to the network management station entered in the device. Industrial HiVision evaluates this message and displays the devices in the default map entered (see on page 324 “[Basics]”).
  This method is suitable for use during ongoing monitoring in networks where the bandwidth needs to be managed.
- Discovering devices using the HiDiscovery V1 protocol
  The HiDiscovery V1 protocol uses the MAC address to communicate with devices in the network on which the HiDiscovery V1 protocol is active. This method enables you to detect devices in your network to which you have not yet assigned a valid IP address.
  Industrial HiVision displays the devices in the default map entered (see on page 324 “[Basics]”).
  This method is suitable for when you start up a newly installed network and want to assign the IP address to the new devices.
- Discovering devices using a defined IP address range
  Using Net Scan, Industrial HiVision periodically sends Ping and SNMP requests to the devices with an IP address in the defined IP address ranges. Industrial HiVision positions the devices thus detected in the default map for this IP address range. When defining the IP address range, you can assign a default map to each IP address range (see on page 324 “[Basics]”).
  This method is suitable for monitoring a running network. Adapt the frequency of the requests to the bandwidth of your network.
- Discovering newly created devices
  Industrial HiVision allows you to create a device manually and to assign an IP address to the entry for this device. After the device is created, Industrial HiVision can send an inquiry to this IP address in order to detect it (see on page 132 “Creating new devices”).
- Discover devices from a list of IP addresses
  Industrial HiVision allows you to scan IP addresses using a text or an Microsoft Excel csv file. The “Create Devices from List“ dialog allows you to search for and upload the file to Industrial HiVision. If a device in the list is unreachable, then Industrial HiVision displays the device in the topology map as a generic device. (see on page 257 “Devices from List”)

5.1.1 Device Icons

After Industrial HiVision scans your network, the “Map“ tab displays the results. The tab displays the various icons for the devices discovered during the network scan. If the devices have a PSM assigned, then the tab displays the PSM. Otherwise, Industrial HiVision displays an icon in accordance with the status of the device.

The following list contains a description of the Industrial HiVision icons:

- Yellow cube -
  The device only responds to ping requests.
- Blue cube -
  The device responds to HiDiscovery V1 requests, but is not a Hirschmann device.
- Hirschmann icon -
  The device responds to HiDiscovery V1 requests. Industrial HiVision has determined that the device is a Hirschmann device based on the MAC address, but the device does not have a PSM.
- Unknown node icon -
  A user entered the device manually into Industrial HiVision, but the device is unreachable.
- PSM Switch -
  The device responds to SNMP requests, but Industrial HiVision does not know the Object ID.
- Windows PC -
  The device is a computer running a Windows operating system
- Linux PC -
  The device is a computer running a Linux operating system

5.1.2 TXCare

TXCare lets you monitor the Dragon PTN devices, tunnels, and services running in the tunnels. The TXCare icon displayed in Industrial HiVision represents the Dragon PTN devices, tunnels and services.

You can download the TXCare manuals from the Hirschmann document web page: www.doc.hirschmann.com

In order for you to add the TXCare icon in Industrial HiVision proceed as follows:

Perform the following steps in TXCare:

- ☐ Navigate to the `Dashboard> Tools> Add-ons> SNMP-Northbound> Configuration` tab.
- ☐ In the `Agent` frame, mark the `Enabled` checkbox.
- ☐ In the `Agent> IP Address & Port` field, type in the IP address of the PC where TXCare is running.
- ☐ You use the `Port` field to set the SNMP port that is used to communicate with Industrial HiVision. The default port setting is `161`. This is also the default setting for Industrial HiVision.
- ☐ In the `Agent` frame, mark the `SNMP v3` checkbox.
- ☐ Configure either the `admin` or `user` parameters. Configure the `admin` parameters for device management. The `user` parameters only let you monitor the device.
  - – In the `Authentication Protocol` drop-down list, select the required authentication type.
    Industrial HiVision uses either `Md5` or `sha`.
  - – In the `Encryption Protocol` drop-down list, select the required encryption type.
    Industrial HiVision uses either `None`, `Des`, or `Aes128`.

Perform the following step in Industrial HiVision:

- ☐ Open the “Map“ tab.
- ☐ To add a new device to the topology, right-click an empty place in the “Map“ tab.
  - ▶ In the drop-down list, select `New > Device`.
  - ▶ In the `IP Address > Device > IP Address` fields, type in the IP address of the PC where TXCare is running.
  - ▶ You use the `SNMP Port No` field to set the SNMP port that is used to communicate with TXCare. The default port setting is `161`. This is also the default setting for TXCare.
  - ▶ In the `Properties > Name` field, type in TXCare.
  - ▶ Click the “OK“ button.

Industrial HiVision displays the TXCare icon in the “Map“ tab.

The following worksteps explain how to monitor the “Tunnel List“ in Industrial HiVision. You monitor the “Service List“ in the same manner.

- ☐ Make 2 tunnels in TXCare, and name them `Tunnel 1` and `Tunnel 2`.
- ☐ Verify that you have the “Edit Mode“ active.
- ☐ Double click on the TXCare icon in the “Map“ tab.

- ☐ Double click on the “Tunnel List“ entry in the “List“ tab.
- ☐ In the “Properties“ dialog, click the “Status Config“ button.
- ☐ Enter the values as displayed in (see figure 30).
- ☐ To add additional rows, use the “New“ button.

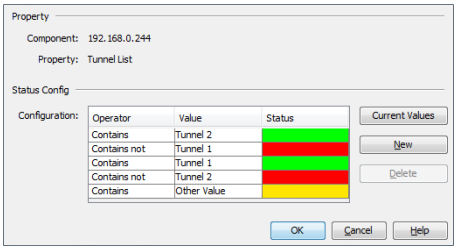
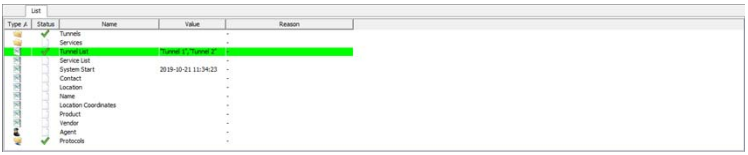


Figure 30: Status Configuration for TXCare Tunnels

The “Tunnel List“ entry in the “List“ tab displays a green checkmark as long as the entry only contains `Tunnel 1` and `Tunnel 2`. If `Tunnel 1` or `Tunnel 2` go down for any reason, then Industrial HiVision displays the entry with an error. If the entry contains another value, then Industrial HiVision displays the entry as a warning.



5.2 Assigning device icons

To visualize the devices more clearly in the detail display, Industrial HiVision allows you to assign different icons as default icons to the device types.

Figure 31: Device icons

In the state on delivery, Industrial HiVision detects a number of device types (e.g. Hirschmann devices) and assigns the corresponding device icons to these devices.
You can assign icons to other device types in the “Preferences“ dialog. To differentiate the device types, Industrial HiVision provides you with the following assignment characteristics in the device detection (see on page 366 “Device Icon”):

- System Object Identifier (SysOID)
  The SysOID denotes an MIB variable. As the SysOID of a manufacturer MIB contains the manufacturer, you can use different icons here to differentiate the devices on the manufacturer level. In the state on delivery, Industrial HiVision contains the SysOIDs for Hirschmann, Schneider, Siemens, Rockwell and Cisco.
- EtherNet/IP
  Similarly to the System Object Identifier, EtherNet/IP devices contain information about the manufacturer and the product. Here you can get Industrial HiVision to assign the icons down to the device level.

- Modbus/TCP
  Similarly to the System Object Identifier, Modbus/TCP devices contain information about the manufacturer and the product. Here you can get Industrial HiVision to assign the icons down to the device level.
- MAC Address
  The MAC address also contains manufacturer information. Depending on the manufacturer's coding depth, you can perform icon assignment from the manufacturer level down to the device type level.

5.3 Device arrangement

5.3.1 Creating a network plan

For a new network plan, you create a new folder in the folder frame.

☐ Click with the right mouse button on the globe symbol and select `New >` Folder in the drop-down list.

☐ Click with the right mouse button on the new folder and select “Properties...“ in the drop-down list. Give the new folder the name that you want to use for this network plan.
You can also change the name of a folder by selecting the folder twice or marking the folder and pressing the `F2` key. Complete the entry for the name by pressing the `Enter` key.

☐ Right-click on the new folder and select “Scan Ranges“. The “Scan Ranges“ dialog allows you to define IP address ranges. In this folder, Industrial HiVision represents newly detected devices with IP addresses from this IP address range.

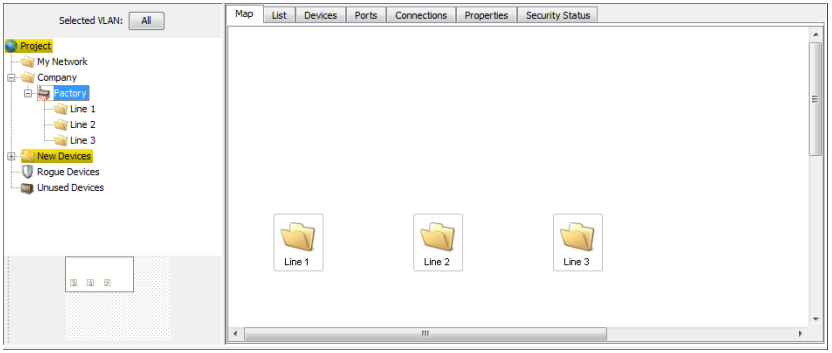


Figure 32: Example of a structure of a network plan

5.3.2 Moving devices into the network plan

Move the newly detected devices into the network plan folder.

☐ Mark these devices.

☐ Click on a device you have marked and move it onto the network plan folder in the folder frame.

5.3.3 Creating new devices

If you want to enter the network plan before the devices are installed in the network, you position new devices in the detail display.

☐ Click with the right mouse button in the detail display frame and select `New > Device` in the drop-down list.

☐ Enter the IP address of the new device in the “IP Address“ tab.
If you have selected the `Device > Scan` field, when you close the dialog with “OK“, Industrial HiVision automatically scans the network for the device.
If you selected `Device > Generate`, Industrial HiVision adds the option to create modules and ports for the device to this dialog.

If the new device is separated from the network management station by a NAT router, for example, then Industrial HiVision can communicate with the new device using the port forwarding of the NAT router.
You then enter the IP address of the NAT router and the SNMP port number of the port by means of which Industrial HiVision communicates with the new device in the “IP Address“ tab. Enter the combination of the port and the IP address of the new device in the NAT table of the NAT router.

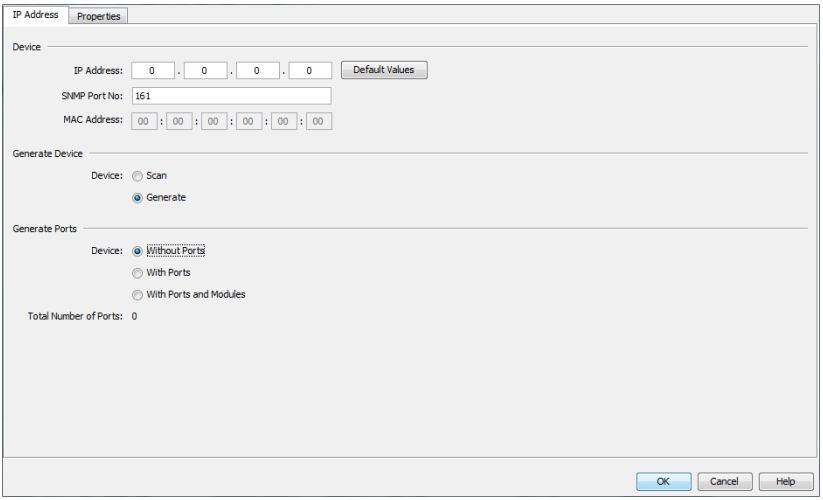


Figure 33: Entering the IP address of a new device

☐ In the “Properties“ tab you enter
- ▶ the name you want to give the device and
- ▶ the status propagation/status determination, if required (see on page 278 “Properties of a folder/device”).

☐ Select the device and press the F5 key on your keyboard, or right-click on the device, and select “Refresh“ so that Industrial HiVision detects the device in the network and calls up its data.

5.3.4 Arrange devices in the detail display

Industrial HiVision supports you in arranging the devices inside the detail display.

☐ Right-click in the detail frame and select “Auto Layout“, so that Industrial HiVision repositions the objects in the detailed display, taking your connections into account.

☐ Right-click in the detail display and select `Drawing > Line Up all Objects` to arrange the devices line-by-line.

☐ Select multiple objects in the detail frame, right-click on the detail frame, and select `Drawing > Align Tops`/`Align Bottoms`/`Align Left`/`Align Right` to line up the selected objects in rows/columns.
Here Industrial HiVision selects the outermost object as the position for the row/column.

☐ Select multiple objects in the detail frame, right-click on the detail frame, and select `Drawing > Center Horizontally`/`Center Vertically` to line up the selected objects in rows/columns.
Here Industrial HiVision selects the first object selected as the position for the row/column.

Note: If you have pushed individual objects out of the visible area by moving object groups, and if they are still contained in the folder frame, you can pull the objects back into the visible area by right-clicking in the detail window and selecting “Auto Layout“ or `Drawing > Line Up all Objects` all objects.

5.3.5 Naming devices and ports

The device/port name that Industrial HiVision displays in the folder frame or the detail display is taken from the “Properties“ dialog of the device/port by Industrial HiVision. If no name is entered, Industrial HiVision displays the management IP address for a device and the module/port number for a port.

☐ To enter the name, right-click on a device/port and select “Properties“.

The configuration settings (see on page 395 “Device/Port Names”) enable you to automatically transfer

- the device/port names from the device and
- in the case of the device name, also from the Domain Name Server (DNS) or from a private hosts file.

5.3.6 Copying devices

In order to represent different monitoring scenarios, for example, Industrial HiVision gives you the option of copying devices. For this purpose you can enter different status configurations for copied devices in the “Properties“ dialog. Industrial HiVision has one data record for each device. Every copy has its own data record. The content of the data record is taken from the original by the copy.

Example with two monitoring scenarios:

In one monitoring scenario, you want to display only events that you determine to be critical. A connection break on port 3 of device A would be critical.
In the other monitoring scenario, you want to display events relevant for maintenance. The loss of a redundant voltage supply on device A would be relevant for maintenance.

- ☐ To realize this, you create two new folders in the folder frame and give one folder the name “Critical” and the other “Maintenance”.
- ☐ Right-click on device A and select “Copy“.
- ☐ Add a copy of device A to each of the “Maintenance” and “Critical” folders.
- ☐ Double-click on the “Critical” folder to get to the component level. Double-click on port 3 to go to the detail level.
- ☐ In the dialog (see on page 285 “Properties of a component detail”),enter the relevant settings for the“Link“ detail.
- ☐ Proceed in the same way in the “Maintenance” folder.

5.3.7 Paste as new Network

When you use the “Copy“ and “Paste“ function, Industrial HiVision adds a duplicate of the original device to the selected folder. The original and duplicate refer to the same device.

When you use the “Copy“ and “Paste as new Network“ function, Industrial HiVision copies the device and pastes a new device to the selected folder. The copied device is another device.

Note: The “Paste as new Network“ function is not available for the following folders:

- ▶ “New Devices“
- ▶ “Rogue Devices“

The “Paste as new Network“ function is useful for identical networks, where the devices and connections are the same, but the IP addresses are different.

Along with the connections, the “Paste as new Network“ function also copies the device parameters. The “Paste as new Network“ function lets you select which parameters you copy to the devices of the new network. You can verify the copied parameters in the following dialogs:

- “Copy Device Credentials“
  The function copies the parameters located in the `Preferences > Device Credentials` dialog.
- “Copy Event Forwarding“
  The function copies the parameters located in the `Preferences > Event Forwarding` dialog.
- “Copy Event Actions: Alarms“
  The function copies the parameters located in the `Preferences > Event Actions > Alarms` table.
- “Copy Tasks and Schedules“
  The function copies the parameters located in the `Configuration >` Scheduler dialogs.

The prerequisites for this function are as follows:

- Industrial HiVision is in the “Edit Mode“.
- Industrial HiVision has discovered the devices you wish to copy.
- The devices you wish to copy for the new network are located in the same folder.
- You configure the connections, polling and status configurations on the original devices.
- You only use the original network for other networks with the same devices and connections.

Example Configuration:

An example for this function, is a train network. When you compare train networks, they are basically the same. If you make a copy of a train network, then you change the IP addresses and use the network for another train.

The prerequisites for the example are as follows:

- ☐ You have discovered and configured the `Train A` devices in Industrial HiVision.
- ☐ You have the devices that you wish to copy in the same folder.

- ☐ You have made a `Train Networks` folder.
- ☐ The `Train A` folder is a sub-folder of the `Train Networks` folder.

In the example that follows you copy the `Train A` folder, and wish to use the folder as the `Train B` network. To use the “Copy“ and “Paste as new Network“ function proceed as follows:

▶ Make a `Train B` sub-folder in the `Train Networks` folder
- ☐ Open the “Map“ tab of the `Train Networks` folder.
- ☐ Right-click on a blank part of the dialog.
- ☐ Select `New > Folder` from the drop-down list.
- ☐ Rename the new folder `Train B`.

▶ Copy the devices in the `Train A` folder that you wish to use in the `Train B` network.
- ☐ Open the “Map“ tab of the `Train A` folder.
- ☐ Select the devices you wish to copy.
- ☐ Right-click on a selected device.
- ☐ Select “Copy“ from the drop-down list.

▶ Paste the devices from the `Train A` folder to the `Train B` folder.
- ☐ Open the “Map“ tab of the `Train B` folder.
- ☐ Right-click on a blank part of the dialog.
- ☐ Select “Paste as new Network“ from the drop-down list.

▶ Give the `Train B` devices new IP addresses.
- ☐ Double-click the “Source IP Address“ cell in the first row of the “Copy Devices“ dialog.
- ☐ In the `Edit > IP Address of the Copy` field, enter the first IP address of the `Train B` network.
- ☐ Click the “OK“ button.
  The “Copy Devices“ dialog now displays the first IP address of the `Train B` network in the “IP Address of the Copy“ column.
- ☐ To automatically calculate the IP address of the other devices, click the “Calc with Offset“ button.
  Industrial HiVision calculates the offset as follows:
  `IP Address of the Copy` = `Source IP Address` + `IP address of the first manually set device`
- ☐ To select which parameters you wish to copy to the new devices, mark the checkboxes at the bottom of the dialog.

- ☐ To have Industrial HiVision scan the network automatically after you close the “Copy Devices“ dialog, mark the “Scan Devices after Copy“ checkbox.
- ☐ Click the “OK“ button.
  Industrial HiVision displays the devices for `Train B` with the IP addresses you entered in the “Copy Devices“ dialog.

Note: When you make new IP addresses, verify that you make unique IP addresses. Industrial HiVision displays duplicate IP addresses with a red background.

The definition for the icons in the “Type“ column are as follows:

- ▶ - the IP address is set manually.
- ▶ - the IP address is calculated.

5.3.8 Devices with multiple IP addresses

Industrial HiVision represents devices with multiple IP addresses, such as a router, as one device. In the “Properties“ dialog of the device, on the “MAC/IP Addresses“ tab, you can see which IP addresses are assigned to the device.
For unique assignment, Industrial HiVision identifies a device with only 1 IP address. If you want to identify a device with a different IP address, you delete the device in the interface and create it again with the desired IP address. After the device is updated, Industrial HiVision identifies the device with this IP address.

5.3.9 Creating a link

To display a device in a number of network plans, Industrial HiVision gives you the option of creating links from devices. Connections are particularly useful if you want to divide your network into several folders. You can then display in both network plans the device connecting the two network plans with one another. In contrast to making a copy, the link accesses the data record of the original. Every change to the original is reflected in the link.

As well as links for devices, you can also create links for components.

☐ Copy the object for which you want to create the link.

☐ Right-click on the position where you want to place the link and select “Paste as Link“.

5.4 Device connection

5.4.1 Automatically displaying the topology

The easiest way of displaying links between devices is provided by the “Auto Topology...“ function of Industrial HiVision.

☐ Select `Edit > Auto Topology...`.

☐ In the dialog for automatic topology discovery (see on page 273 “Auto Topology...”) you select how you want Industrial HiVision to execute the “Auto Topology...“ function and click “OK“.

Then Industrial HiVision queries the devices for their links. Industrial HiVision displays the detected links in the interface and starts monitoring the link state and load.

In the case of Wireless Local Area Networks (WLAN), Industrial HiVision displays wireless connections with dashed lines. Because access stations can be mobile, roaming from one access point to another is a completely normal process. Therefore, Industrial HiVision does not include the connection status in the status configuration of radio connections. Industrial HiVision detects a break in the connection to the access point after the polling time for determining the status of the access point has elapsed.

5.4.2 Connecting devices manually

After you have arranged the devices to meet your requirements, you add the connections between the devices.

☐ Click on the center of a device symbol. Click again and, holding down the mouse button, move the cursor onto the device symbol with which you want to connect the device.

5.4.3 Reshaping a connection line

Industrial HiVision allows you to reshape connection lines. Thus, for example, you can represent a HIPER-Ring just like a ring.

☐ Select the connection in order to bend the line or give it a curved shape. Depending on the shape of the connection and the selection, the following options are available to you (see bubble help):

- ▶ Add an anchor point with one click on the handle.
- ▶ Switch between “Add anchor point” and “Change shape of curve” by re-selecting the connection.
- ▶ Delete the anchor point by double-clicking.
- ▶ Change the shape of the curve using the handle.
- ▶ Straighten the connection piece with one click on the handle.

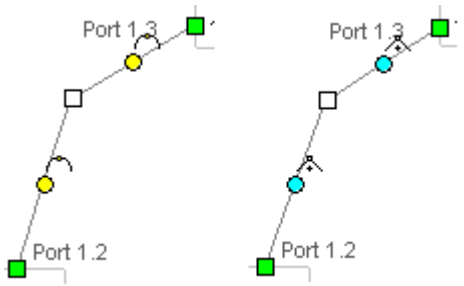


Figure 34: Reshaping a connection
- left: change shape of curve
- right: add anchor point

5.4.4 Specifying the line thickness

Depending on the selected background image, the connection lines can blend into the background. Industrial HiVision gives you the option of changing the line thickness. This enables you to make the lines more distinct from the background.
You set the line thickness globally in the menu `Preferences > Display >` Device (see on page 363 “Appearance”).

5.4.5 Other connections

In the same way as you can connect devices, Industrial HiVision also gives you the option of connecting folders and components other than symbols and text with one another. In the illustration below, (see figure 35) you will find an example of a connection with a folder.

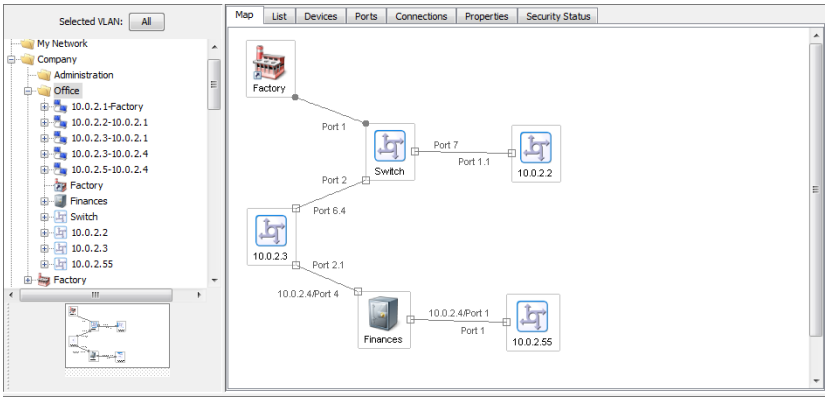


Figure 35: Connection with a folder

5.4.6 Detecting a link to another folder

Industrial HiVision uses a flag to indicate links to a device or folder outside the current folder. Beside the flag you will find information about where the link leads to. If the link has multiple destinations, Industrial HiVision groups the destinations together and the bubble help shows you the destinations.

When you double-click on the flag,

- you go directly to the port named in the destination if a single device is connected, or
- you open a drop-down list if the flag points to multiple destinations. The drop-down list shows the destination of the link. Select the link whose ports you want to go to.

Figure 36: Flags as link indicators

5.4.7 Specifying connection properties

Specify the connection properties.

☐ Right-click on a connection line and select “Properties...“ (see on page 292 “Properties of a connection”).

☐ On the “Connection“ tab you enter the ports to which the line is connected. Click your way through the tree structure until you can select the port on the device to which you are connecting the line.

☐ Also on the “Connection“ tab, select the properties you want to monitor under “Monitor“. In the default setting, Industrial HiVision automatically monitors the connection interruption, network load and port redundancy.

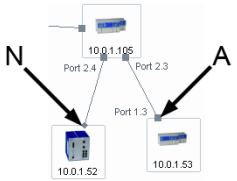


Figure 37: Monitoring state of a connection
N - No link monitoring
A - Active link monitoring

5.4.8 Link types

For clarification purposes, Industrial HiVision represents the links in different ways, according to their character.

Representation	Meaning
	Normal link
	Stand-by link
	Interrupted link
	Radio link
	Stand-by radio link
	Interrupted radio link
	Redundant Link

Table 10: Link types

5.4.9 Representation of the connection medium

Industrial HiVision enables you to identify the medium of a connection based on the icon for the connection ends (see on page 293 “Connection”).

Representation	Meaning
■	Copper
●	Optical
◆	Wireless, sawtooth line
□	Unmanaged
◀	Unknown

Table 11: Representation of the connection medium

5.5 The Network changing over time

Rarely does your network remain in a static condition. Generally, from time to time new devices are added and other devices removed and then reinserted in other positions.

5.5.1 Adding devices with HiDiscovery V1

A simple method of adding a new device is to use the HiDiscovery V1 button in the tool bar.

☐ Click on the HiDiscovery V1 button in the tool bar.
Industrial HiVision starts a network request.
Industrial HiVision displays newly detected Hirschmann devices that do not have an IP address yet in the “New Devices“ folder.
Industrial HiVision displays newly detected Hirschmann devices that already have an IP address in the default map for the address range (see on page 324 “[Basics]”).

As described on the previous pages, you can move the new devices among your network folders and create links.

Assigning the IP address

After you have added a new device for example, with HiDiscovery V1, Industrial HiVision gives you an option of assigning an IP address to the device (see on page 415 “IP Configuration”).

☐ Right-click on the device and select “IP Configuration“. With the “IP Configuration“ dialog you can enter the following parameters
– the device name
– the IP address
– the network mask
– the gateway IP address

5.5.2 Adding devices with network scan

A method of adding a new device with a previously configured IP address is provided by the “Scan Network“ button in the tool bar.

☐ Click on the “Scan Network“ button in the tool bar.
Industrial HiVision starts a network inquiry in accordance with the settings under “[Basics]” on page 324. Industrial HiVision displays newly detected devices in the default map for the address range (see on page 324 “[Basics]”).

As described on the previous pages, you can move the new devices among your network folders and create links.

5.5.3 Adding devices manually

Another option for adding a new device is to add the device manually (see on page 132 “Creating new devices”).

As described on the previous pages, you can move the new devices among your network folders and create links.

5.5.4 Startup procedure for Hirschmann devices

Industrial HiVision simplifies the startup procedure for Hirschmann devices. Apart from the installation, you can start up Hirschmann devices from your network management station:

- ☐ Detect Hirschmann devices using HiDiscovery V1 (see on page 122 “Device detection”).
- ☐ Configure the IP parameters (see on page 415 “IP Configuration”).
- ☐ Enter the trap destination address (see on page 417 “SNMP V1 Trap Destination”).
- ☐ For a new device, you use the Web interface to change the SNMP password.
- ☐ Enter the new SNMP password in Industrial HiVision (see on page 377 “Device Credentials”).

5.5.5 Interrupting device monitoring

To reduce the load on your network, Industrial HiVision provides you with the following options for interrupting the monitoring for individual devices and folders:

- ▶ Move the device into the “Unused Devices“ folder.
- ▶ Right-click on the device and select “Unmanage“ in the drop-down list. Industrial HiVision displays the device in gray.

5.5.6 Removing devices

To remove a device proceed as follows:

☐ Right-click on the device and select “Delete“ in the drop-down list (see on page 94 “Folder frame”).
Industrial HiVision allows you to delete the device or move it into the “Unused Devices“ folder.

5.5.7 Exchanging devices

In order to meet the time requirements, by degrees you will have to replace existing devices in your data network with newer devices that have new functions.
Industrial HiVision provides a conversion tool for this scenario, with which you can save the configuration of a Classic device as an XML file in a file path.
A list of the devices that support this feature can be found on the FAQ page of Hirschmann:

https://hirschmann-support.belden.com/kb/articles/how-can-i-migrate-the-configuration-of-a-powermice-to-msp

☐ Highlight the Classic device that you want to replace with a HiOS device.
☐ Select `Configuration > MultiConfig™`.
☐ In the MultiConfig™ dialog select:
`Device Settings > Advanced > Configuration Saver`
☐ Check the file path, file name and click on “Write“
Industrial HiVision saves the configuration in an XML-format file.

In the next step, migrate the saved Classic devices configuration to the HiOS device, which you previously installed and created in the network plan.

☐ Highlight the HiOS device, onto which you want to apply the configuration of the Classic device.
☐ Select `Configuration > MultiConfig™`.
☐ In the MultiConfig™ dialog select:
`Device Settings > Advanced > Configuration Migrator`
☐ Select the previously saved XML file using the file selection dialog.
☐ Check the file path and file names for the log file, in which Industrial HiVision will log the result of the migration and then click “Write“.
Industrial HiVision transfers the migrated configuration from the Classic device onto the HiOS device.
If the “Status“ column in the dialog shows that the HiOS device has rejected the configuration data, you will find information on possible causes in the log file.
You will find the path to the log file under `Configuration >` Preferences `> Advanced > Load/Save > Configuration Saver`.

5.6 Network Documentation

Industrial HiVision provides a number of functions to assist you in the documentation of your network.

5.6.1 Saving Industrial HiVision projects

Industrial HiVision allows you to save your current network data and the configuration of Industrial HiVision in a project file (see “Save” on page 259 and “Save as...” on page 260).

5.6.2 Saving reporting data

Industrial HiVision records the data of the reporting function (see on page 309 “Reporting”) in a separate database outside of the project. You will find this database in the installation directory in the subdirectory `report_db`. As this subdirectory may contain reporting databases from multiple projects, Industrial HiVision creates a subdirectory for each project therein:
`<INSTALL_DIR>/report_db/<UUID>/pm.h2.db`
You will find the UUID in the help menu in the kernel info.

5.6.3 Exporting the content of the detail display

Industrial HiVision allows you to export the content of the detail display (see on page 262 “Export...”).

☐ Choose `File > Export...` and select the file type in the “Save“ window.

5.6.4 Printing the content of the detail display

Industrial HiVision allows you to print the content of the detail display.

☐ Select `File > Print`.
Industrial HiVision creates a temporary PDF file of the content of the detail display and opens this PDF file in the PDF display program for example, Acrobat Reader, that is installed on your management station.

5.6.5 Exporting the event list

Industrial HiVision allows you to export the complete event list (see on page 262 “Export Events...”).

☐ Choose `File > Export Events...` and select the file type in the “Save“ window.

5.6.6 Printing the event list

Industrial HiVision allows you to print the complete event list.

☐ Select `File > Print Events`.
Industrial HiVision creates a temporary PDF file of the content of the detail display and opens this PDF file in the PDF display program for example, Acrobat Reader, that is installed on your management station.

5.6.7 Creating device documentation

Industrial HiVision allows you to create device documentation. In the device documentation, Industrial HiVision creates a PDF file for every device selected. The PDF file contains information about the device and its settings.

☐ In the detail window, mark the devices you want to document.

☐ In the menu bar, select `Edit > Device Documentation > Document Selected Devices` or right-click a selected device and choose “Document Selected Devices“.

☐ In the “Choose a directory for placing device documentation files“ window, enter the folder in which you want Industrial HiVision to write the PDF files and click “Select“.

For each device selected, Industrial HiVision writes a PDF file with the name: “`inventory_<IP address>.pdf`” in this folder.

5.6.8 Printing or exporting the status configuration

Industrial HiVision allows you to print or export the status configuration (see on page 404 “Status Configuration”).

☐ Select `Configuration > Status Configuration`.

☐ Click “Print“.
Industrial HiVision creates a temporary PDF file of the status configuration and opens this PDF file in the PDF display program for example, Acrobat Reader, that is installed on your management station.

☐ Click “Export“.
Industrial HiVision allows you to export the list in the following forms:
- a PDF file
- an HTML file
- a CSV file (see on page 457 “CSV export”)

5.6.9 Agent

The “Agent“ folder is found in the expanded device tree in the folder frame. The “Agent“ folder contains the following information about the PSM device discovered by Industrial HiVision:
- “GVRP“ - displays the status of the GVRP protocol
- “VLANs“ - displays the configured VLANs
- “LLDP Chassis ID“ - displays the chassis ID
- “LLDP System Name“ - displays the device name
- “Number of Users“ - displays the number of connected devices on the port
- “Base MAC Address“ - displays the MAC address of the device
- “Firmware Version“ - displays the running firmware version

- “Other Firmware Info“ contains the following information about the PSM device:
  - “Backup Firmware“- displays the stored backup firmware
  - “Stored Firmware“ - displays the current stored firmware
  - “Boot Code Firmware“ - displays the stored boot code firmware
- “Interface“ contains the following information about the PSM device:
  - “Netmask“ - displays the configured Netmask
  - “Default Gateway“ - displays the configured Default Gateway
  - “MAC Address“ - displays the MAC address of the device
  - “IP Address“ - displays the IP Address of the device
- “IP Address Conflict“ - displays the status if an IP Address Conflict occurs

6 Configuring the network

When you have your network displayed in Industrial HiVision, with your devices and connections, you can configure the devices.
The multi-configuration function (MultiConfig™) allows you to perform configurations on the device and in Industrial HiVision for:

- one or more devices
- one or more device properties, also device overlapping
- one or more device details, also device overlapping

You go to the MultiConfig™ dialog by selecting at least one device or property in the detail display and choosing `Configuration > MultiConfig™` in the menu bar.

Note: Keep in mind how this affects your system resources (see on page 228 “Effect on system resources”).

When you select objects for example, devices, ports, or connections, to configure with MultiConfig™, Hirschmann recommends that you only select objects with the following matching characteristics:

- “Device Class“
- “Product“
- “Chassis“
- “Firmware Version“

The reason for matching the characteristics, is that MultiConfig™ only displays the common supported dialogs. Displaying only common dialogs leads to a smaller number of dialogs. A smaller number of dialogs leads to fewer number of functions available for the selected objects.

Note: With different software versions on the devices, MultiConfig™ can display dialogs which are available for the selected objects. In this case, you can configure the functions in the dialogs. When you configure functions on devices with different software, warning and error messages can result depending on the object you are configuring.

6.1 Using the dialog box

The MultiConfig™ dialog contains 3 frames:

- Web-based, interface-type menu tree
- Object frame
- Function frame

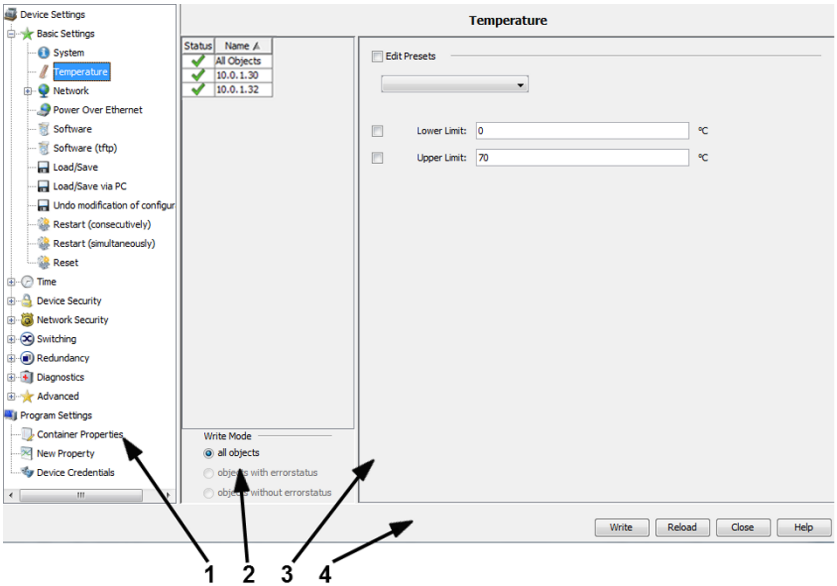


Figure 38: MultiConfig™ dialog overview
1 - Menu tree
2 - Object frame
3 - Function frame
4 - Control elements

6.1.1 Description of the menu tree

In the Web-based, interface-type menu tree, you select the function that you want to configure. Here you will find functions
– that you configure on the devices
– and properties that you configure for the monitoring in Industrial HiVision

6.1.2 Description of the object frame

The object frame contains a table of the objects that you selected for configuration in the detail display.
In the first row of the table you will find the summary of the statuses of the objects in the table.

The status symbols behind the objects have the following meanings:

Symbol	Meaning
	Industrial HiVision has read the values of the parameters and displays the matches in the function frame.
	Action initiated but not started yet.
	Industrial HiVision is reading/transferring the values of the parameters.
	Move the mouse pointer over the symbol to obtain information about any peculiarities. A peculiarity could be, for example, that a table contains hidden entries. These hidden table entries are lost when data is written.
	Industrial HiVision can reach the device. One or more values are missing from the transfer. Move the mouse pointer over the symbol to obtain information.
	The objects have not supplied any values. The connection to the device is interrupted. Move the mouse pointer over the symbol to find out the reason why you cannot read/write the values.

Table 12: Meaning of the status symbols

6.1.3 Description of the function frame

In the function frame, Industrial HiVision provides a selection of parameters and actions. Industrial HiVision selects the configurable parameters and executable actions that represent an intersection of the selected objects and the selected function.

As the number of variations for representing the parameters is too large, you will find additional application examples later on (see on page 164 “Examples for using the MultiConfig™”).

You use the selection field on the left side of the function frame to select the parameters you want to configure.

The symbols beside the selection fields, if there are any, have the following meanings (see table 13).

Symbol	Meaning
	The objects read have different values for this parameter.
	The object selected has no value for this parameter.
	Some objects have no values for this parameter.

Table 13: Meaning of the symbol beside the selection fields

To simplify entering settings that reoccur, Industrial HiVision allows you to create default settings (see on page 165 “Using contact person with default setting”).

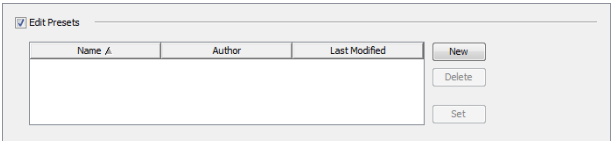


Figure 39: Default setting for the MultiConfig™ function.

Because the MultiConfig™ function provides a range of input options on different device types, Industrial HiVision allows any values to be entered in the input fields.
If Industrial HiVision detects an inconsistency during entry, Industrial HiVision changes the font color to red.

To load or save files, enter a path in the respective dialogs describing the storage location of the file. Industrial HiVision can handle absolute and relative paths. A relative path begins with `<Install-Dir>/service`.

6.1.4 Description of the control elements

- “Write“
  With “Write“ Industrial HiVision transfers the data for the parameters selected to the following locations:
  – every object contained in the table of the Object frame.
  – the objects with an error status contained in the table of the Object frame.
  – every object without an error status contained in the table of the Object frame.
  You select the objects you want to write to in the Object frame under “Write Mode“.
  When you write configuration parameters on devices in this way, these parameters are located in the temporary memory of the devices. To save the device configuration data, the last configuration step you perform is to save the new configuration on the devices.
- “Reload“
  With “Reload“, Industrial HiVision transfers the data in the selected parameters from the objects contained in the table of the object frame.
  To display the values of the parameters for an object, click on the object in the object frame.
- “Cancel“
  With “Cancel“ Industrial HiVision closes the dialog. Changes that you entered after the last “Write“ command are lost.
  Actions that have already started are completed by Industrial HiVision.
- “Help“
  With “Help“ Industrial HiVision opens the on-line help on the relevant page.
  If an example exists for the opened dialog (see on page 164 “Examples for using the MultiConfig™”), then Industrial HiVision opens the on-line help on the page for the example.

6.2 Examples for using the MultiConfig™

Depending on the menu item you select, you will find different representations in the function frame. The following examples show you the different representations.

6.2.1 Same contact person on multiple devices

You want to enter the same contact person for example, Michael, on multiple devices.

- ☐ In the detail display, open the “Map“ view or another view that displays devices.
- ☐ Select the devices on which you want to enter the same contact person.
- ☐ To open the MultiConfig™ dialog, right-click on a selected device and select “MultiConfig™”.
- ☐ In the MultiConfig™ dialog, select `Device Settings > Basic Settings >` System in the menu tree.
  You will then find the table with the related devices in the object frame, and the configurable parameters in the function frame.

Displaying current parameter values

- ☐ To display the values of the parameters for a device, click on a row of the table in the object frame.
- ☐ To display the values of the parameters that are the same on each device, click on the first row “All Objects“ of the table in the object frame.

Writing contact persons on devices

- ☐ Mark the “Contact“ checkbox.
- ☐ Enter the name of the contact person for example, Michael, in the “Contact“ text field.
- ☐ To transfer the change to the devices and temporarily save them there, click the “Write“ button.
- ☐ To save the changes to the devices into the permanent memory, select `Device Settings > Basic Settings > Load/Save`, in the menu tree.
- ☐ Select “Save to Device“, from the “Action“ drop-down list.
- ☐ Click the “Write“ button.

Using contact person with default setting

Industrial HiVision allows you to create a name as the default setting so that you do not have to enter the name again when configuring additional devices later on.

- ☐ Mark the “Contact“ checkbox.
- ☐ Enter the name of the contact person for example, Michael, in the “Contact“ text field.
- ☐ Mark the “Edit Presets“ checkbox. Industrial HiVision now opens the preset table.
- ☐ Click the “New“ button beside the preset table to enter the selected parameters as presets.
- ☐ To give the new table entry a meaningful name, double-click the name cell for this entry and enter the name for example, “Contact person Michael”.
- ☐ Click on the “Write“ button to take over the change.

From now on, you can select the “Contact person Michael” preset instead of having to select and enter the name.

- ☐ To change an existing table entry, select the desired row, change the parameters, and click “Set“.
- ☐ To select an object in the Object frame, deselect “Edit Presets“ in the Function frame.

6.2.2 Software update on similar devices

You want to perform a software update on a number of similar devices:

- ☐ In the detail display, select the “Devices“ view.
- ☐ Select the Device Class.
- ☐ Select the devices on which you want to perform the software update.
- ☐ To open the MultiConfig™ dialog, right-click on a selected device and select “MultiConfig™”.
- ☐ In the MultiConfig™ dialog, select `Device Settings > Basic Settings >` Software in the menu tree.
  You will then find the table with the related devices in the object frame, and the settings for the update in the function frame.
- ☐ To open the file selection screen, click on “File“> “`...`” in the function frame. Select the software update file or use drag & drop to pull it into the row and click the “`Open`” button.
- ☐ Mark the “Update“ and “File“ checkboxes.
- ☐ Click the “Write“ button to transfer the update to the devices.
  In the object frame, the ✔ symbol in the “Status“ column informs you that the transfer was successful.
- ☐ To activate the new software on the devices, perform a cold start on the devices (see on page 167 “Restarting multiple devices”).

6.2.3 Restarting multiple devices

With its MultiConfig™ function,Industrial HiVision offers the option of initiating a restart on multiple devices.
Industrial HiVision distinguishes between a successive “Restart (consecutively)“ and a concurrent “Restart (simultaneously)“.

- “Restart (consecutively)“
  Industrial HiVision sends a restart command to a device and waits until the device has executed the restart. Then Industrial HiVision sends the restart command to the next device.
  You select this method if the devices you want to start are connected to the network management station in a line.

- “Restart (simultaneously)“
  Industrial HiVision sends the restart command to the devices to be started nearly simultaneously. You select this method if the network management station accesses the devices directly.

  Note: Restarting a device interrupts the transfer. This means that some devices may not receive the restart command.

☐ In the MultiConfig™ dialog, select `Device Settings > Basic Settings >` Restart (consecutively) or `Device Settings > Basic Settings >` Restart (simultaneously) in the menu tree.
In the object frame, you will now find the restart options for the devices.
☐ Mark the checkboxs for example, in the “Cold Start“ row after a software update.
☐ Click the “Write“ button.

6.2.4 Loading/saving the configuration for multiple devices

Depending on the devices you have selected, Industrial HiVision gives you multiple options for transferring configurations:

Action	Load/Save	Load/Save using PC
Save on device Copy the current configuration from the non-volatile memory of the device to the permanent memory of the device.	X	
Save on TFTP server (binary) Copy the current configuration in binary form from the non-volatile memory of the device to the specified URL.	X	
Save on TFTP server (script) Copy the current configuration as an editable and readable script from the non-volatile memory of the device to the specified URL.	X	
Load from device Copy the configuration from the permanent memory of the device to the non-volatile memory of the device.	X	
Load from TFTP server Read the configuration from the specified URL to the non-volatile memory of the device.	X	
Load from TFTP server and save on device Read the configuration from the specified URL to the non-volatile and permanent memories of the device.	X	
Delete: current configuration Overwrite the configuration in the non-volatile memory of the device with the configuration in the permanent memory of the device.	X	
Delete: current configuration and from device Delete the configuration in the non-volatile memory of the device and the configuration in the permanent memory of the device, and replace with the configuration from the state on delivery. After the next restart, the IP address is also in the state on delivery.	X	
Save on PC (script) Copy the configuration as an editable and readable script from the non-volatile memory of the device to a file on the PC.		X
Save on PC (binary) Copy the configuration in binary form from the non-volatile memory of the device to a file on the PC.		X

Table 14: Transfer options for configurations

Action	Load/Save	Load/Save using PC
Load from PC (script) Read the configuration from a file as an editable and readable script from the PC to the non-volatile memory of the device.		X
Load from PC (binary) Read the configuration from a file in binary form from the PC to the non-volatile memory of the device.		X

Table 14: Transfer options for configurations

- ☐ In the detail display, open the “Map“ tab or another tab that displays the devices.
- ☐ Select the devices from which you want to save a configuration, or on which you want to load a configuration.
- ☐ To open the MultiConfig™ dialog, right-click on a selected device and select “MultiConfig™”.

The next steps describe how to save a configuration file:

- ☐ Select `Device Settings > Basic Settings > Load/Save` in the menu tree. You can also select `Device Settings > Basic Settings > Load/Save via PC`
  You can then find the table with the related devices in the object frame, and the options for transferring the configuration in the function frame.
- ☐ “Load/Save“
  - For this example, select the “Load/Save via PC“ option.
  - Select the desired transfer type from the “Action“ drop-down list.
  - Verify that the checkbox is marked.
- ☐ Mark the “File“ checkbox and enter the file name with the complete path, for example, `D:\Data\Network Management\Configurations/$CURRENT-DATE/$IP_ADDRESS.$EXTENSION` or the URL `tftp://10.0.1.159/configs/2009_10_28/$IP_ADDRESS.cfg`
  Industrial HiVision lets you enter a file name and a URL in the settings (see on page 398 “Load/Save”).
  When writing the data, Industrial HiVision creates any subfolders that are missing.

Depending on the device, Industrial HiVision lets you save a configuration file with a different profile. The next steps describe how to save a configuration file and change the profile:

☐ Select `Device Settings > Basic Settings > Load/Save > Load via PC with name`
You can then find the table with the related devices in the object frame, and the options for transferring the configuration in the function frame.

☐ “Load/Save“
- For this example, select the “Load via PC with name“ option.
- In the “File“ field, verify that the URL points to the configuration file you wish to load.
- Enter a name in the “Profile name“ field.

Save the configuration file to the non-volatile memory of the device.

☐ To transfer the data, click the “Write“ button.
In the object frame, the ✔ symbol in the “Status“ column informs you that the transfer was successful.

6.2.5 Configuring an SNMPv1 trap destination on multiple devices

You want to configure the same trap destination on multiple devices.

☐ In the detail display, open the “Map“ view or another view that displays devices.

☐ Select the devices on which you want to configure the same trap destination.

☐ To open the MultiConfig™ dialog, right-click on a selected device and select “MultiConfig™”.

☐ In the MultiConfig™ dialog, select `Device Settings > Diagnostics >` Status Config `> SNMP V1 Trap Destinations` in the menu tree.
MultiConfig™ opens a table with the related devices in the “All Objects“ frame, and a table for the trap users in the “SNMP V1 Trap Destinations“ frame.

☐ To create a new entry in the table, click “New“.

☐ Enter the IP address of the trap destination, select the active status and click “OK“.
In the table you will find the rows with the new trap destination.
☐ To transfer the changes to the non-volatile memory of the devices, click the “Write“ button.
☐ To save the changes in permanent memory of the devices, open the `Device Settings > Basic Settings > Load/Save > Save to Device` dialog in the menu tree.
☐ Click the “Write“ button.

6.2.6 Configuring SNMPv3 traps

You want to configure the same trap destination on multiple devices.

☐ In the detail display, open the “Map“ view or another view that displays devices.

Note: For security reasons, Hirschmann recommends that you use SNMPv3 traps.

Configuring an SNMPv3 trap user

The “SNMP V3 Trap Users“ are cloned from the `admin` profile located in the `Device Settings > Device Security > User Management > Users` dialog. When you make a new user, verify that you use the same authentication and encryption values as configured in the `admin` profile.

☐ Select the devices on which you want to configure the same trap user.
☐ To open the MultiConfig™ dialog, right-click on a selected device and select “MultiConfig™”.

- ☐ In the MultiConfig™ dialog, select `Device Settings > Device Security > User Management > SNMP V3 Trap Users` in the menu tree.
  MultiConfig™ opens a table with the related devices in the “All Objects“ frame, and a table for the trap users in the “SNMP V3 Trap Users“ frame.
- ☐ To create a new entry in the table, click the “New“ button.
  In the “New Entry“ dialog, perform the following steps:
- ☐ Enter a name in the “Username“ field. Use a unique name, for example, `snmpv3trap`.
- ☐ Use the same “SNMP Auth Type“, or none (-), as the user that has access to the device. This is normally the `admin` user.
- ☐ Assign a unique password for the authentication in the “Password“ field.
- ☐ Re-enter the password in the “Repeat“ field.
- ☐ Use the same “SNMP Encryption Type“, or none (-), as the user that has access to the device. This is normally the `admin` user.
- ☐ Assign a unique password for the encryption in the “Password“ field.
- ☐ Re-enter the password in the “Repeat“ field.
- ☐ To activate the user, select the “Active“ item from the “Status“ drop-down menu.
- ☐ Click the “OK“ button.

Configuring an SNMPv3 trap destination

- ☐ In the MultiConfig™ dialog, select `Device Settings > Diagnostics >` Status Config `> SNMP V3 Trap Destinations` in the menu tree.
  MultiConfig™ opens a table with the related devices in the “All Objects“ frame, and a table for the trap destinations in the “SNMP V3 Trap Destinations“ frame.
- ☐ To create a new entry in the table, click the “New“ button.
  In the “New Entry“ dialog, perform the following steps:
- ☐ Enter a unique name in the “Name“ filed. The name identifies the profile in the table.
- ☐ Enter the IP address of the management station in the “IP Address“ fields.
- ☐ In the “User Name“ field, enter the name of a user, with the profile that you wish to use, from the `Device Settings > Device Security >` User Management `> SNMP V3 Trap Users` dialog.

- ☐ Select the “Authentication, Privacy“ item from the “Security Model“ drop-down menu. If the authorization and encryption are set to “-”, then use “No Authentication, no Privacy“.
- ☐ To activate the trap destination, select the “Active“ item from the “Status“ drop-down menu.
- ☐ Click the “OK“ button.
  Industrial HiVision displays the row with the new trap destination in the table.
- ☐ To transfer the changes to the non-volatile memory of the devices, click the “Write“ button.
- ☐ To save the changes in permanent memory of the devices, open the `Device Settings > Basic Settings > Load/Save > Save to Device` dialog in the menu tree.
- ☐ Click the “Write“ button.

6.2.7 Make firewall rules on multiple devices

You can use the MultiConfig™ dialog to specify firewall rules. The MultiConfig™ dialog also lets you save the presets for the firewall rules, then upload the firewall rules on other EagleOne devices.

The MultiConfig™ Firewall Rules Table

The MultiConfig™ dialog shows an index table with rows which contain the firewall rules saved on the selected EagleOne device.
When you select multiple devices, the index table can show a subset of rules on the selected EagleOne devices. The index table identifies the subset with an “unequal” symbol. The “unequal” symbol means that the rule is different on the selected devices. The difference for the rule can be either information contained in the rule or sequence of the rules on each device. If you save presets with rules identified as “unequal”, then MultiConfig™ saves the “unequal” cell as blank. You can remove rows which contain the blank cells or enter the necessary information.
The firewall dialogs have “Up” and “Down” arrow buttons. The arrow buttons allow you to change the sequence of the rules in the index table.

Note: You cannot change the information in the rows identified as “not equal”. However, you can remove the rows from the index table.

Example

The server for the virus update files requires you to release another port in the firewalls of your company. For this, you want to add a new 1st rule for the relevant firewalls that releases this port.

Save a new rule as a preset

- ☐ In the detail display, open the “Map“ tab or another tab that shows devices.
- ☐ Right-click on the EagleOne device to which you want to add the rule(s) and select the “MultiConfig™” function from the drop-down list.
- ☐ In the menu tree of the MultiConfig™ dialog, select the relevant packet filter.
- ☐ In the function frame of the MultiConfig™ dialog, mark the “Edit Presets“ checkbox.
- ☐ To save a preset for the rules in the index table, in the “Edit Presets“ frame click the “New“ button.

  Note: If you want to save the complete content of the index table as a preset, deselect the rules in the index table. If you want to save a rule or multiple rules as a preset, in the index table select the rule(s).

- ☐ In the “Edit Presets“ table, double-click in the name cell and enter a meaningful name for the preset.
- ☐ After you enter the name, e.g. “Existing rule set”, click the “Set“ button or press the “Enter” button on your keyboard.
- ☐ After you save the rules as a preset, delete the rules in the index table.
- ☐ In the index table, make a new rule for the port release, or if necessary, make multiple rules.
- ☐ To save the new rule or multiple rules as a preset in the Industrial HiVision database, in the “Edit Presets“ frame click the “New“ button.
  - In the “Edit Presets“ table, double-click in the name cell and enter a meaningful name for the preset.
  - After you entered the name, e.g. “Virus update”, click the “Set“ button or press the “Enter” button on your keyboard.

- ☐ To restore the original rules, select the preset “Existing rules set” from the “Edit Presets“ table.
- ☐ To save the data on the device, click the “Write“ button.
  In the object frame, the ✔ symbol in the “Status“ column tells you that MultiConfig™ saved the rules to the device.

After these actions, the firewall device is in its original state, and MultiConfig™ saved the preset “Virus update” in Industrial HiVision.

- ☐ Close the MultiConfig™ dialog.

Add a new rule to the relevant firewall devices

- ☐ In the detail display, open the “Map“ tab or another tab that displays devices.
- ☐ Select the firewall devices to which you want to add this rule.
- ☐ Right-click on a selected firewall device and select “MultiConfig™”.
- ☐ To add the new rule for the port release as the first rule, you select the first rule.
  With the “Edit Presets“ checkbox unmarked, select the “Virus update” preset in the drop-down list.

Industrial HiVision adds the rules with the “Virus update” preset above the selected rule.

Note: If the rules on the devices in this dialog are identical, Industrial HiVision allows you to add the new rules above the last rule.

- ☐ To save the data on the device, click the “Write“ button.
  In the object frame, the ✔ symbol in the “Status“ column tells you that MultiConfig™ saved the rules to the device.
- ☐ Close the MultiConfig™ dialog.

General information for the Edit Presets table

- "Edit Presets" activated:
  When the mode is active you can show and edit rules.
  - To show a preset in the bottom frame, you select the preset.
  - To save the rules from the bottom frame as a preset, click the "New" button.
  - To change a preset, you select the preset from the "Edit Presets" drop-down list. Edit the rules in the bottom frame. Confirm the action with "Set".
- "Edit Presets" deactivated:
  When the mode is inactive, you can add rules.
  - To add rules from a preset to the rules in the bottom frame, select the row above which you want to add the rules in the bottom frame, and select the necessary preset.
  - To add rules from a preset to the end of the rules in the bottom frame, deselect the rows in the bottom frame and select the necessary preset.

6.2.8 Configuring the Industrial HiVision property

The availability of your transmission component has the highest priority. Therefore, you want Industrial HiVision to keep you informed if the redundancy of the supply voltage is missing.
In the standard status configuration of the power unit status of Industrial HiVision
- Industrial HiVision assigns the status "OK" to the value "Not installed".
- Industrial HiVision assigns the status "No status" to the value "Not available".

However, in both cases you want to receive the status "Warning".

☐ In the detail display, open the "Properties" tab.
☐ In the "Property:" drop-down list, select the property "Status" ("Power Supply").
☐ In the table you select the power units for which you want to change the configuration.

☐ To open the MultiConfig™ dialog, right-click on a selected row and select “MultiConfig™”.
☐ In the MultiConfig™ dialog, select “Status Config“ in the menu tree. You will then find the table with the related devices in the object frame, and the options for setting the status configuration in the function frame.
☐ Mark the following checkboxes:
– “Value“ = “Not Installed“
– “Value“ = “Unavailable“
☐ In the drop-down list for the two rows, select the status “Warning“.
☐ To save the change in Industrial HiVision, click the “Write“ button.

6.2.9 Saving reference values for each device

The MultiConfig™ function provides support when processing the same values on several devices, and also when processing individual values for several devices. An example can be found at “Configuration signature check” on page 208.

6.2.10 Password synchronization

Industrial HiVision allows you to synchronize the SNMP v1/v2 passwords with the SNMP v3 passwords. This function allows you to change the SNMP v1/v2 passwords in various dialogs at the same time. The function is useful in cases where the network is also monitored by another network management system that uses only SNMP v1/v2 for device access.

The function changes the SNMP v1/v2 passwords in the following dialogs:

▶ `MultiConfig™ > Device Security > SNMP V1/V2 > Stations`
▶ `MultiConfig™ > Program Settings > Device Credentials` for the “V1“ settings.

To synchronize the passwords proceed as follows:

- ☐ Verify that Industrial HiVision uses SNMP v3 to access the selected devices.
  - ☐ In the MultiConfig™ device frame, highlight the uppermost device.
  - ☐ Open the `MultiConfig™ > Program Settings > Device Credentials` dialog.
  - ☐ The “SNMP Version“ field displays the SNMP version used to access the device.
  - ☐ Verify every device listed in the MultiConfig™ device frame.
- ☐ Select the devices on which you wish to synchronize the passwords.
- ☐ Right click on a selected device.
- ☐ Select “MultiConfig™“ from the drop-down list.
- ☐ Open the `MultiConfig™ > Device Security > SNMP V3 > Password/ SNMP Access` dialog.
- ☐ Enter the SNMP v3 passwords in the “Read-only password (user)“ and the “Read-write password (admin)“ fields. You can reuse the current passwords or specify new password in the fields.
- ☐ Mark the “Synchronize password to v1/v2 community“ checkbox.
- ☐ Click the “Write“ button.

Note: Using the SNMP v1/v2 protocol is a security risk.

6.2.11 MultiConfig™ Search Function

The MultiConfig™ search function scans the menu tree and dialogs for a match to the word entered in the search field. The function allows you to find a function quickly. After you enter the first character in the search field, Industrial HiVision begins to search the menus tree nodes and dialogs for the character string. Industrial HiVision then displays only the menu tree nodes and dialogs with the character string in the menu tree node name or dialog.

The search function may return an empty dialog or a dialog without the word entered in the search field. The reason for this is that Industrial HiVision finds the function in a dialog, but not every device selected has the function. If a device, within a group of selected devices, does not have the function containing the search word, then Industrial HiVision hides the function.

6.2.12 MultiConfig™User Management

The MultiConfig™ “User Management“ function allows you to specify user credentials on several devices in your network at the same time. The “User Management“ function is available only on HiOS devices.

When you edit user credentials in the “User Management“ dialog, Industrial HiVision requires that you enter a “Password“. The reason for this is security. Industrial HiVision does not store device passwords nor retrieve the passwords stored on a device. The password that you enter during editing can be a new password or if known, the current password stored on the device for the specific user.

To modify the credentials of a user, high light the user, then click the “Edit“ button. The rules listed in the following table apply:

Parameter	Meaning
Access	Specifies the user with which you access the device. Industrial HiVision allows only 1 user to have access at a given time. **Note:** The following list contains the prerequisites for activating the access for a user: • Mark the “Active“ checkbox. • Specify a password. • Unmark the “User locked“ checkbox.
Username	The name of the user account. **Note:** The prerequisite for modifying the user name is that you specify a password.
Active	Activates/deactivates the user account. Possible values: ▶ `Selected` The user account is active. Industrial HiVision uses the credentials to log in to the device. ▶ `Not selected` The user account is inactive. **Note:** The prerequisite for deactivating the user is that you unmark the “Access“ checkbox.

Table 15: MultiConfig™ “User Management“

Parameter	Meaning
Password	Specifies the password with which Industrial HiVision logs in to a device. Possible values: ▶ 6..64 alphanumeric characters ▶ including the following special characters: !#$%&'()*+,-./:;<=>?@[\\]^_`{}~  When you select the “Policy Check“ checkbox, the device verifies that the password complies to the policies defined in the `Device Security > User Management > Global` dialog. **Note:** Industrial HiVision prohibits the use of 2 sequential asterisks, for example “**”.
Access Role	Specifies the access role that regulates the access to the individual functions of a device. Possible values: ▶ `unauthorized` The user is locked, and the device rejects the log in of the user. You assign this value to temporarily lock a user account. ▶ `guest` The user is only authorized to monitor the device. ▶ `auditor` The user is authorized to monitor the device and to save the log file in the Diagnostics > Report > Audit Trail dialog. ▶ `operator` The user is authorized to monitor and configure the device with the exception of security settings for device access. ▶ `administrator` The user is authorized to monitor and configure the device.

Table 15: MultiConfig™“User Management“

Parameter	Meaning
User locked	Displays whether the user account is locked due to excessive failed login attempts Possible values: ▶ `Selected` The device automatically locked the user out due to excessive failed login attempts. Only the device can mark the checkbox. ▶ `Not selected` Unlocks access to the device for the user. **Note:** The prerequisite to unlocking a user account is that you log in to Industrial HiVision as an administer.
Policy Check	Specifies whether Industrial HiVision verifies if the password is in accordance to the defined policy when it is being configured or changed. Possible values: ▶ `Selected` The device verifies that the password complies to the policy defined in the `User Management > Global` dialog. ▶ `Not selected` The device accepts the password without verification.
SNMP Auth Type	Specifies the authentication protocol that the device applies for user access via SNMPv3. Possible values: ▶ `hmacmd5` For this user account, the device uses protocol HMAC-MD5. ▶ `hmacsha` For this user account, the device uses protocol HMAC-SHA.
SNMP Encryption Type	Defines the encryption protocol that the device applies for user access via SNMPv3. Possible values: ▶ `none` No encryption ▶ `des` DES encryption ▶ `aesCfb128` AES-128 encryption

Table 15: MultiConfig™ "User Management"

6.2.13 MultiConfig™ Time Sensitive Networking

Hirschmann devices support time-aware queuing defined in IEEE 802.1 Qbv. This TSN feature allows the TSN-capable ports to transmit data packets of every traffic class scheduled relative to a defined cycle, in the gate control list. The VLAN tag of an Ethernet packet – or the port priority in case of an untagged packet – contains the priority.

The feature helps to avoid latency and congestion loss for reserved data streams. The precise synchronization of cycles and gate states using IEEE1588 (PTP) allows congestion-free and thus low-latency communication. The prerequisite is that every device in the network supports IEEE 802.1 Qbv.

To help you monitor the TSN ports, Industrial HiVision provides a TSN widget in the dashboard. You can find more information about the TSN widget in the chapter titled “TSN Schedule Widget” on page 435.

You can learn more about TSN networks in the “TSN for Dummies” book under the following URL:
https://www.belden.com/resources/knowledge/ebooks/time-sensitive-networking-for-dummies-lp

TSN Example Network

It is necessary to configure some functions on the devices before you configure the TSN schedule using MultiConfig™. To configure the devices used in the TSN network, the prerequisites for using MultiConfig™ are as follows:

- configure the VLANs and VLAN port membership
- configure the Forwarding Database for the TSN stream

For our example, we configure a parallel network to pass a mission-critical data stream between the end devices.

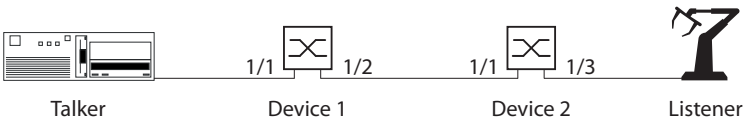


Figure 40: TSN network with TSN compatible devices

The cycle time is application specific. For our example we use the cycle time value `1000000` ns. To configure the time-specific settings for the TSN function, first determine and calculate the following delays.

- Propagation delay depends on the cable length (approximately `5` ns/m).
- Bridge delay = Reception delay + Transmission delay
  - Reception delay = Independent delay + Dependent delay of the receiving port
  - Transmission delay = Independent delay + Dependent delay of the transmitting port
- Gate open time = Propagation delay + Bridge delay
- Minimal gate open duration is the duration necessary to transmit a packet, which consists of the Service Data Unit (SDU) + 36 bytes, with the maximum possible delay.
  To calculate the minimal gate open duration, multiply the total number of bytes with a factor which depends on the TX port speed, 80 ns for 100 Mbit/s, and 8 ns for 1 Gbit/s
- When scheduling gates intended to pass a single packet, consider some internal overhead. Consider using the following overhead values, 1400 ns for 100 Mbit/s, and 180 ns for 1 Gbit/s.

Note: You can find the reception and transmission delay times for Hirschmann devices in the device documentation.

TSN Example Calculation

In the example, we use RSPE devices with the software version 07.3.00. You calculate the delays for the TSN network and devices as follows:

- The following list contains the characteristics of the Talker:
  - sends a single packet with a 300 bytes long SDU in the cycle at time t = 0.
    12 octets MAC + 4 octets VLAN + 300 octets SDU + 4 octets FCS = 320 octets long Ethernet packet

- The following list contains the characteristics of Device 1:
  - receives the packet over twisted pair copper wire on port 1/1, the port speed is 1 Gbit/s
  - the cable length between the Talker and Device 1: 10 m
  - transmits the packet over fiber cable on port 1/2, the port speed is 1 Gbit/s

Device 1 Delay			
Propagation delay		10 m × 5 ns/m	50 ns
Bridge delay (RX)	Independent delay	port 1/1	1094 ns
	Dependent delay	8 ns/oct. × 300 oct.	2400 ns
Bridge delay (TX)	Independent delay	port 1/2	530 ns
Total Bridge delay			4024 ns
Gate open time	Propagation delay		50 ns
	Total Bridge delay		4024 ns
Total gate open time			~4100 ns
Minimal gate open duration	TX port speed	8 ns/oct. × 340 oct.	2720 ns
	Internal overhead	Value for 1 Gbit/s.	180 ns
	PTP accuracy margin	1 µs	1000 ns
	Minimal gate open duration		~3900 ns

Table 16: Device 1 calculation table

- The following list contains the characteristics of Device 2.
  - receives the packet over fiber cable on port 1/1, the port speed is 1 Gbit/s
  - the cable length between Device 1 and Device 2: 50 m
  - transmits the packet over twisted pair copper wire on port 1/3, the port speed is 100 Mbit/s

Device 2 Delay			
Gate open time of Device 1			4100 ns
Bridge delay of Device 1 (TX)	Dependent delay		0 ns
Propagation delay		50 m × 5 ns/m	250 ns
Bridge delay (RX)	Independent delay	port 1/1	954 ns
	Dependent delay	8 ns/oct. × 300 oct.	2400 ns
Bridge delay (TX)	Independent delay	port 1/3[a]	9900 ns
Total Bridge delay		5040 ns + 5200 ns	13254 ns
Gate open time	Gate open time of Device 1		4100 ns
	Bridge delay of Device 1 (TX)		0 ns
	Propagation delay		250 ns
	Total Bridge delay of Device 2		13254 ns
Total gate open time			~17650 ns
Minimal gate open duration	TX port speed	80 ns/oct. × 340 oct	27200 ns
	Internal overhead	Value for 100 Mbit/s	1400 ns
	PTP accuracy margin	1 µs	1000 ns
	Minimal gate open duration		~29600 ns

Table 17: Device 2 calculation table

a. Due to the device architecture, port 1/3 has an additional packet length-dependent delay after the gate open operation.

- The following list contains the characteristics of the Listener:
  - receives the packet on a copper port, the port speed is 100 Mbit/s
  - the cable length between Device 2 and the Listener: 10 m

Listener Delay			
Gate open time of Device 2			**17650 ns**
Bridge delay of Device 2 (TX)	Dependent delay	80 ns/oct. × 300 oct.	2400 ns
Propagation delay		10 m × 5 ns/m	50 ns
Reception time	Gate open time of Device 2		17650 ns
	Bridge delay of Device 2 (TX)		24000 ns
	Propagation delay		50 ns
	PTP accuracy margin	1 µs	1000 ns

Table 18: Listener calculation table

Listener Delay	
Total receive time listener	~42700 ns

Table 18: Listener calculation table

Example Configuration

The work steps that follow describe the configuration of Device 1, configure Device 2 the same way.

When you enable the TSN function globally, the TSN-capable ports share a common Forwarding Database (FDB) which contains up to 256 entries.

The Gate Control List (GCL) determines when to open the transmission gate for the TSN data stream. The GCL contains up to 256 entries.

Note: This example assumes that the devices still have the default TSN and time synchronization settings configured.

To configure the cycle time, proceed as follows:

- ☐ Open the “Devices“ tab.
- ☐ Double-click the TSN device that you wish to use as Device 1.
- ☐ Open the “List“ tab.
- ☐ Right-click on `Port 1`.
- ☐ Select the “MultiConfig™“ option from the drop-down list.
- ☐ Open the `TSN > Configuration` dialog.
- ☐ In the “Cycle time - Configured“ field, enter the cycle time of `1000000` ns.
- ☐ To save the changes on the device, click the “Write“ button.
- ☐ Specify the parameters for Device 2.

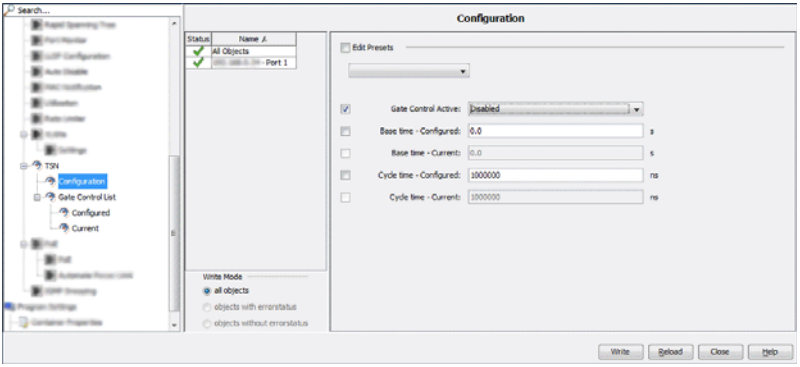


Figure 41: Enter the Cycle time

The work steps display the values calculated for Device 1 taken from table 16 on page 185. To configure the parameters for Device 2, use the values calculated in table 17 on page 186. You assign the mission-critical data to the priority 5 data stream.

- ☐ Open the `TSN > Gate Control List > Configured` dialog.
- ☐ Select row `1` and click the “Edit“ button.
- ☐ In the “Interval“ field, enter the value `4100` ns. This is the total gate open time of Device 1.
- ☐ Mark the checkboxes for every gate except for “Gate“ 5.
- ☐ Click the “OK“ button.
- ☐ To add a new row to the table for the priority 5 TSN data, click the “New“ button.
- ☐ In the “Interval“ field, enter the value `3900` ns. This is the minimal gate open duration of Device 1.
- ☐ Mark only the checkbox for “Gate“ 5.
- ☐ Click the “OK“ button.
- ☐ To allocate the remaining time to the priorities `0, 1, 2, 3, 4, 6,` and `7`, click the “New“ button. The remaining time = cycle time - (total bridge delay + minimal gate open duration).
- ☐ In the “Interval“ field, enter the value `992000` ns.
- ☐ Mark the checkboxes for every gate except “Gate“ 5.
- ☐ Click the “OK“ button.
- ☐ To save the changes on the device, click the “Write“ button.
- ☐ To close the “Configured“ dialog, click the “Close“ button.
- ☐ Specify the parameters for Device 2.

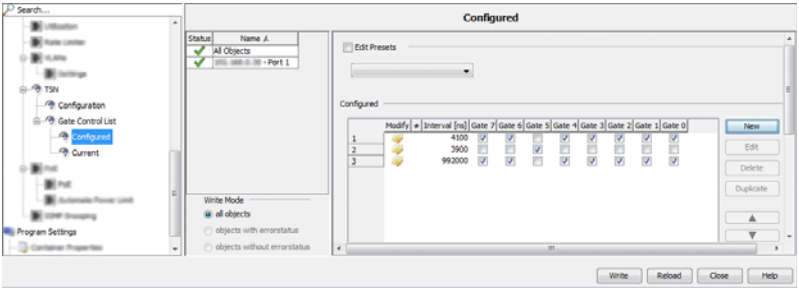


Figure 42: Device 1 `TSN > Gate Control List > Configured`

After you specified the TSN gate times, enable the PTP and TSN functions. To enable the functions proceed as follows:

- ☐ In the folder frame, right-click on the device that you configured as Device 1. To identify the folder frame, See “Main window of Industrial HiVision” on page 72.
- ☐ Select the “MultiConfig™“ option from the drop-down list.
- ☐ Open the “TSN“ dialog.
- ☐ In the “Operation“ drop-down list, select the “On“option.
- ☐ To save the changes on the device, click the “Write“ button.
- ☐ Specify the parameters for Device 2.

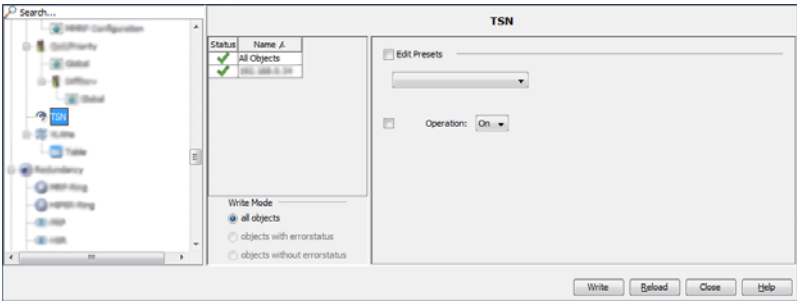


Figure 43: Enable the function

After you have enabled the functions apply the configuration changes. To apply the changes proceed as follows:

- ☐ Open the “Devices“ tab.
- ☐ Double-click the TSN device that you configured as Device 1.
- ☐ Open the “List“ tab.

- ☐ Right-click on `Port 1`.
- ☐ Select the “MultiConfig™“ option from the drop-down list.
- ☐ Open the `TSN > Configuration` dialog.
- ☐ In the “Gate Control Active“ drop-down list, select the “Enabled“ option.
- ☐ To save the changes on the device, click the “Write“ button.
- ☐ Click the “Close“ button.

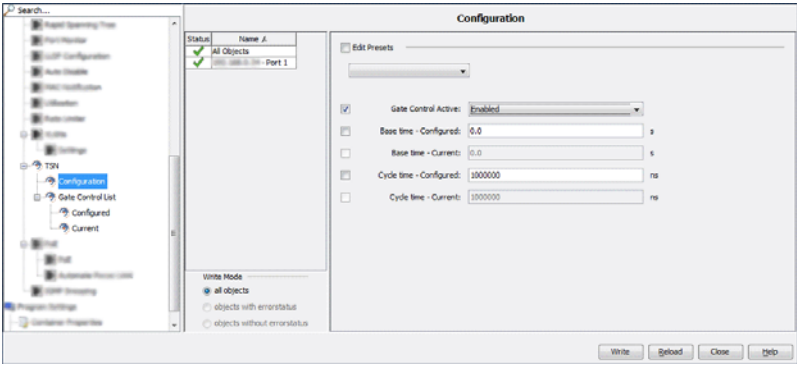


Figure 44: Enable the port and apply the configuration change

Note: You use the `TSN > Gate Control List > Current` dialog to display the setting of the device only. To display the current settings, click the “Refresh“ button.

Reception delay

Port speed	RX port	Medium	Independent delay [ns]	Dependent delay [ns]	Max. Reception delay [ns] 68 octets data packet (incl. 4 octets VLAN tag)[a] 48 octets SDU[b]	Max. Reception delay [ns] 1522 octets data packet (incl. 4 octets VLAN tag)[a] 1502 octets SDU
100 Mbit/s	1/1	Twisted pair	3920 … 3940	80 × SDU	7780	123780
	1/2	Optical	3830 … 3840	80 × SDU	7680	123680
	1/3	Twisted pair	11480 … 11690	160 × SDU	27050	251370
		Optical	11380 … 11600	160 × SDU	26960	251280

Port speed	RX port	Medium	Independent delay [ns]	Dependent delay [ns]	Max. Reception delay [ns] 68 octets data packet (incl. 4 octets VLAN tag)[a] 48 octets SDU[b]	Max. Reception delay [ns] 1522 octets data packet (incl. 4 octets VLAN tag)[a] 1502 octets SDU
1 Gbit/s	1/1 1/2	Twisted pair	1064 … 1094	8 × SDU	1478	13078
		Optical	924 … 954	8 × SDU	1338	12938
	1/3	Twisted pair	3388 … 3538	16 × SDU	4306	27506
		Optical	3238 … 3388	16 × SDU	4156	27356

a. These octets are included in the Independent delay, together with PREAMBLE, MAC addresses and FCS.
b. The VLAN tag is not part of the SDU.

Transmission delay

Port speed	TX port	Medium	Independent delay [ns]	Dependent delay [ns]	Max. Transmission delay [ns] 68 octets data packet (incl. 4 octets VLAN tag)[a] 48 octets SDU[b]	Max. Transmission delay [ns] 1522 octets data packet (incl. 4 octets VLAN tag)[a] 1502 octets SDU
100 Mbit/s	1/1 1/2	Twisted pair	1660 … 1690	0	1690	1690
		Optical	1720 … 1750	0	1750	1750
	1/3	Twisted pair	9670 … 9900	8 × SDU	13740	129740
		Optical	9730 … 9960	8 × SDU	13800	129800
1 Gbit/s	1/1 1/2	Twisted pair	530 … 550	0	550	550
		Optical	510 … 530	0	530	530
	1/3	Twisted pair	2904 … 3124	8 × SDU	3508	3892
		Optical	2884 … 3104	8 × SDU	3488	3872

a. These octets are included in the Independent delay, together with PREAMBLE, MAC addresses and FCS.
b. The VLAN tag is not part of the SDU.

6.2.14 Configure polling of device properties

This function lets you easily modify the default settings for polling and status configuration for a set of device properties. The related MultiConfig™ dialog is available for every device that supports SNMP and on which you enabled this protocol. The following categories of properties are monitored through this dialog:

- Device related properties
- Redundancy related properties
- Reachability related properties
- Protocol related properties
- Security related properties
- Port and interface related properties

To modify the polling and status configuration settings of a property related to one or more devices, perform the following steps:

- ☐ In the detail display, open the “Map“ view or another view that displays the devices.
- ☐ Select the device or devices on which you want to configure the polling and status configuration settings.
- ☐ To open the “MultiConfig™“ dialog, right-click on a selected device and select “MultiConfig™“.
- ☐ In the “MultiConfig™“ dialog, select `Program Settings > Device Monitoring` in the menu tree.
  The “Device Monitoring“ dialog opens.
- ☐ To enable the polling operation for a property, mark the related “Polling“ checkbox.
- ☐ To disable the polling operation for a property, unmark the related “Polling“ checkbox.
- ☐ To modify the time interval at which Industrial HiVision queries the device, specify the value in the “Polling Interval“ field. From the related drop-down list, select the unit of measurement for the time.
- ☐ To enable Industrial HiVision to determine the status of the property, mark the “Determine“ checkbox.
- ☐ To disable Industrial HiVision to determine the status of the property, unmark the “Determine“ checkbox.
- ☐ To enable Industrial HiVision to forward the status of the property, mark the “Forward Status Up“ checkbox.
- ☐ To disable Industrial HiVision to forward the status of the property, unmark the “Forward Status Up“ checkbox.

- ☐ The following steps are available only for the “Temperature“ (“Device“) property:
  - ☐ To modify the lower temperature threshold, specify the value in the “Threshold 1“ field.
  - ☐ To modify the upper temperature threshold, specify the value in the “Threshold 2“ field.
- ☐ To save the changes, click the “Write“ button.

Note: If minimum one of the selected devices does not support a property, then the rows related to that property are marked with a blue information icon.

Note: If none of the selected devices support a property, then the polling and status configuration settings related to that property are not displayed.

Note: If the value of a setting is different for the selected devices, then the related row is marked with a yellow flag icon. The value related to that setting is not displayed.

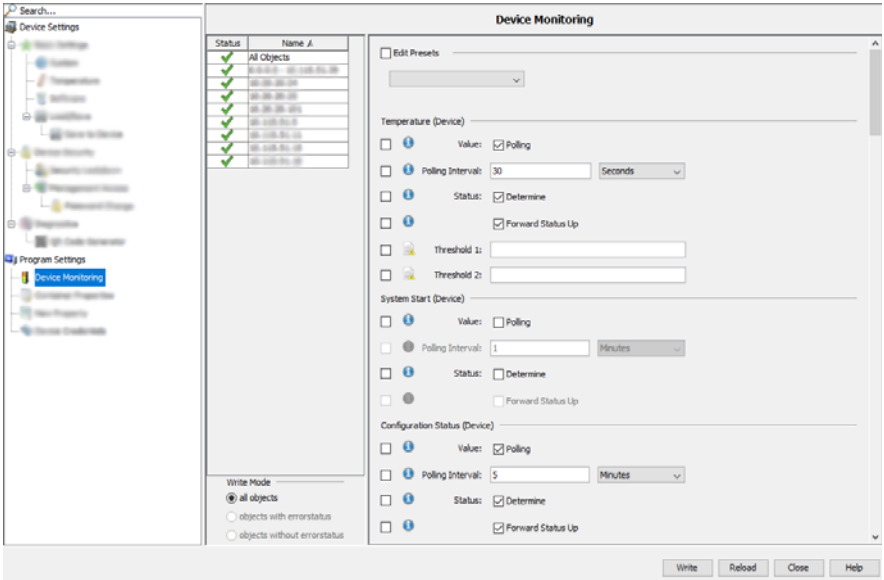


Figure 45: `MultiConfig™ > Program Settings > Device Monitoring`

6.2.15 Zero Touch Device Replacement

The “Zero Touch Device Replacement“ function helps you configure a replacement device. The function imports a previously saved device configuration from a TFTP server to the replacement device.

The replacement device gets some of the configuration information from its neighbor device. When the DHCP server function is active, and you saved the DHCP configuration information on the neighbor device, the neighbor sends the configuration information to the replacement device. The configuration information specifies, for example, which IP address, network mask, default gateway and the default path to the TFTP server.

Note: You cannot use the “Zero Touch Device Replacement“ function on a device that you configured as a router.

After you install devices in your network, it is recommended that you set up the DHCP server on the neighboring devices and save the current device configuration to the TFTP server. To set up the DHCP server on the neighboring devices and save the current device configuration to the TFTP server, perform the following steps:

- ☐ In the “Map“ tab, select the device you added to your network and its neighbors.
- ☐ Right-click on a device.
- ☐ Select the MultiConfig™ item from the drop-down list.
- ☐ Open the `Advanced > Zero Touch Device Replacement` dialog.
- ☐ Click the “Save config to tftp Server“ button.
- ☐ To activate the DHCP server function on a device and enter the configuration information of its neighboring devices to the pool table, click the “Configure DHCP Server“ button.
- ☐ On HiOS devices, beginning with release 7.0, when saving the configuration on the device, you can set up a device to also save its configuration to the TFTP server. To activate the auto-save function on a HiOS device, click the “Auto Save Config to tftp Server“ button.

  Note: The Classic Switch devices do not support the “Auto Save Config to tftp Server“ function. The Classic devices require that you manually save the configuration to the TFTP server after each change you make on the device.

There are certain prerequisites that are required before you can use the “Zero Touch Device Replacement“ function. The following list contains the prerequisites:

- ▶ You have a TFTP server installed and operational in your network,
- ▶ You entered the path to the TFTP server in the `Preferences > Load/Save > Load/Save via tftp > URL` field,
- ▶ You have discovered the devices in your network,
- ▶ You have completed an auto topology discovery,
- ▶ The topology is correct,
- ▶ You have configured the DHCP function on the neighboring devices.
- ▶ You have the configuration of the device that you wish to replace saved to the TFTP server,

- The replacement device has the same firmware version as the device you wish to replace.
- If you change the topology, then complete another auto topology discovery, reconfigure the DHCP configuration, and save the configuration to the tftp server.
- If you change the configuration of a device, then save the configuration to the TFTP server again.

The following devices support the “Zero Touch Device Replacement“ function:

- Classic Switch devices with the following firmware variants:
  - L2E
  - L2P
- HiOS devices starting with version 7.0.

Example Configuration

The following is an example of how to use the “Zero Touch Device Replacement“ function. The example network consists of Classic and HiOS devices. When you select the devices, remember that MultiConfig™ only displays the functions that the devices have in common.

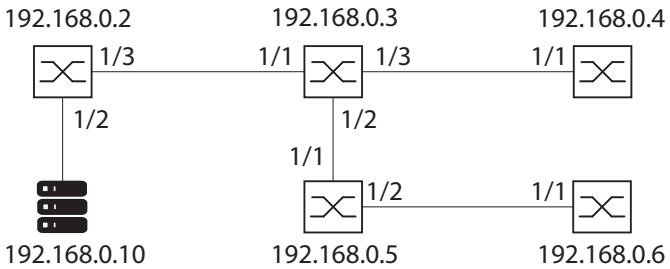


Figure 46: Network with TFTP server

The following table contains a description of the devices in the network:

Device IP	Device Description
192.168.0.2	HiOS device
192.168.0.3	HiOS device

Table 19: MultiConfig™“Zero Touch Device Replacement“

Device IP	Device Description
192.168.0.4	Classic device with firmware version L2P
192.168.0.5	Classic device with firmware version L2E
192.168.0.6	HiOS device
192.168.0.10	TFTP Server

Table 19: MultiConfig™"Zero Touch Device Replacement"

To prepare your network for the "Zero Touch Device Replacement" function, perform the following steps:

- ☐ Verify that you discovered the devices in your network, (see on page 325 "Discovering devices")
- ☐ Complete an auto topology discovery, (see on page 273 "Auto Topology...")
- ☐ Verify that the topology is correct,
- ☐ Verify that you have a TFTP server installed and running in your network,
- ☐ Open the `Preferences > Advanced > Load/Save` dialog.
- ☐ In the `Server > tftp Server` field, enter the IP address of the TFTP server, for example, `192.168.0.10`.
- ☐ Verify that the `Load/Save for Zero Touch Device Replacement >` Example URL displays the correct information, for example, `tftp://192.168.0.10/devicereplacement/<IP_address>.cfg`.
- ☐ Verify that the replacement device has the same firmware version as the device you wish to replace.

After you verify that the configuration is saved to the TFTP server, you can replace the device.

Using the same ports, install the replacement device in the network. With the device operable and connected to the network, the neighbor sends the configuration information to the replacement device. The device then gets its configuration from the tftp server.

Buttons

Parameter	Meaning
Save config to tftp Server	Saves the configuration of the selected devices to the TFTP server entered in the “URL“ field.
Auto Save Config to tftp Server	Activates the “Backup config on a remote server when saving” function on the selected devices. **Note:** This function is only available on HiOS devices.
Configure DHCP Server	Activates the "DHCP Server" function on the selected devices. Enters information about the neighbors connected to the active ports in the DHCP server of the selected device. The button also replaces outdated port information.

Table 20: MultiConfig™“Zero Touch Device Replacement“

7 Monitoring the network

The basic settings of Industrial HiVision enable you to begin monitoring your network immediately after you set up the network plan.
Important components for modifying the settings relating to the network monitoring are contained in the following list:

- Security-relevant settings
- Status configuration
- Status determination
- Trap target address
- Status forwarding
- Event actions
- History

You can find an overview of the monitored components under “Monitor” on page 306.

You can find settings for monitoring the properties of a folder/device, a component or a connection in the chapters:

- “Properties of a folder/device” on page 278
- “Properties of a connection” on page 292
- “Properties of a component detail” on page 285

7.1 Improving security on the network

An IT network offers many attack targets for uninvited intruders.
Awareness of potential security vulnerabilities and consistent closing of these security gaps enhance the security of your network.
Industrial HiVision gives you a convenient approach to configuring security-relevant settings.
The following sections show you step-by-step details how Industrial HiVision helps you to improve the security of your network.

7.1.1 Password-protecting devices on your network

Configurable network switching devices such as hubs, switches, routers, firewalls, and wireless access points are attack targets for potentially causing damage to your network.

☐ To make it more difficult to access network switching equipment management features, assign effective passwords to these devices.

Industrial HiVision gives you a multiple configuration feature that lets you assign the same password to multiple devices in a single step. But keep in mind that access protection improves with each individually assigned password.

☐ Assign new passwords to these devices periodically. Select effective passwords.

7.1.2 Password change during first time log on

To help prevent undesired access, it is crucial that you change the default password during the initial login. “min“

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

- HiOS
  07.1.00
  08.1.00
- Classic
  09.0.17
  09.1.00
- RSB
  05.4.00
- HiSecOS
  Eagle 20/30/40 03.3.00
  EagleONe 05.4.00
- GarrettCom
  DX
  DX940 4.2.0
  DX940e 1.0.3
  MN4 4.2.0

  10RX
  XRX 5.0.0

  MNS
  MNS-6k 5.1.0

Industrial HiVision gives you the ability to change the default password during initial login. When you use the `MultiConfig™ > Password Change`, dialog you can change the default password on several devices at the same time.

Example configuration

In this example, you use MultiConfig™ to change the default password on a device where it is necessary to change the default password during the initial login.

The following list contains prerequisites for changing the default password using MultiConfig™:

- the device is installed in your network
- the device has an IP address
- you discovered the device using the “HiDiscovery Scan“ button, or manually add the device with `New > Device`.

To discover devices using the “HiDiscovery Scan“ button, see “HiDiscovery Scan” on page 439.

To add devices manually, see “Creating new devices” on page 132.

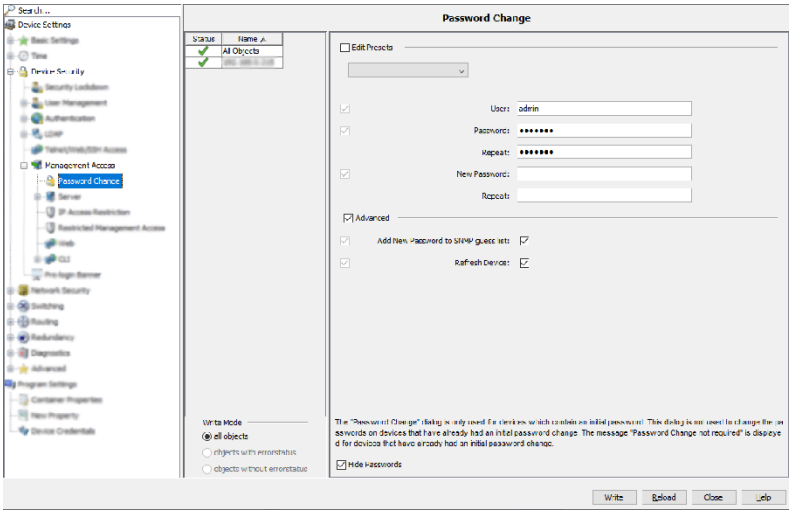
After Industrial HiVision discovers the device, Industrial HiVision displays the device as either a ping or HiDiscovery V1 device.

The following steps guide you through a password change:

- ☐ Open the “Map“ tab.
- ☐ Select the newly added devices.
- ☐ Right-click on a selected device.
- ☐ In the drop-down list, select the MultiConfig™ option.
- ☐ In the menu tree, select `Device Settings > Device Security >` Management Access `> Password Change`. The “Password Change“ dialog opens.
  - The “User“ field contains the device default user name. Industrial HiVision uses the value to log on the device.
    The default setting for this field is `admin`.
  - The “Password“ field contains the device default password. Industrial HiVision uses the value to log on the device.
    The default setting for this field is `private`.
- ☐ Type in the password that you wish to use for future access in the “New Password“ field.
  The default setting for this field is empty.
- ☐ Confirm your new password in the “Repeat“ field.
- ☐ To upload the configuration to the device, click the “Write“ button.

When you mark the “Advanced“ checkbox, the “Advanced“ frame expands where you can change other values. The settings in the “Advanced“ frame take effect after you click the “Write“ button.

- When you mark, the “Add New Password to SNMP guess list“ checkbox Industrial HiVision adds the values in the “User“ and “New Password“ fields to the `Preferences > Advanced > Device Credentials > SNMP Guess List`.
  The default setting for this checkbox is marked.
- When you mark the “Refresh Device“ checkbox, Industrial HiVision reloads the device.
  The default setting for this checkbox is marked.
- When you mark, the “Hide Passwords“ checkbox, Industrial HiVision hides or displays the passwords in plain text. This checkbox only hides or displays the passwords in the “Password Change“ dialog.
  The default setting for this checkbox is marked.



7.1.3 Security status view and configuration

Security Status

In the “Security Status“ dialog, Industrial HiVision provides an overview of the security properties of the devices in the selected folders.
The “Status“ column displays the critical condition of a property in this line.
The symbols have the following meanings:

- this property was not queried
- the results of querying this property comply with the general security policies
- the results of querying this property infringe on general security policies. Please check the settings against your general security policies.
- “-” means, that the device does not possess this function.

To configure the properties that you want Industrial HiVision to monitor, make selections in the “Configure Monitoring“ table.
The selected properties are displayed in the Status column.
The properties of the following columns can be found dependent on the device in the device sub-folder “Security“ for the respective devices:

- “Tftp“
- “Profinet IO“
- “IEC61850“
- “Inbound ANY Rule“
- “Outbound ANY Rule“
- “Time Synchronization“
- “Telnet“
- “HiDiscovery“
- “Http“
- “802.1X Port Access Control Enabled“
- “Restricted Management Access“
- “Ethernet/IP“
- “SNMP V1/V2“
- “Unused Active Ports“
- “Default Password“

Industrial HiVision queries these properties periodically (default setting: 24 hours). To instantly import the values into Industrial HiVision, click the “Refresh“ button.

In order to increase the security of your network, the MultiConfig™ function gives you the option of changing several properties with the `warning` status with one operation.

- ☐ Highlight the device rows in the table, where you want to perform changes and right click MultiConfig™.
  The “Security Lockdown“ dialog under “Device Security“ enables you to carry out several security settings at once.
- ☐ To check the affected settings in the “Security Status“ dialog, refresh the display by clicking on the “Refresh“ button. The altered properties now display the secure status 🔒 .

The “Security Status“ tab only displays the operational status of the security functions contained on a device. When you activate the security functions on the devices, you make the network as secure as possible with the available device functions. Missing or out-dated security functions on the network devices can allow an intruder to access your network. Verify that your network devices are up-to-date and that you have configured the functions in accordance with your security definitions.

Some firmware variants do not support every security function listed in the table. Since you cannot enable a missing function, the table displays the missing functions as unsecure.

Inbound ANY Rule and Outbound ANY Rule

When the “Packet Filter” function is enabled on a device, then Industrial HiVision examines the contents of the rules and displays the results in the “Security Status“ dialog.
The separation of inbound and outbound statuses is accomplished by inspecting the rule assignments on the interfaces. The default policy is also verified. If no rule applies, then the default policy determines how the firewall handles the data packets. If the default “Action“ policy is specified as “Accept“, then the status is `Unsecure`. To determine the status displayed in the “Inbound ANY Rule“ and “Outbound ANY Rule“ column, Industrial HiVision also searches the following fields for an “any” statement:

- EagleOne and EAGLE 20/30/40:
  Industrial HiVision searches the following L3 firewall rules for an “any” statement:
  “Source IP (CIDR)“ = “any“
  “Destination IP (CIDR)“ = “any“
  “Source Port“ = “any“
  “Destination Port“ = “any“
  “Protocol“ = “any“

  Industrial HiVision searches the following L2 firewall rules for an “any” statement:
  “Source IP (CIDR)“ = “any“
  “Destination IP (CIDR)“ = “any“
  “Protocol“ = “any“

For the rest of device families supported by Industrial HiVision, the “Inbound ANY Rule“ and “Outbound ANY Rule“ default status is considered `SECURE`.

Time Synchronization

Industrial HiVision verifies the clock synchronization status of each device in your network. The following list describes the configurations that cause the devices to display a warning in the “Time Synchronization“ column.

On Classic devices the “Time Synchronization“ column displays a warning if SNTP and PTP are both unsecure:

- If the device is configured as follows, then SNTP is unsecure:
  - operation off
  - operation on + client off

  - operation on + client on + accepts broadcast on
  - operation on + client on + accepts broadcast off + not synchronized
- If the device is configured as follows, then PTP is unsecure:
  - operation off
  - operation on + not synchronized

On HiOS devices the “Time Synchronization“ column displays a warning if SNTP and PTP are both unsecure:

- If the device is configured as follows, then SNTP is unsecure:
  - client off
  - operation on + client on + broadcast mode
  - operation on + client on + unicast mode + not synchronized
- If the device is configured as follows, then PTP is unsecure:
  - operation off
  - operation on + not synchronized

On HiSecOS devices the “Time Synchronization“ column displays a warning if SNTP and NTP are both unsecure:

- If the device is configured as follows, then SNTP is unsecure:
  - operation off
  - operation on + accepts broadcast on
  - operation on + accepts broadcast off + not synchronized
- If the device is configured as follows, then NTP is unsecure:
  - operation off
  - operation on + sever mode
  - operation on + client-broadcast mode
  - operation on + active symmetric mode + not synchronized
  - operation on + passive symmetric mode + not synchronized
  - operation on + client mode + not synchronized
  - operation on + client-server mode + not synchronized

On HiSecOS devices the “Time Synchronization“ column displays a warning if NTP is unsecure:

- If the device is configured as follows, then NTP is unsecure:
  - Client off
  - Client on + broadcast mode
  - Client on + unicast mode + not synchronized

7.1.4 Security-related settings of devices on the network

Disabling HiDiscovery V1

The HiDiscovery V1 protocol uses Ethernet to give you the ability to assign a device, a device name and IP parameters. To keep this assignment as easy as possible, HiDiscovery V1 does not include a mechanism to limit access to the devices.

Note: When you have the HiDiscovery V1 function enabled on a device, the “Security Status“ tab displays the device and function as unsecure.

☐ To limit access and modifications to the IP parameters and devices names of the devices on your network, disable HiDiscovery V1 on the devices as soon as you finish device configurations.
The MultiConfig™ function lets you deactivate HiDiscovery V1 on several devices in a single step.
- Highlight several devices.
- Right-click on a highlighted device and select the MultiConfig™ option from the drop-down list.
- Open the Under `Device Settings > Basic Settings > Network >` Global dialog.
  To disable HiDiscovery V1 on Classic devices, in the “HiDiscovery Access“ drop-down list, select the “Disable“ option.
  To disable HiDiscovery V1 on HiOS devices, unmark the “HiDiscovery Enable“ checkbox.

Note: The checkbox on the left side of the function names only displays a change to the function.

Configuration signature check

Classic devices from Hirschmann supply device configurations with an individual configuration signature.
HiOS devices from Hirschmann provide device configurations with an individual fingerprint.
The configuration signature changes every time you save a configuration on the device, even if the existing configuration remains the same.

The fingerprint changes when you save a configuration on the device and the existing configuration is altered.
The device saves the randomly generated configuration signature / fingerprint together with the configuration.
Industrial HiVision allows you to monitor the configuration signature / fingerprint. You are consequently in the picture if someone changes the configuration of a device.

- ☐ To select the devices with a configuration signature / fingerprint, open to the detail view in the “Properties“ tab. Use the “Property:“ drop-down list to select the "Configuration Signature (Device)" option.
- ☐ Highlight the devices in the table, where you want to monitor the configuration signature / fingerprint.
- ☐ Right-click on the device and select MultiConfig™.
- ☐ In the MultiConfig™ menu tree, click the “Status Config“ option.
- ☐ In the MultiConfig™ function frame, click the “Set current to reference“ option.
- ☐ In the “Reference Value“ frame, select the status, which the property is supposed to adopt, if a current value is different from the reference value.
- ☐ To adopt the current configuration signature / fingerprint as a reference in Industrial HiVision click the “Write“ button.

Port Security

The port security feature allows you to specify, which device is permitted to send data to this port. Thus enabling you to block the receipt of data from other devices.
The MultiConfig™ dialog from Industrial HiVision provides support while configuring the port security feature of Classic devices.

Loading device certificates / keys

When you want to communicate with a device, in some circumstances you want to know whether you are really communicating with the genuine device. Certificates exist to verify the authenticity of devices.
Certification Authorities (CA) provide such certificates for example, Verisign, Symantic. Some companies maintain their own institution with a separate server, which issues proprietary certificates.
Industrial HiVision allows you, using the MultiConfig™ dialog, the opportunity to upload certificates to devices.

Using a separate certificate for each device, provides you with greater security than if you were to use one certificate for several devices.

☐ In the “Map“ tab, right-click on the device whose certificate you want to upload to the device and select MultiConfig™.
In the menu tree of the MultiConfig™ dialog, you can find the dialogs for uploading the certificates/keys under `Device Settings > Device Security > Management Access > Server`.

7.1.5 Configuring security-relevant settings on the network

Security Lockdown

The “Security Lockdown“ function (access restrictions) gives you the ability to apply security features that already exist on Hirschmann devices at the push of a button on the managed or selected devices.
The degree of restriction is oriented on the current conditions in the network. In other words, current network operations are maintained, but additional access are restricted.
The “Security Lockdown“ function includes the following security functions, assuming the devices support the functions:

- Restricted management access
  Industrial HiVision restricts management access to the devices on the network management station. In as-delivered condition, any IP address is open to access.
- Port security
  Industrial HiVision enables the port security feature on ports associated with a MAC address.
  If the MAC address is invalid for a connection for example, due to a timeout, the device performs a selectable and configurable action. Such an action could for example, send a trap to the network management station.
  This function is disabled in as-delivered condition.

- Port security action
  If the device detects an unauthorized access attempt, the device performs the action that you configured previously.
  The possible actions are:
  – Do nothing
  – Disable port
  – Send trap
  – Disable port and send trap
- Disable unused ports
  Industrial HiVision disables the unused ports on a device.
- Disable unused slots
  Industrial HiVision disables those slots of a modular device on which the device does not discover a module.
- Disable unsecure protocols
  Various protocols are used to access devices on the network for management. Industrial HiVision disables the protocols that are considered to be unsecure. Protocols considered to be unsecure include: HTTP, Telnet, SNMPv1, SNMPv2, HiDiscovery V1. The SNMPv3 function is maintained.

The MultiConfig™ feature gives you the ability to configure the “Security Lockdown“ function for several devices together in a single step.

☐ To access the “Security Lockdown“ dialog, open the “Devices“ tab in the detail view.
☐ Select the devices to configure.
☐ To open the MultiConfig™ dialog, right-click on a selected device and click the MultiConfig™ option.
☐ To open the “Security Lockdown“ dialog, select `Device Settings >` Device Security `> Security Lockdown` in the MultiConfig™ dialog.

The “Security Lockdown“ function has the following restrictions:

- The “Port Security“ function is unavailable for the Eagle and BAT devices.
- The “Disable Unused Slots“ function is only available for the modular Classic and HiOS devices.
- The “Disable Unused Slots“ function is only available function for the GarrettCom RX10 devices.
- The “Restricted Management Access“, and “Disable HiDiscovery“ functions are available for the following devices:
  – The Classic devices starting with Version 09.0.01
  – The HiOS devices starting with Version 06.0.00
  – The HiSecOS devices starting with Version 03.0.00

Comparing IP/MAC address pairs

Attackers often use their own devices to gain access to your data network. To do this, the attacker uses the IP address of an existing device that is currently switched off, or a free IP address on the subnet they want to access.
However, the MAC address of the attacker's own device can differ from the MAC address on the device whose IP address the attacker is spoofing.
Industrial HiVision gives you the ability to track down this kind of attacker with the help of this feature.
To do this, Industrial HiVision collects the IP/MAC address pairs of the connected devices. Industrial HiVision lists the IP/MAC address pairs it collected in a table. You can manually extend this table with user-defined entries.
Industrial HiVision gives you the ability to automate the process of regularly checking the content of this table against the live IP/MAC address pairs on your network. If Industrial HiVision detects a difference, Industrial HiVision notifies you in line with the action you defined.

☐ Make the relevant settings in order to monitor the IP/MAC address pairs.
See “MAC/IP Address Pair Security” on page 413.

Detecting rogue devices

A rogue device is a device accessing a part of the network where it does not belong.
Let's assume that you completed the configuration of your data network in Industrial HiVision, and Industrial HiVision has the valid topology for your devices and device connections. This is the right time to freeze this state in Industrial HiVision.
Industrial HiVision then gives you the ability to reference the frozen state and identify intruders on your data network.
When you activate this function, Industrial HiVision stores an image of the topology.

But how do you deal with new devices on your data network beyond the existing installation? These new devices could pose a potential risk to your data network. This is why the “Rogue Device Detection“ function has a special procedure for these devices.

☐ After initially setting up Industrial HiVision, activate the “Rogue Device Detection“ feature under `Configuration > Preferences >` Basics `> Discover Devices > Discovery Mode`.
  – Industrial HiVision lists any newly detected devices in the “Rogue Devices“ folder. Since you consciously enter manually created devices in a certain folder, Industrial HiVision leaves manually created devices in the relevant folder.
  – When Industrial HiVision lists a new device in the “Rogue Devices“ folder, Industrial HiVision generates both a “New device detected” event and a “Rogue Device Detection“ event.

☐ You can use “Event Actions“, or “User defined Actions“, to define how Industrial HiVision should react to a new device displayed in the “Rogue Devices“ folder.

7.2 Status configuration

The status configuration specifies which status is assigned to the value of the component detail. Possible statuses are:

- “No Status“
- “Not Available“
- “OK“
- “Warning“
- “Error“

Example:
You can assign the status “OK“, “Warning“ or the status “Error“ to a connection break.
In the case of a terminal device that you regularly turn off, a connection break (= device switched off) is not an error.
In the case of a server that should be available, a connection break is a serious error that should be monitored.

Industrial HiVision allows you to perform the status configuration of a component detail device overlapping for the devices in a device class (see on page 404 “Status Configuration”).

If you want to change the status configuration of individual devices, you can find access to the status configuration in the Properties window of a component detail. The status configuration allows you to enter status configuration settings for each component detail (see on page 285 “Properties of a component detail”).

A pre-condition for determining a status is monitoring a component detail. When it monitors a component detail, Industrial HiVision queries the value periodically. Industrial HiVision assigns a status to this value as part of the determination.

In the state on delivery, the status configurations are set so that you can monitor your network properly right after the installation.

7.3 Status determination

To monitor your network, your network management station requires information from the components of the network. To acquire this information,

- the network management station can query the components periodically or
- the components send information (traps) on their own initiative to the network management station.

Note: When router interfaces are active in combination with a stateful inspection firewall, no SNMP communication is possible between Industrial HiVision and the agent of a Classic device.
The Classic agent answers SNMP request with the IP address of the router interface that is closest to the Industrial HiVision management station. If you specify an IP address other than the router interface closest to Industrial HiVision, then the destination IP address of the Industrial HiVision SNMP packets differs to the source IP address of the SNMP packets coming from the device agent.
If you use a firewall that does not have the right rule set for this type of communication it can drop the packets resulting in a loss of communication between Industrial HiVision and the device agent. For detailed information about using firewalls with Industrial HiVision (see on page 62 “Using Industrial HiVision with Firewalls”)

Periodic querying (polling)

Depending on the size of the network and the querying frequency, periodic querying can lead to significant loss of available bandwidth.
In the case of, for example, short-term overloading of the network, an answer or a trap can get lost. An advantage of periodic querying is the high probability that the network management station receives an answer when it makes the next query.

- **Traps**
  As soon as a device detects a status change, it sends an alarm message (trap) to the network management station. Since the device only sends a trap if there has been a status change, this method has little effect on the network load. However, if a packet gets lost, the network management station may not be informed of the status change.

7.3.1 Trap destination address

To send alarm messages, a device needs the IP address (= trap destination address) of the network management station, to which it sends any alarm messages that arise. You can enter the trap destination address directly on the device using, for example, the Web-based interface, or more straightforwardly using Industrial HiVision (see on page 417 “SNMP V1 Trap Destination”).

☐ Right-click on the device and select “SNMP V1 Trap Destination“ in the drop-down list. The trap configuration dialog opens.
☐ Mark the “Send Traps“ checkbox.
☐ Click the “Write“ button.

7.3.2 Updating device status

Industrial HiVision displays the status that the device had at the time of the device detection, or the status from the received traps or status queries.

▶ “Refresh“ allows you to read in the properties again.

7.4 Status propagation

The status propagation specifies whether the status is propagated to the next highest level.

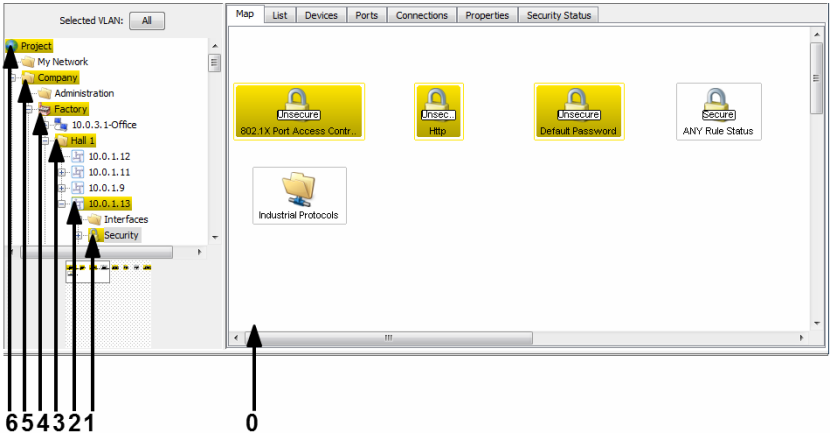


Figure 47: Status propagation to a higher level
0 - Lowest level = component detail
1 - 1. higher level
2 - 2. higher level
3 - 3. higher level
4 - 4. higher level
5 - 5. higher level
6 - 6. higher level

A folder takes the worst status that the content of a component displays. The evaluation is based on the following sequence:

- “Error“ (worst status)
- “Warning“
- “OK“
- “Not Available“
- “No Status“

☐ You specify the meaning of the color assignment at `Configuration > Preferences > Display > Status Colors`.

☐ In the properties window of the relevant component, you specify the determination of the status and the propagation. The component can also be a folder in the folder frame.

7.5 Management actions

In addition to passive observation of the network, network monitoring also consists of active intervention into network events. Active intervention manifests itself in the response to events in the network or administrative actions such as switching ports on and off according to a schedule.

7.5.1 Event actions

Industrial HiVision allows you to react automatically to events such as a status change.

☐ Select `Configuration > Preferences > Basics > Event Actions` or click “Preferences“ in the tool bar and select `Basics > Event Actions`.

The automatic reaction options (see on page 335 “Event Actions”) provided by Industrial HiVision are:

- “Popup Message Box“
- “Send SMS“
- “Send E-Mail“
- “Run Executable“
- “Play Sound“

In the second frame of this dialog, Industrial HiVision enables you to assign a selected reaction to an event.

Note: If you configure Industrial HiVision to run an executable file as an event action and you get an error message, then refer to the kernel log for more information about the error.

7.5.2 Time-linked actions

Industrial HiVision offers you the opportunity to set a time period during which Industrial HiVision responds to an event with an action.

☐ Select `Configuration > Preferences > Basics > Event Actions` or click “Preferences“ in the tool bar and select `Basics > Event Actions`.

☐ Create a new entry in “Alarms“.
The “Time“ frame in the “Alarms“ dialog gives you the option of defining a fixed period with a fixed start and end point.

7.5.3 Industrial HiVision “I'm alive” event

Industrial HiVision enables you to receive an “I'm alive” event from Industrial HiVision when using remote monitoring.

☐ Select `Configuration > Preferences > Event Actions` or click “Preferences“ in the tool bar and select `Basics > Event Actions`.

☐ Define an action that Industrial HiVision is to perform as an “I'm alive” event for example, send an SMS.
(see on page 335 “Event Actions”)

☐ Define an alarm that triggers Industrial HiVision to perform the action.
(see on page 335 “Event Actions”)

7.6 Time-related recordings

Industrial HiVision allows you to record time-related values from properties in various databases:
- in a project database (history)
- in a separate report database (report)

With the size of a database the access time for the database increases.
For this reason, Industrial HiVision restricts the number of history entries that can be recorded to the project database.

7.6.1 History

To monitor your network over a user-specified period of time, Industrial HiVision allows you to log states with time information.
You can find settings for logging and displaying the history in the properties dialogs
– “Properties of a connection” on page 292 and
– “Properties of a component detail” on page 285.

Protocol Configuration

The “Properties“ dialog of a component detail and the connection dialog of a “Connection“ enable you:
- to switch on the protocoling of the history
- to enter the recording/querying interval
- to enter the maximum number of entries recorded. When the maximum number of entries is reached, Industrial HiVision throws out the oldest entry when a new one is recorded.
  100 entries (= default setting) take up approx. 5 kB of your hard disk capacity.

Network load

Double-click on a link to open the history window. There you can find for each data direction a graphic representation of the network load.

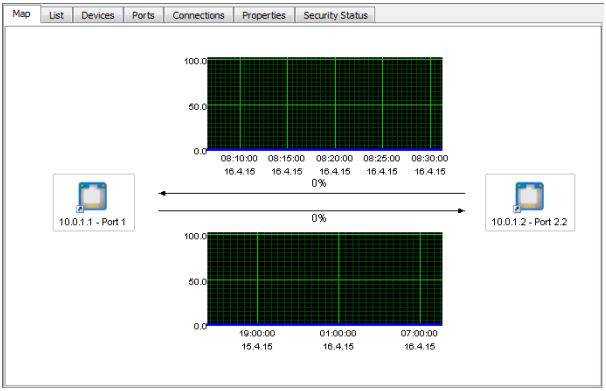


Figure 48: Network load

If no ports are assigned to the link yet, you can double-click on the link to open the dialog for assigning the ports.
If you activated polling of the threshold values in the “Properties“ dialog of a link, then the graphic displays the threshold lines.

7.6.2 Reports

The reporting function allows you to manage long-term statistics outside the database of the network management system program.
Industrial HiVision stores values from properties with time information in a special report database.
To evaluate the recorded values, the reporting function allows you to output reports in the form of graphics and tables.

Note: Depending on your settings, Industrial HiVision can collect any amount of data and save it on your hard drive. Make sure that your hard drive has sufficient free memory space.

Application example for temperature monitoring

You want to monitor the temperature fluctuation within a switch over the course of a 5-day work week for a period of several weeks. Industrial HiVision should generate a report for each week. You would like to have the first report on Sunday, October 7, 2012 and further reports at weekly intervals.

Add the temperature property to reporting:

- ☐ To go to the properties level, double-click on the desired device in the “Map“ tab.
- ☐ Right-click on the icon for the “Temperature“ property. Select “Add to Reporting...“.
  Industrial HiVision opens a dialog for entering the reporting parameter.
- ☐ Enter October 1, 2012, 12:00 am as the recording start time.
  Press the Enter key to close the date dialog.
  Set the recording start time no later than the time at which the report requires the first entry.
  Retain “Indefinite“ as the recording stop time.
  Choose a polling interval as large as possible, but short enough that Industrial HiVision is able to record the expected fluctuations.
  Enter 10 minutes as the “Polling Interval“.
  Click the “OK“ button.

Create a template for the report:
A template defines the appearance of the report to be generated. In this example you want the report to be a line graph in a PDF file.

- ☐ Select `Configuration > Reporting` in the menu bar.
- ☐ In the “Reporting“ dialog, open the “Templates“ tab.
- ☐ To create a new template for your report, click the “New“ button.
- ☐ Enter the parameters for the template (see table 21):
- ☐ Click the “OK“ button.

Parameter	Meaning
Report	
Name	Temp. SW1
Title	Temperature fluctuation in switch 1

Table 21: Defining a new template

Parameter	Meaning
Report Type	
Type	PDF
Layout	Chart
Chart Type	Line
Data	
Monitored Properties	Select the property and click the right arrow button.

Table 21: Defining a new template

Create scheduling for the report:
With the scheduling function, you define the points in time at which you want Industrial HiVision to create reports as well as the time period the report should cover.

- ☐ In the menu bar select `Configuration > Reporting`.
- ☐ In the “Reporting“ dialog, open the “Scheduling“ tab.
- ☐ To create a new schedule for your report, click the “New“ button.
- ☐ Enter the parameters for the template (see table 22):
- ☐ Click the “OK“ button.

Parameter	Meaning
Report	
Name	Temp. SW1
Relative	This type of scheduling generates successive reports.
Duration	5 days
Offset to execution	6 days, as you want the report to include data from Monday through Friday and the first generation of the report is to take place on Saturday.
First Execution	Sunday, 7 October 2012, 00:00:00 am CET
Schedule every	1 week

Table 22: Defining a new schedule

7.7 User-defined properties

To use this function you require advanced knowledge of SNMP MIB and the device.

7.7.1 Description of user-defined properties

In the default setting, Industrial HiVision already recognizes a large number of devices and their properties.
With the “User defined Properties“ function, Industrial HiVision allows you to include additional properties from the MIB of SNMP-capable devices in the management.
In this way you can add and monitor the properties of any SNMP-capable devices in Industrial HiVision. You can also add additional properties from MIB to devices already recognized by Industrial HiVision and monitor them.

7.7.2 Application example for user-defined properties

In a sensitive network, you want to use ICMP packets to monitor the load on the network components. If a device receives more than 10 ICMP requests within 5 minutes, you want Industrial HiVision to send a warning.

☐ To inform Industrial HiVision about this new property, you select the `Configuration > User defined Properties` dialog.

☐ To create a new entry with a new property, in the “User defined Properties“ dialog, click the “New“ button.

- ☐ In the “Name“ field, give the new property a unique name for example, `UserDef_ICMP-Message`. Here Industrial HiVision expects a name that starts with “`UserDef_`“.
- ☐ In the “Label“ field, enter an identifier for this property that Industrial HiVision displays in the user interface for example, `ICMP-Watch`.
- ☐ In the “Parent Property“ drop-down list select, “Agent“.
- ☐ In the “MIB Variable/OID“ field, enter the MIB variable of the new property. Alternatively, the MIB Manager allows you to search for the MIB variables in the MIB of the device:
  - To open the MIB Viewer, click the “...” button.
  - To get an overview of the MIBs that the “MIB Viewer“ has loaded, click the “MIB Manager“ button.
    Industrial HiVision also allows you to load additional MIBs into the MIB Viewer, click the “Load...“ button. Then select the desired MIB from your file system.
  - Open the path `iso:org:dod:internet:mgmt:mib-2:icmp`.
  - Select the MIB variable `icmpInMsgs`.
  - To close the “MIB Viewer“, click the “OK“ button.
- ☐ In the “Instance“ field, enter the instance of the MIB variables, in this case `0`.
- ☐ In the “Type“ drop-down list, select, “Delta“.

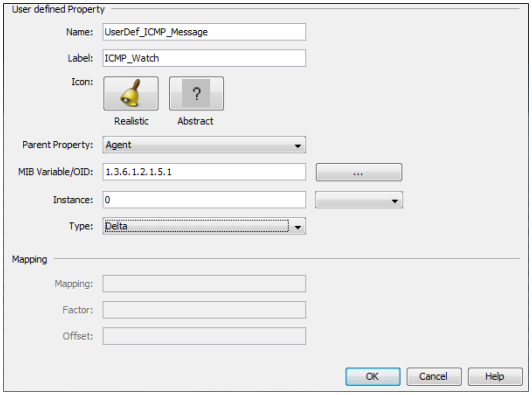


Figure 49: Creating a new user-defined property

- ☐ To finish defining the property, click the “OK“ button.
  You can now see the new defined property in the “User defined Properties“ window.
- ☐ To close the “User defined Properties“ window, click the “OK“ button.
- ☐ Now go to the list view from the detail display.
- ☐ In the list view, select the agent of the device that you want to monitor.
- ☐ To open the “New Property“ window, right-click on the list view and select `New > Property`.
- ☐ To close the window again, select the newly-defined property `ICMP Watch` in the “New Property“ window.
- ☐ Click the “OK“ button.

You have now assigned the new property `ICMP Watch` to the agent. To monitor the new property of the agent, configure the status (see on page 214 “Status configuration”) and the status determination (see on page 215 “Periodic querying (polling)”).

7.8 Effect on system resources

Industrial HiVision provides you with a range of options for managing and monitoring your network. This range of options also makes it possible for you to exhaust your system resources and even to overload them.

In this chapter, you can find the following information about the utilization of your system resources:

- detect
- influence
- minimize

7.8.1 Detecting utilization of system resources

Polling operations and history records are the main activities that affect your system resources.
In extreme cases, when you change such settings you can see that your system has slowed down.
In other cases, you require objective indicators to back up your subjective perception. You can find these indicators in `Help > Kernel Info > Polling`.

Indicator	Meaning
Number of polled properties	Displays the number of properties for which polling is activated. This display takes into account the devices (see on page 269 “Manage”) monitored by Industrial HiVision and their properties.
Number of properties recording history	Displays the number of properties for which the history recording is activated. This display takes into account the devices (see on page 269 “Manage”) monitored by Industrial HiVision and their properties.
Polling operations per minute	Industrial HiVision sums up the properties for which polling is activated and relates the total to the polling interval. As some polling intervals are greater than 1 minute, the number of polling operations can exceed this calculated value within the last minute. This display takes into account the devices (see on page 269 “Manage”) monitored by Industrial HiVision and their properties.
Polling operations in the last minute	Displays the number of polling operations performed in the last minute. This display takes into account the devices (see on page 269 “Manage”) monitored by Industrial HiVision and their properties.
Total number of history entries set	Displays the number of entries saved by Industrial HiVision (see on page 221 “Protocol Configuration”).
Total number of actual history entries	Displays the number of entries actually saved by Industrial HiVision.

Table 23: Indicators for system resource utilization in the kernel info

7.8.2 Influencing utilization of system resources

You have the most influence on the utilization of your system resources by using the settings for polling operations and history recording. You can see for which properties you have currently activated the polling or the history recording in the “Monitor“ dialog (see on page 306 “Monitor”).

To keep the utilization of your system resources as low as possible, note the following points:

- Every property that you have activated in Industrial HiVision for periodic querying creates a load on your network management station and increases the network traffic.
  - ☐ Check which properties you really want to monitor.
  - ☐ Check which query frequency you require for this monitoring.
- Every history entry creates a load on your network management station and uses up the free memory space on your network management station.
  - ☐ Check which properties you really want to record.
  - ☐ Check which buffer size you require.
- The MultiConfig™ function allows you to set up statistic counters on multiple devices at the same time. By setting up statistic counters, you activate the polling and recording operations.
  - ☐ Before you use the MultiConfig™ function, verify what effect the settings has on your system resources.
- Many events increase the memory requirement, the program start time and the start time of the event filter dialog.

For a sufficient performance of your network management station, consider the following additional factors:

- Network range
- Number of nodes
- Complexity of the node management
- Network load
- Computer resources of your network management station
- Memory size (RAM and hard drive) of your network management station

7.8.3 Minimizing polling

Industrial HiVision gives you the option of adjusting polling gradually to your requirements. You can change the polling interval and also determine which properties are to be queried by Industrial HiVision.

Changing the polling interval for the properties of several devices

The table (see on page 455 “Monitored properties in the basic setting”) displays which properties Industrial HiVision monitors with the basic polling setting.

To reduce the polling volume from temperature monitoring for the devices in the detail display, proceed as follows:

- ☐ Select the “Properties“ tab in the detail display.
- ☐ In the “Device Class:“ drop-down list, select “All“
- ☐ In the “Property:“ drop-down list, select "Temperature (Device)".
- ☐ Select every device in the table with “Ctrl”+“a”.
- ☐ Right-click on a device and select MultiConfig™.
- ☐ In the function frame of the MultiConfig™ dialog, select “Property Properties“.
- ☐ In the “Polling Interval“ text box, enter 15 minutes.
- ☐ To save the change in Industrial HiVision, click the “Write“ button.

You can also turn off polling completely in the same way.

Turning off polling for connection properties

With the default value, Industrial HiVision polls the network load every 30 seconds.

To turn off network load polling, proceed as follows:

- ☐ Select the “Connections“ tab in the detail display.
- ☐ Select every connection in the table with “Ctrl”+“a”.
- ☐ Right-click on a connection and select MultiConfig™.
- ☐ In the function frame of the MultiConfig™ dialog, select “Connection Properties“.
- ☐ In the function frame of the MultiConfig™ dialog, unmark the `Monitor > Polling > Load` checkbox.
- ☐ To save the change in Industrial HiVision, click the “Write“ button.

7.8.4 Minimizing network load

Industrial HiVision gives you the option of reducing the network load caused by the device detection.

- ☐ Select `Configuration > Preferences > Advanced > Service Parameters`.
- ☐ Under “Device Discovery“, reduce the “Scan Rate [devices/min]“.
- ☐ Under “Device Discovery“, reduce the value for “Simultaneously Discovered Devices“.

7.9 Process visualization systems

7.9.1 Link to process visualization system

As an interface to process visualization systems (SCADA, Supervisory Control and Data Acquisition) Industrial HiVision contains OPC services on Windows operating systems.

If the Hirschmann Industrial HiVision 8.4 Service is active, then the OPC services can read data from Industrial HiVision and make it available to the process visualization systems. The OPC services can also write data in Industrial HiVision. The OPC services support Data Access V1 to V3 and OPC Unified Architecture for communication purposes.
OPC DA is based on the Distributed Component Object Model (DCOM) protocol from Microsoft. DCOM is designed as a transport protocol on multiple layers for example, on the HTTP Internet protocol. Thus DCOM supports direct communication between software components through the LAN.
Windows 2008 R2, Windows Server 2012 R2 support DCOM. For further information on DCOM, visit the Microsoft website.
Activate the DCOM protocol and the remote access to the network management station, in order that an OPC client has remote access to the OPC server.
OPC UA is an XML-based, operating-system-independent protocol.

Initial setting for the Industrial HiVision OPC server service: OPC UA Server is set as the default server and the server is active (see on page 374 “Services Access”).

Note: If you activate the Industrial HiVision OPC server service, an OPC client uses the OPC service and Industrial HiVision with write permission to access devices managed by Industrial HiVision.

To deactivate the write permission, open the `Configuration > Preferences > Advanced > Services Access` dialog, in the “OPC Server“ frame, unmark the “Global Write“ checkbox.

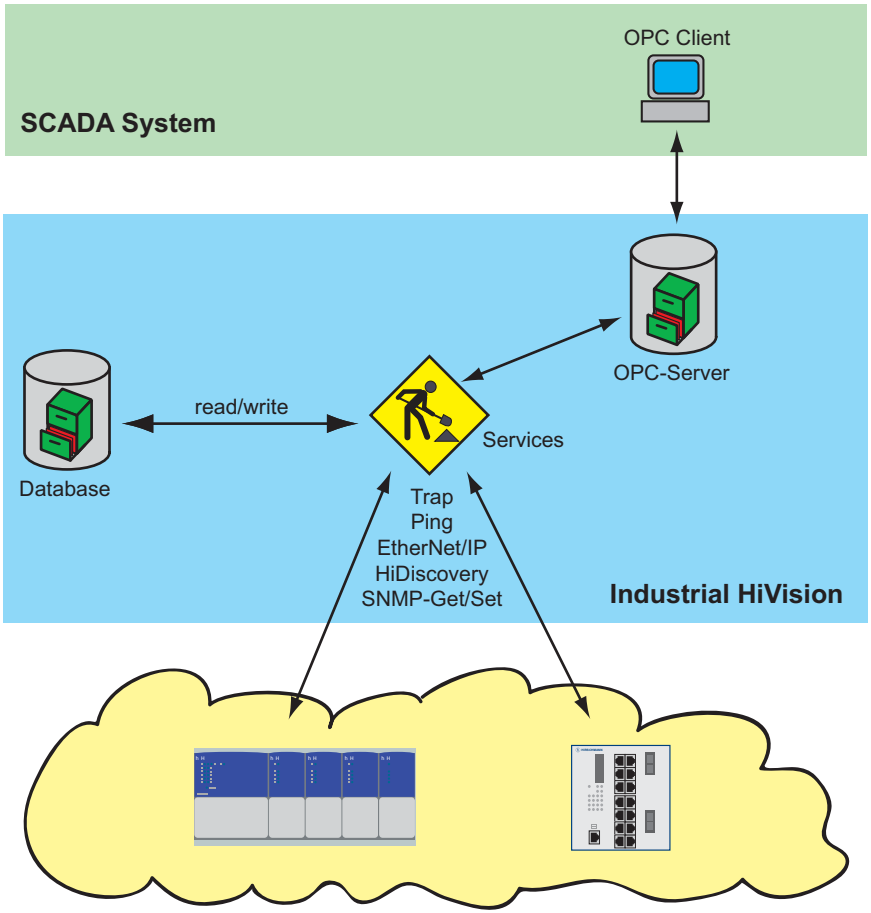


Figure 50: Link to process visualization system

7.9.2 Structure of the transfer data for OPC

The Industrial HiVision OPC server maps the data to be transferred in the same tree structure in which Industrial HiVision represents it in the folder frame. The individual elements and their values are known as tags. To indicate the hierarchy, Industrial HiVision uses prefixes which Industrial HiVision puts before the tag name. The tag names correspond to the names of Industrial HiVision in the English language version.
Changing the names in Industrial HiVision has the effect that OPC clients cannot access the tags any more. The same applies to moving components into other folders.

Note: If you intend to move components regularly, you can put a link to the components in your own folder (e.g. Folder/OPC) and access the link using OPC. This method can be useful if your process visualization system has a length restriction for the tag name.

Prefix	Type of component
C_	Link
D_	Device
F_	Folder
L_	Link
P_	Port
V_	Device detail

Table 24: Tag name for OPC

For device names, Industrial HiVision represents the IP addresses with dots instead of underscores. The Industrial HiVision OPC server replaces dots and spaces with underscores.
Every node/folder in the structure consists of 5 tags, with the exception of devices, device details and links.
A device also has the “Managed” tag.
A device detail also has the “Value” tag.
A link also has the “ConnectionState”, “Utilization_AB” and “Utilization_BA” tags.

Tag name	Meaning	Component
Label	Name of the component, as displayed by the program interface.	all
Security status	Current status as numerical value. 0=No Status, 1=Unavailable, 2=Ok, 3=Warning, 4=Error	all
Status	Current status as numerical value. 0=No Status, 1=Unavailable, 2=Ok, 3=Warning, 4=Error	all
StatusString	Current status as readable (English) text for example, "OK", "Error"	all
StatusReason	List of all the reasons that contribute to the status of the component, in readable (English) text form.	all
StatusChanged	Shows whether the status of the object is unconfirmed. 0=Confirmed 1=Unconfirmed You can use OPC to set the value to "0".	all
Managed	Shows whether Industrial HiVision is monitoring the device.	Device
Value	Current value of the component detail.	Device detail
ConnectionState	Link status, as displayed by the program interface through line representation: 1=Unavailable 2=Active (unbroken line) 3=Standby (dotted line) 4=Inactive (chain line)	Link

Table 25: Available tags

Tag name	Meaning	Component
Utilization_AB	Load on the line from the first terminal point to the second terminal point (sequence as represented in the OPC tree).	Link
Utilization_BA	Load on the line from the second terminal point to the first terminal point (sequence as represented in the OPC tree).	Link

Table 25: Available tags

Note: The OPC server from Industrial HiVision supports the querying of up to 3000 OPC tags.

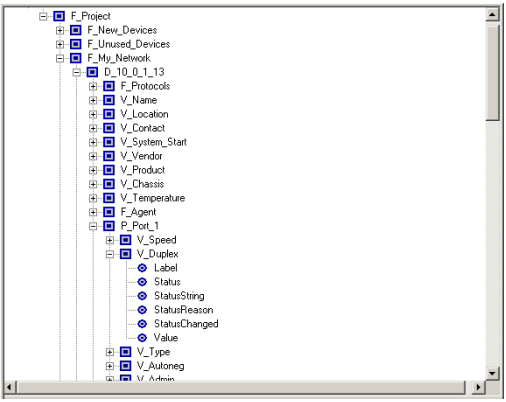


Figure 51: Example of the representation as an OPC tree structure

7.9.3 Supported applications OPC DA

Hirschmann has tested Industrial HiVision with the following applications:

Software	Version	Manufacturer
RS View 32	7.20.00	Rockwell Automation
Genesis 32	8.00.138.00	Iconics, Inc
Simatic WinCC	6.0	Siemens AG
Citect SCADA	6.0	Citect Corporation
Softing OPC Demo Client	4.10 Built 512	Softing AG

7.9.4 Supported applications OPC UA

To connect a SCADA client with the Industrial HiVision OPC UA server, the SCADA client requires the following URL:
`opc.tcp://<IP-ADDRESS>:11210/OPCUA/HiVisionUaServer`
You can find the OPC UA Server Port in the `Preferences > Advanced >` Services Access dialog.

Hirschmann has tested Industrial HiVision with the following applications:

Software	Version	Manufacturer
Ignition	7.9.6	Inductive Automation
Prosys	2.3.3-170	Prosys OPC
UaExpert	1.03.0.201	Unified Automation

7.9.5 OPC UA Connection Example

The OPC UA server is active in the default setting. To verify that the OPC UA server is active, open the `Preferences > Advanced > Services Access` dialog. The “Services Access“ dialog also displays which OPC server type is installed.

If you wish to change the OPC server type, then proceed as follows:

The following work steps are only applicable to version 6.0 and 7.0.

- ☐ If you have the Industrial HiVision service running, then stop the service.
- ☐ Open the `Windows Control Panel> Programs and Features` dialog.
- ☐ Highlight the Industrial HiVision program and select the `Change` option.
- ☐ In the Industrial HiVision maintenance dialog, select the `Modify` option and click the `Next` button.
- ☐ In the `Select Components` dialog, mark the desired `OPC service` checkbox.
- ☐ Verify that you have only one checkbox marked, then click the `Next` button.
- ☐ In the `Setup Needs The Next Disk` dialog, click the `Browse...` button.
- ☐ On the installation disk, navigate to the folder that contains the file named data2.cab and click the `OK` button.
- ☐ In the `InstallShield Wizard Complete` dialog, mark the desired checkboxes and click the `Finish` button.

If your Industrial HiVision version is 7.1 or later, Industrial HiVision requires a re-installation.

- ☐ Make a backup of your database before you begin the re-installation.
- ☐ Deinstall Industrial HiVision.
- ☐ In the `Attendant question` dialog, click the `No` button. If you click the `No` button, then Industrial HiVision keeps the installation folder which contains your database, PSMs and license files.
- ☐ Re-install Industrial HiVision.
- ☐ In the `Select Components` dialog, mark the desired `OPC service` checkbox.

This example explains how to connect the Industrial HiVision OPC UA server to an `Inductive Automation Ignition` OPC UA client. The prerequisite for this example is that the OPC UA server and client are installed on the same PC.

- ☐ Install and open the OPC UA client software.
- ☐ In the `Ignition Gateway Control Utility`> `Port` field, enter the value `8088`.
- ☐ Restart the gateway.

- ☐ In the `Ignition Gateway Control Utility` dialog, click the `Start the Ignition Service` button.
- ☐ In the `Message` dialog, click the `OK` button.
- ☐ In the `Ignition Gateway Control Utility` dialog, select the `Go to webpage` option.
- ☐ In the `Ignition localhost` dialog, select the `Configure` option.
- ☐ In the `Sign In` dialog, enter the default sign in credentials: `User name = admin`, `Password = password`
- ☐ In the `Configuration` dialog, select the `OPC Connections> Servers` option.
- ☐ In the `OPC Server Connections` dialog, select the `Create new OPC Server Connection...` option.
- ☐ In the `Add OPC Server Connection Step 1: Choose Type` dialog, select the `OPC UA` option.
- ☐ In the `Discover OPC-UA Endpoints` dialog, enter the following URL: `opc.tcp://127.0.0.1:11210/OPCUA/HiVisionUaServer`
- ☐ During the discovery process Industrial HiVision saves the `Ignition` certificate in the installation directory under `services\PKI\CA\rejected`. If you wish to use a secure connection, then cut the certificate from the `rejected` directory and paste it in the `services\PKI\CA\cert` directory.
- ☐ The `Discover OPC-UA Endpoints` dialog now displays various options. To use a secure connection, select the `SecurityPolicy: Basic128Rsa15, MessageSecurity: SignAndEncrypt` option.
- ☐ In the `New OpcUaConnectionSettings`> `Main` frame, enter a meaningful name and description. You can edit the parameters after the configuration is done.
- ☐ Click the `Create new OPC Server Connection` button.
- ☐ The `OPC Server Connections` dialog opens and displays the new server with the status.

You are now ready to configure the `Ignition Designer` dashboard.

7.9.6 OPC UA Server Custom Certificates

The Industrial HiVision OPC UA installation functions in accordance with the Tier 2, Server Authentication OPC UA specifications. Industrial HiVision provides an OPC UA server that uses CA certificates for server identity. The OPC UA clients then can trust the connection to the server. The syntax of these certificates conform to the X509 specification.

The OPC UA server uses the following types of certificates for identification:

- a Certification Authority (CA) certificate, which you can use for signing certificates in a corporate environment for example, HirschmannSampleCA
- an application identity certificate, which identifies the OPC UA server for example, HiVisionUaServer
- an HTTPS certificate, which identifies the OPC UA HTTPS server for example, HiVisionUaServer_https

Each CA certificate contains the following files:

- a private key using the `.der` format
- a public key using the `.pem` format

When the OPC UA server starts, the server verifies that the certificates are present in the installation subdirectory. If the certificates are missing, then the server creates the default certificates.

Note: The CA certificates are located in the `services/PKI/CA/private` Industrial HiVision installation subdirectory. The CA certificates are highly sensitive data. Safeguard the subdirectory against unauthorized read or write access.

The OPC UA server configuration file, `server.properties.xml`, is located in the `lib/opcua/config/` subdirectory. The configuration file contains the following parameters that control the behavior of the server with respect to certificate handling:

- `OpcUaServer.issuer.name`: is the base file name of the CA certificate. The default base file name is HirschmannSampleCA. If the CA certificate does not exist, the server creates the certificate with the specified file name, and uses the default base file name as the issuer name.
- `OpcUaServer.private.password`: this is the password that the server uses to encrypt or decrypt the private keys of the certificates. The default password is `opcua`. If you change the password, then verify that you use the new password for every certificate that you create. Replace or recreate existing certificates based on the obsolete password.

Note: The private key password is highly sensitive data. Safeguard the configuration file, `server.properties.xml`, against unauthorized read or write access.

Default Certificates

If there is no specific requirement regarding certificates, then the server uses the default CA certificates and values in the installation bundle to create self-signed certificates. The client then imports or trusts the self-signed certificates.

Corporate CA Certificates

If an organization issues a corporate CA certificate to sign the certificates, then you can use the corporate CA certificate with the OPC UA server. To use the corporate CA certificates with the OPC UA server, proceed as follows:

- ☐ Delete the certificates located in the `services/PKI/CA/private` subdirectory.
- ☐ Convert your CA certificates to the `.pem` and `.der` formats, and copy the certificates to the `services/PKI/CA/private` subdirectory.
- ☐ Open the `server.properties` file.

- ☐ Enter the base name of the corporate CA certificate files on the `OpcUaServer.issuer.name` line.
- ☐ Enter the password of the private key on the `OpcUaServer.private.password` line.
  - – If you do not use a password, then use an empty string.

When the OPC UA server starts for the first time, the server creates an application identity certificate and an HTTPS certificate based on the corporate CA certificate.

Application Identity Certificates

If you have a certificate that either your organization, or a trusted authority has created for you, then you can use the certificate as the application identity certification for the HTTPS server. To use the application identity certification with the OPC UA server, proceed as follows:

- ☐ Delete the certificates in the `services/PKI/CA/private` subdirectory.
- ☐ Convert your certificates to the `.pem` and `.der` formats. Copy the certificates to the `services/PKI/CA/private` subdirectory.
  - – Set the base filename to HiVisionUaServer for the application identity certificate.
  - – Change the HTTPS certificate, to HiVisionUaServer_http.
- ☐ Open the `server.properties` file.
- ☐ Enter the password of the private key in the `OpcUaServer.private.password` line.
  - – If you do not use a password, then use an empty string.

When the OPC UA server starts for the first time, the server creates a CA certificate. The CA certificate created during startup certificate is not used in this situation. The OPC UA server also creates any other missing certificates.

7.10 Remote access to Industrial HiVision

7.10.1 Web access to Industrial HiVision

Industrial HiVision allows you to access the Web server of Industrial HiVision with a browser using the HTTP or HTTPS protocol. We recommend that you use the secure HTTPS protocol and certificate (see on page 247 “Certificate for the HTTPS connection”). You can thus monitor your network from anywhere in the world.
Example of an Internet address entry:

```
https://[IP address of your network management station]:11208
```

You can restrict the access with a password. To have information on accessing, Industrial HiVision can create an event for every successful access (see on page 370 “Program Access”).

Note: Verify that this communication is possible. This is particularly important if the connection is made using firewalls / port forwarding.
When using a firewall, take note of this information (see on page 25 “Installation”).

The Industrial HiVision Web server provides the following pages:

- Selection of the different websites
- Graphic user interface
- Event view

Note: If you wish to test Industrial HiVision before connecting the application to an actual network, then use the demo network provided by Industrial HiVision (see on page 441 “Demo Network”).

Selection of the different websites

On this page, the Industrial HiVision Web server presents for selection the websites provided by Industrial HiVision.

URL for this website:

```
https://[IP address of your network management station]:11208/idx
```

Graphical user interface

The Industrial HiVision Web server provides the same graphic interface as the one used in your network management station. This enables you to monitor and configure your network remotely in the same way as you are accustomed to doing on-site.

URL for this website:

```
https://[IP adresse of your network management station]:11208
```

Events on the website

PDAs, smartphones and other portable devices are increasingly important tools for IT administrators. For administrators, the event list is an important part of Industrial HiVision. The event list contains a concentrated overview of the state of the monitored network (see on page 112 “Event list”).
The Industrial HiVision Web server provides the event list in HTML format, optimized for display on portable devices such as the iPhone, BlackBerry devices, etc.

The following is an example of the URL for the Industrial HiVision Web server:

```
https://[IP address of your network management station]:11208/events
```

The event website allows you to confirm events. Industrial HiVision synchronizes the confirmations between the graphic user interface and the mobile device.

For the sake of clarity, Industrial HiVision restricts the display to the following events:
– Unconfirmed events
– Confirmed events of the types “Warning“ and “Error“.
When you confirm a standard event in the list, Industrial HiVision removes the confirmed standard event from the list.

Industrial HiVision refreshes this page every 5 minutes.
You can select different refresh cycles in the `Configuration >` Preferences `> Display > Event` dialog.
(see on page 353 “Event”)

In addition to the predefined filters by “Category“, Industrial HiVision offers user-defined filters according to the “Source“ and the “Component“ that caused an event.
☐ Copy a string from the “Source“ or “Component“ table column to the corresponding filter field. You can make the string more general by using the wildcard “*”.

Note: When accessing the event list using HTTP(S), Industrial HiVision saves the filter settings in a Web session on the Web server of Industrial HiVision.
Industrial HiVision gives you the option to change the lifetime of this Web session in the `Configuration > Preferences > Advanced >` Services dialog.
Use the setting `Industrial HiVision Web Server > Web Server Session Timeout [min]`.
If a password is configured for the Web access, this password remains valid after the Web session is finished.

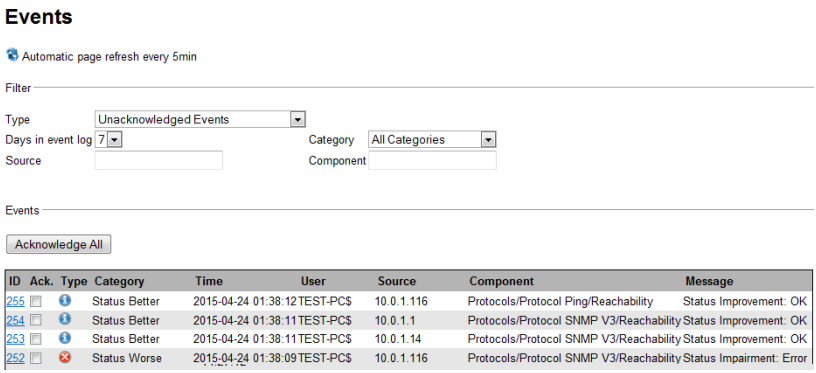


Figure 52: Events on the website of Industrial HiVision

7.10.2 Certificate for the HTTPS connection

To provide greater protection for the connection between your mobile device or a browser and Industrial HiVision, you require a new certificate. For this, you require a web server keystore. The web server keystore is a file that contains the key for the HTTPS connection.

The following example also applies to Linux operating systems when you use a “/” instead of a “\”.

- ☐ In the command line interpreter of the operating system, go to the installation directory of Industrial HiVision.
- ☐ Generate a Industrial HiVision web server keystore in the command line interpreter of the MS-DOS Microsoft operating system with the following command:
  ```
  lib\java_x86\bin\keytool -genkey -alias Industrial HiVision
  -keyalg RSA -keystore keystore -keysize 2048 -keypass
  password -storepass password
  ```
  Respond to the request for your first name and surname with the unique domain name of the domain to which your network management station is connected.
  You can enter any responses you want to the requests for your organizational unit, your city or community, and your federal state.
  Respond to the request for your country code with the two letters that make up the country code of your country.
  You can find the “keystore” file in the directory from which you executed the command.
- ☐ To request a certificate from a certification body, you require a certificate signing request file (*.csr).
  You generate this file in the command line interpreter of the operating system with the following command:
  ```
  lib\java_x86\bin\keytool -certreq -alias Industrial HiVision
  -keystore keystore -file ihivision.csr -storepass password
  ```
  You can find the *.csr file in the directory from which you executed the command.
- ☐ With this *.csr file you request a certificate from a certification body, such as Verisign.de.
  The certification body supplies the signed certificate in the form of a file or an ASCII character string.
  If you receive a file, rename this file to ihivision.crt.
  If you receive an ASCII character string, copy this completely to a text file with the name ihivision.crt.
- ☐ Import the certificate into the web server keystore in the command line interpreter of the operating system with the following command:
  lib\java_x86\bin\keytool -import -trustcacerts -alias Industrial HiVision -file ihivision.crt -keystore keystore -storepass password
- ☐ Save the “keystore” file in the installation directory of Industrial HiVision before replacing the existing file with the newly generated file.
- ☐ Replace the “keystore” file in the installation directory of Industrial HiVision with the newly generated “keystore” file.

Note: The files contain confidential keys that are comparable to passwords. Protect these files from unauthorized access.

Alternatively you can create your certificate yourself - see, for example, www.openssl.org. For this, you import the required CA certificate to the mobile device or browser by means of which you want to connect with Industrial HiVision.

7.11 Interface to InfluxDB® and Grafana®

This function lets you visualize a graphical representation of the evolution of different properties for the connected devices during a past period of time. You can monitor the statuses and the values for properties of different network topology items related to the following categories:

- device
- port general
- port statistics
- PoE
- performance
- WLAN

Industrial HiVision lets you select these categories and exports them to a InfluxDB® server. InfluxDB® is an open source database optimized for fast, high-performance storage, and retrieval of time-series data. From this database Grafana® retrieves the data exported from Industrial HiVision. Grafana® is a multi-platform open source web application used for analytics and interactive visualization of data. When connected to supported data sources, Grafana® provides charts, graphs, and alerts.

7.11.1 Configure InfluxDB® and Grafana®

In order for this functionality to work, you need to install InfluxDB® and Grafana®. You can do this through the following methods:

- ▶ The InfluxDB® and Grafana® applications installed on the same or different workstations and configured to work together.
- ▶ A Docker installation that runs the InfluxDB® and Grafana® containers configured to work together. This is an unsecure method, that uses only the HTTP protocol.

Note: It is necessary to install the following application versions:
- for InfluxDB®: version 1.8.x
- for Grafana®: version 8.x.x

To configure InfluxDB® and Grafana®, perform the following steps:
- ☐ Install InfluxDB®. Follow the instructions from the link https://portal.influxdata.com/downloads/.

  Note: In order to enable secure communication for InfluxDB®, in some cases it is necessary to have a self-signed certificate. To do this, follow the instructions from the link https://docs.influxdata.com/influxdb/v1.8/administration/https_setup/#set-up-https-with-a-self-signed-certificate.

  Note: For authentication and authorization in InfluxDB®, follow the instructions from the link https://docs.influxdata.com/influxdb/v1.8/administration/authentication_and_authorization/#user-management-commands.

- ☐ Install Grafana®. Follow the instructions from the link https://grafana.com/grafana/download?pg=get&plcmt=selfmanaged-box1-cta1.
- ☐ To install Industrial HiVision, follow the instructions from chapter “Software Overview” on page 23.
- ☐ To detect the devices from your topology, follow the instructions from chapter “Device detection” on page 122.
- ☐ To configure the connection parameters to the InfluxDB® server, follow the instructions from chapter “Export to InfluxDB®” on page 381.
- ☐ If you want to monitor port statistics, then you need to configure the user defined properties for those ports explicitly. If you want to add user defined properties to specific ports of a device, then perform the following steps:
  - ☐ In the detail display, click the “Ports“ tab and select the desired ports.
  - ☐ To open the “MultiConfig™“ dialog, right-click on the desired ports and select “MultiConfig™“.
  - ☐ In the menu tree of the “MultiConfig™“ dialog, open the “New Property“ dialog.
  - ☐ To add a new user defined property, click the “New“ button. The “New Entry“ dialog opens.

- ☐ In the “Property“ drop-down list, select the property that you want to export and click the “OK“ button.
  The selected property is added to the “New Property“ table.
- ☐ Click the “Write“ button.

Note: If you want to save the user defined properties as a MultiConfig™ preset, follow the instructions from chapter “General information for the Edit Presets table” on page 176

Note: The user defined properties are then displayed under the “Port Statistics“ category in the `Export to InfluxDB® > Categories` table. You can add the following user defined properties:

- “CRC Alignment Errors“ (“Delta“)
- “Collisions“ (“Delta“)
- “In Errors“ (“Delta“)
- “In Octets“ (“Delta“)
- “In Unicast Packets“ (“Delta“)
- “In non Unicast Packets“ (“Delta“)
- “Out Errors“ (“Delta“)
- “Out Octets“ (“Delta“)
- “Out Unicast Packets“ (“Delta“)
- “Out non Unicast Packets“ (“Delta“)

- ☐ To select the desired categories of properties, follow the instructions from chapter “Export to InfluxDB®” on page 313.
- ☐ To login to Grafana®, perform the following steps:
  - ☐ Open a web browser.
  - ☐ In the address bar, enter the IP address and the port of the workstation where Grafana® is installed in the following form:
    [IP_address_of_Grafana®_installation]:3000
    The `Welcome to Grafana` page opens.
  - ☐ In the `Email or username` field, enter the default user name: `admin`.
  - ☐ In the `Password` field, enter the default password: `admin`.
  - ☐ Click the `Log in` button.
    The page where you can change the password opens.
  - ☐ In the `New Password` and the `Confirm new password` fields, enter the same password.
  - ☐ Click the `Submit` button.
    The `General / Home` page opens.

Note: If you choose to click the `Skip` button, then Grafana® prompts you to change the password on the next log in.

- ☐ In the Grafana® `General / Home` page, hover the mouse cursor over the `Configuration` icon.
  The `Configuration` menu opens.
- ☐ In the `Configuration` menu, click the `Data sources` button.
  The `Data sources` tab opens.
- ☐ To add the data source, click the `Add data source` button.
  The `Add data source` page opens.
- ☐ To select the InfluxDB® server, click the `Select` button related to the `InfluxDB` row.
  The `Data Sources / InfluxDB` page opens.
- ☐ In the `Name` field, enter the default name of the database: `InfluxDB`.
- ☐ In the `URL` field, enter the IP address and the port of the workstation where InfluxDB® is installed in the following form: https://[IP_ADDRESS_OF_INFLUXDB®_INSTALLATION]:8086
- ☐ In the `Database` field, enter the default name of the database: `ihivision_data`.
- ☐ In the `User` field, enter the user name.
- ☐ In the `Password` field, enter the password.
- ☐ Click the `Save & test` button.

  Note: If you specified the correct data, then the `Data source is working` message is displayed.

7.11.2 Import the Grafana® dashboard templates

Hirschmann provides a series of dashboard templates for the available export categories. You can use these dashboards to visualize the data exported from Industrial HiVision.

To import the dashboard templates into Grafana®, perform the following steps:

- ☐ Open a web browser.
- ☐ In the address bar, enter the following URL: https://grafana.com/orgs/hirschmann/dashboards
  The Hirschmann `Dashboards` web page opens.
- ☐ Select the name of the dashboard that you want to import.
  The web page related to the selected dashboard opens.

- ☐ To copy the dashboard ID, click the `Copy ID to Clipboard` button.
- ☐ In the Grafana® `General / Home` page, hover the mouse cursor over the `Dashboards` icon.
  The `Dashboards` menu opens.
- ☐ In the `Dashboards` menu, click the `Manage` button.
  The `Manage` tab opens.
- ☐ In the `Manage` tab, click the `Import` button.
  The `Import` page opens.
- ☐ In the `Grafana.com dashboard URL or ID` field paste the copied ID and click the `Load` button.
  The `Importing dashboard from Grafana.com` page opens.
- ☐ In the `Select a InfluxDB data source` drop-down list, select the `InfluxDB` entry.
- ☐ To open the selected dashboard, click the `Import` button.
  The page related to the selected dashboard opens.

7.11.3 Security

To improve the security for the export to InfluxDB® feature, we recommend that you use the secure HTTPS protocol. Also use this protocol in combination with the enabled user authentication for InfluxDB® and Grafana®.

8 References

The descriptions in the previous chapters have been task-oriented, while the preference chapter describes the individual dialogs and menu items in a function-oriented way. Here you will find descriptions of function details for performing basic tasks that are of lesser importance.

8.1 File

The “File“ menu contains functions relating to file operations.
Industrial HiVision performs file operations on the computer with whose “Hirschmann Industrial HiVision 8.4 Service” service your interface communicates. If you have installed the service and the user interface on different computers, you get the file selection dialog for the file selection (see figure 53).

You double-click on a table row to go one level lower on the file tree structure.You click “Up“ to go one level higher in the file tree structure.

Above the table you see the path you are currently on.

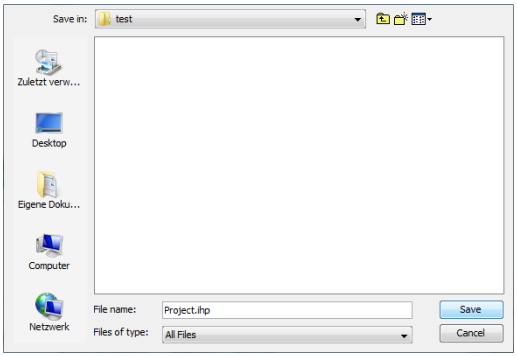


Figure 53: File selection dialog for different computers

8.1.1 New Project

You can use this selection to create a new project in which you can save your network data.

Note: By selecting “New Project“ you delete the current project. To save the data of the current project, you export this project under another name before selecting the new project (see on page 259 “Save”).

8.1.2 New

You use this selection for the following functions:

- to add a new folder
- to add a new device to the selected folder
- to add a new device from a list to the selected folder
- to add a new subdomain the selected folder
- to create a new connection
- to add counters with properties on the port level for example “In non Unicast Packets”.
- to add a text line
- to add a symbol. You can change the symbol in the “Properties...“ window of the symbol.

Devices from List

Industrial HiVision allows you to scan IP addresses using a text or an Microsoft Excel csv file. The “Create Devices from List“ dialog allows you to search for and upload the file to Industrial HiVision. If a device in the list is unreachable, then Industrial HiVision displays the device in the topology map as a generic device.

The “Create Devices from List“ dialog allows you add the IP addresses contained in the file to the `Preferences > Basics > Discover Devices >` Network Scan table. When you mark the “Add IP addresses to 'Preferences - Basics - Discover Devices - Network Scan'“ checkbox, Industrial HiVision enters the IP address ranges from the text file into the table.

When you mark both the “Add IP addresses to 'Preferences - Basics - Discover Devices - Network Scan'“ and the “Combine consecutive IP addresses into ranges“ checkboxes, Industrial HiVision enters the IP addresses to the table in the following manner:

- If the IP addresses in the file are within a range of addresses already present in the table, then Industrial HiVision merges the IP addresses into the existing address range.
- If the IP address range overlaps or is adjacent to a larger existing range, then Industrial HiVision uses the netmask from the existing range.
- When the function cannot use a netmask from any existent range, the function automatically assigns the default netmask value `255.255.255.0`.
- The function merges single adjacent IP addresses into IP address ranges entered in the same file.

When you create the IP address file use the following formats:

- 192.168.1.10,
- # this is a single address
- 192.168.1.11
- # this is also a single address
- 192.168.1.12,192.168.1.15,
- # this is a range of addresses
- 192.168.1.16,192.168.1.20
- # this is also a range of addresses
- # this is a comment line
- # 192.168.1.1 this is also a comment line

Note: To separate the IP address ranges, use a comma instead of a space. The comma at the end of the line is optional. To insert text use the hash “#” symbol.

8.1.3 Login

With this selection you can connect the user interface with the service on your own computer (`localhost`) or with the service on a remote computer.

8.1.4 Open...

You use this selection to open a previously saved project in order to view it or make changes in it.

☐ Select the relevant path and the desired file within your folder structure.

Note: Select a path to which both the Industrial HiVision service and you have access.

8.1.5 Save

You use this selection to save your current network data and the configuration of Industrial HiVision into a current project file with the extension `.ihp`.

☐ Select `File > Save`, to overwrite the open project file with the current project and the current configuration of Industrial HiVision.

8.1.6 Save as...

You use this selection to save your current network data and the configuration of Industrial HiVision into a project file.

☐ Select `File > Save as...`

☐ Select the relevant path within your folder structure and enter a project name.

Note: Select a path to which both the Industrial HiVision service and you have access.

☐ Click on “Save“ to save the current project and the current configuration of Industrial HiVision in a new file.

8.1.7 Save Backup

Industrial HiVision lets you save the information you require to restore Industrial HiVision installation.
For this purpose, Industrial HiVision writes the following information in a ZIP file:

- PSM list and PSMs
- Configuration (service properties files)
- Project database
- Reporting database
- License files
- Log files
- User reports
- User scripts, tasks and task results
- info.txt file with version information

Upon summoning “Save Backup“, Industrial HiVision opens a file selection dialog. You are able to specify the destination of the backup file here.

Note: To load the backup file you require the same version of Industrial HiVision that you used to write the backup file. You will find version information in the info.txt file in the backup zip file

8.1.8 Load Backup

Industrial HiVision allows you to restore a damaged Industrial HiVision installation.
For this purpose, a Industrial HiVision backup ZIP files contains the following information:

- PSM list and PSMs
- Configuration (service properties files)
- Project database
- Reporting database
- License files
- Log files
- User reports
- User scripts, tasks and task results
- info.txt file with version information

After starting “Load Backup“, Industrial HiVision opens a file selection dialog. You are able to specify the location of the backup file.

Note: To load the backup file you require the same version of Industrial HiVision that you used to save the backup file. You will find the version information in the info.txt file in the backup zip file.

8.1.9 Export...

With this selection you export the content of the detail display.
Industrial HiVision exports graphics (topology representation) as a:

- PDF file,
- jpg file,
- png file and
- bmp file.

Industrial HiVision exports tables as a:

- PDF file
- HTML file
- CSV file (see on page 457 “CSV export”)

☐ Select `File > Export...` and select the file type in the “Save“ window.

8.1.10 Export Events...

With this selection you export the complete event list as:

- PDF file
- HTML file
- CSV file (see on page 457 “CSV export”)

☐ Select `File > Export Events...` and select the file type in the “Save“ window.

8.1.11 Print

With this selection you print the content of the detail display.

☐ Select `File > Print`.
Industrial HiVision creates a temporary PDF file of the content of the detail display and opens this PDF file in the PDF display program for example, Acrobat Reader, that is installed on your management station.

8.1.12 Print Events

With this selection you print the complete event list.

☐ Select `File > Print Events`.
Industrial HiVision creates a temporary PDF file of the content of the detail display and opens this PDF file in the PDF display program for example, Acrobat Reader, that is installed on your management station.

8.1.13 Exit and Stop Service

This selection is available when running on the Windows operating system. With this selection you exit both the program and, for the local service, the service. By exiting the service you also interrupt the monitoring of your network.

8.1.14 Exit

You use this selection to quit the program. The service remains active in the background and continues to monitor your network.

8.2 Edit

The “Edit“ menu contains functions relating to editing operations and device properties.

8.2.1 Undo

With this selection you undo the last change you made in the program.

8.2.2 Redo

With this selection you redo the last change you made in the program, which you had previously undone.

8.2.3 Edit Mode

You use this selection to activate/deactivate the “Edit Mode“.
You require the relevant access rights for this function, see “Edit Mode” on page 84.
To avoid writing conflicts, Industrial HiVision prevents the “Edit Mode“ from being activated on multiple user interfaces at the same time.

8.2.4 Switch to the free version

With this selection you switch during the free 30-day trial period between the licensed version and the free version.
Industrial HiVision offers 3 versions:

- Licensed version
  After you enter a license key, Industrial HiVision runs as the licensed version. As the licensed version, Industrial HiVision gives you the full function range.
- Free 30-day trial version (licensed)
  After a new installation or after an update, Industrial HiVision starts fully functional for the duration of the free 30-day trial period.
  During the last 7 days of the trial period, a message window tells you that the trial period is running out and that you can save the project file before the trial period expires. If Industrial HiVision is idle during this time, Industrial HiVision shows this message window when it starts again.
- Free version
  As the free version, Industrial HiVision offers the option of detecting devices of Hirschmann and performing updates on the detected devices.

8.2.5 Cut

You use this selection to put data you have selected (screen element, components, devices with their settings) into the clipboard.
The data is deleted, and you can add it in again at another position using the “Paste“ menu item.
You can also copy the names of objects into other applications, such as a text editor.

8.2.6 Copy

You use this selection field to put data you have selected (screen element, components, devices with their settings) into the clipboard.
The data remains where it is, and you can add a copy of it at another position using the “Paste“ menu item.
You can also copy the names of objects into other applications, such as a text editor.

8.2.7 Paste

You use this selection field to add the data (screen element, components, devices with their settings) in your clipboard at the position where your cursor is currently located.

8.2.8 Paste as Link

You use this selection field to add the data (screen element, components, devices with their settings) in your clipboard as a link at the position where your cursor is currently located. Only a reference to the data is inserted. The data themselves remain in their original position (see on page 139 “Creating a link”).

8.2.9 Delete

You use this selection to delete data you have selected (screen element, components, devices with their settings).
When deleting devices, Industrial HiVision allows you to delete the device or move the device into the “Unused Devices“ folder.

8.2.10 Rename

With this selection you rename a selected folder or a tagged device.

8.2.11 Select All

You use this selection to select all parts inside the active folder.

8.2.12 Acknowledge Status Change

You use this selection to acknowledge the status change of the selected components and their sub components.

8.2.13 Manage

With this selection you activate the monitoring of the selected devices (see on page 269 “Unmanage”).

8.2.14 Unmanage

With this selection you deactivate the monitoring of the selected devices. Industrial HiVision keeps the device, its configuration and its current values stored in the database. The monitoring of the device is off until you set it to “Manage“ again (see on page 269 “Manage”). Industrial HiVision releases the license of this device and allows you to use this license for another device.
Industrial HiVision displays a device in the “Unmanage“ state in gray with a stop symbol.

8.2.15 Set Device and Port Names

With this selection you set the detail window to display the following items:
– the device name and port name of the selected devices, instead of
– the IP address and port numbers of the selected devices.

8.2.16 Set Default Device Icon

With this selection you take the symbol for display from the device class. If no default symbol exists for the device class, Industrial HiVision takes the device symbol entered in the preferences (see on page 366 “Device Icon”).

8.2.17 Device Documentation

With this selection, Industrial HiVision generates a PDF file to:
- “Document Selected Devices“
- “Document All Devices“

The PDF file contains information about the device and its settings.

☐ Make a selection and specify the folder in which you want Industrial HiVision to save the PDF files.

8.2.18 Drawing Size

You use this selection to adapt the size of the drawing area for the detail display to meet your requirements. Industrial HiVision provides you with three options for doing this:

- “Enlarge“
- “Reduce“
- “Shrink to Fit“

8.2.19 Background Image

You use this selection field to load, remove or change the background image in your detail display. The following options are available:

- “Paste as Background“
  When you select “Paste as Background“, you add the image in your clipboard to your detail display as a background image. If the clipboard is empty, this menu item is marked in grey and cannot be selected.

- “Select Background Image...“
  When you select “Select Background Image...“ you add the image from a file to your detail display as a background image. Select the relevant path and the desired file within your folder structure.

  Note: High-resolution background images sap the resources of your network management station and therefore reduce the performance of your system.

- “Remove Background Image“
  When you select “Remove Background Image“, you delete the background image in your detail display.

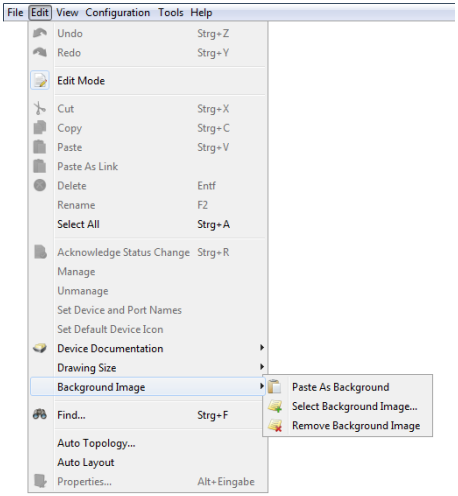


Figure 54: Edit:Background image

8.2.20 Find...

The “Find“ dialog allows you to search for components, MAC addresses or IP addresses in the display.

☐ Select the “Devices by IP Address“ tab if you are searching for an IP address or “Components by Name“ if you are searching for part of a device.

☐ Enter

- ▶ the IP address/MAC address or a part of it, or
- ▶ the component name or a part of it without using wildcards.

☐ Select a device on the left of the tree diagram or a folder in which you want Industrial HiVision to search.

☐ Click the “Find“ button to start searching.

Industrial HiVision displays the result of the search in a list of the search dialog. When you double-click on a line in this list, Industrial HiVision selects the component you want to find in the folder frame.

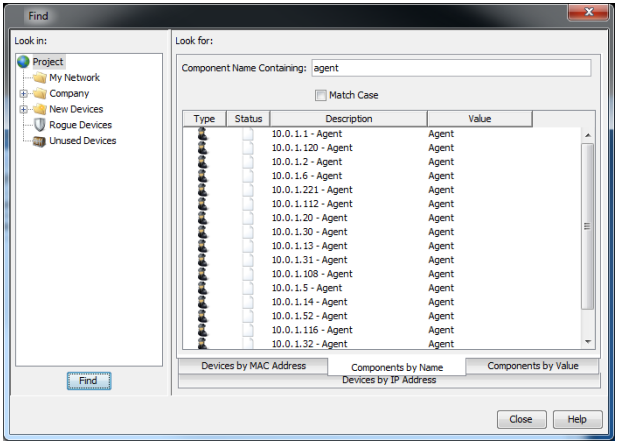


Figure 55: Edit:Find

8.2.21 Auto Topology...

The “Auto Topology...“ function allows you to automatically create the links between the devices. For the topology discovery, Industrial HiVision uses the Forwarding Data Base (FDB) and the LLDP and SNMP functions of the devices.
IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP enables the user to have automatic topology recognition for his LAN. Industrial HiVision detects redundancy mechanisms, such as RSTP, redundant network coupling or HIPER-Ring. Industrial HiVision represents every redundant connection as a separate connection.

Industrial HiVision can detect the terminal device topology across the subnetworks if the router separating the subnetworks supports the SNMP ipNetToPhysicalTable.

☐ Select `Edit > Auto Topology...`

☐ In the dialog for automatic topology discovery, you select how you want Industrial HiVision to execute the “Auto Topology...“ function.

Selection	Action
Entire Network (Recommended)	Detects the topology of the entire network, including switches, routers, WLAN and terminal devices and reads large data quantities from the devices. In large networks, Topology Discovery can take up a significant amount of time. In this case “Entire Network” means the Layer 2 network that is connected with the network interface card of the network management station and all the reachable VLANs.
Infrastructure	Only detects the topology of the infrastructure devices based on LLDP. Is performed very quickly and sometimes with gaps.

Table 26: “Scope“

Selection	Action
Unmanaged Nodes	Industrial HiVision derives topology information from devices without the management function and from devices without an Industrial HiVision license from the information in known neighboring devices. Industrial HiVision represents these unknown devices as a cloud. A cloud can represent one or more unknown devices.

Table 27: “Unmanaged Nodes“

Selection	Action
Create New Topology	Create a completely new topology. Removes existing connections and clouds. Then creates new topology.
Complement Topology	Enhance existing topology, Creates new connections and clouds. The existing connections are kept.
Update Topology	Adds missing connections and removes connections that differ from the current topology. Keeps existing clouds if they correspond to the current topology.

Table 28: “Strategy“

Selection	Action
Automatic	Industrial HiVision unravels the topology and reassigns the objects.
Manual	Industrial HiVision leaves the objects in their current positions.

Table 29: “Layout“

Selection	Action
Current Folder	Performs the selected actions only in the selected folder.
Recursive	Industrial HiVision performs the automatic Auto Topology Discovery in the current folder and in the folders below it, and displays the results in both the current folder and the folders below it.

Table 30: “Range“

☐ Click the “OK“ button.

Then Industrial HiVision queries the links in the network in accordance with the settings and displays the detected links in the interface.

Note: Topology Discovery

- Network components that do not conform to the LLDP specifications or cannot be managed using SNMP can lead to incorrect Auto Topology Discovery.
- An active DHCP request during the discovery procedure can corrupt the result of the discovery.
- VLAN routing can corrupt the result of the discovery.
  MACH 3000 M-Router modules work with VLAN routing.
- To detect subnetworks behind 1:1 NAT routers, select “Infrastructure“ under “Scope“(see table 26).
- In order to identify the topology with VRRP routers correctly, Industrial HiVision requires at least one of the VRRP routers to be located in the same folder or subfolder, where you start the automatic topology function.
- Detecting devices of an LAN behind a wireless client device:
  The BAT-Devices from Hirschmann have the “client bridge support” function.
  For Industrial HiVision to be able to detect devices of an LAN behind a wireless client device, activate the “client bridge support” function in the wireless client device and in the related WAN on the access point.
- Redundantly connected terminal devices can corrupt the result of the discovery.
- The topology discovery detects the topology at the time at which it is executed.
  Industrial HiVision displays other changes in the network (e.g. roaming) when you update the topology display.

Auto Topology for undiscovered devices

The Industrial HiVision “Auto Topology...“ function was made for flat layer 2 topologies. Changes were made for routed topologies, but in rare cases, the detected topology can be incorrect or not complete. The following work steps help you make a topology of your entire network.

This step makes the topology with the information that the devices provide only through LLDP over SNMP.
An example of a device that is in this category is the Dragon PTN.

Do these steps in the root project folder.

☐ Specify the following values in the “Auto Topology“ dialog:
- “Scope“: `Infrastructure`
- “Unmanaged Nodes“: as necessary
- “Strategy“: `Create New Topology`

- – “Layout“: as necessary
- – “Range“: `Recursive`

After Industrial HiVision finishes scanning the devices in the selected folder, the “Map“ tab displays the network topology. The topology can still be incomplete.

Rescan your network using the following steps:

☐ Select the desired folder from the folder frame.
☐ Right-click a blank space in the “Map“ tab.
☐ Select “Auto Topology...“ from the drop-down list.
☐ Specify the following values in the “Auto Topology“ dialog:
- – “Scope“: `Entire Network (Recommended)`
- – “Unmanaged Nodes“: as necessary
- – “Strategy“: `Complement Topology`
- – “Layout“: as necessary
- – “Range“: `Current Folder`

8.2.22 Auto Layout

The “Auto Layout“ function gives you the option of leaving the assignment of the devices to Industrial HiVision.

☐ Select `Edit > Auto Layout`.

☐ To get Industrial HiVision to reposition the objects in the detailed display, click the “OK“ button.

8.2.23 Properties of a folder/device

The “Properties...“ dialog contains the “Properties“, “Subcomponents“, “Status Reason“, “Scan Range“, “Protocols“, “IP Address“ and “MAC/IP Addresses“ tabs.
The “Protocols“ and “MAC/IP Addresses“ tabs describe device properties.

Properties of a folder/device

The “Properties“ tab displays the general properties of the component display.
You click on a symbol once to open a dialog for selecting an image for Industrial HiVision to use in the display. Industrial HiVision adapts the image size automatically.
The status display is important for monitoring your network. Here you select whether Industrial HiVision determines the status of this component and whether Industrial HiVision forwards the status determined to the next highest level. In the basic setting, Industrial HiVision determines the status and forwards it to the next highest level.

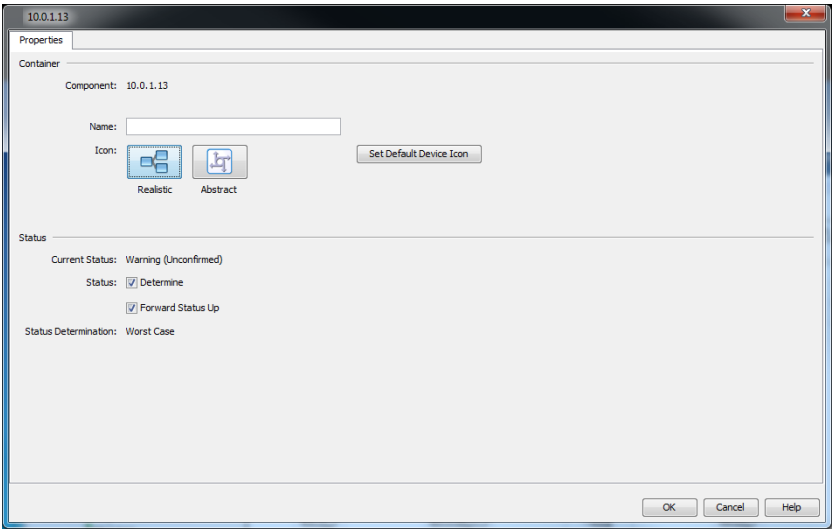
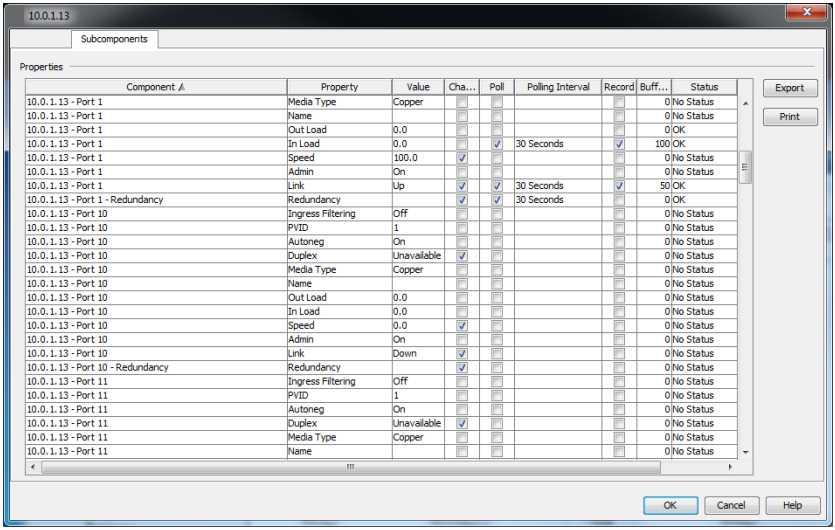


Figure 56: Properties of a folder/device

Subcomponents of a device/folder

The “Subcomponents“ tab displays a table of the entire parts of the component from which you can open the “Configuration Signature“:“Properties“ dialog.
Along with the names of the parts, the table also contains the values of the different properties of these parts.



Component	Property	Value	Cha...	Poll	Polling Interval	Record	Buff...	Status
10.0.1.13 - Port 1	Media Type	Copper					0	No Status
10.0.1.13 - Port 1	Name						0	No Status
10.0.1.13 - Port 1	Out Load	0.0					0	OK
10.0.1.13 - Port 1	In Load	0.0		✓	30 Seconds	✓	100	OK
10.0.1.13 - Port 1	Speed	100.0	✓				0	No Status
10.0.1.13 - Port 1	Admin	On					0	No Status
10.0.1.13 - Port 1	Link	Up	✓	✓	30 Seconds	✓	50	OK
10.0.1.13 - Port 1 - Redundancy	Redundancy		✓	✓	30 Seconds		0	OK
10.0.1.13 - Port 10	Ingress Filtering	Off					0	No Status
10.0.1.13 - Port 10	PVID	1					0	No Status
10.0.1.13 - Port 10	Autoneg	On					0	No Status
10.0.1.13 - Port 10	Duplex	Unavailable	✓				0	No Status
10.0.1.13 - Port 10	Media Type	Copper					0	No Status
10.0.1.13 - Port 10	Name						0	No Status
10.0.1.13 - Port 10	Out Load	0.0					0	No Status
10.0.1.13 - Port 10	In Load	0.0					0	No Status
10.0.1.13 - Port 10	Speed	0.0	✓				0	No Status
10.0.1.13 - Port 10	Admin	On					0	No Status
10.0.1.13 - Port 10	Link	Down	✓				0	No Status
10.0.1.13 - Port 10 - Redundancy	Redundancy		✓				0	No Status
10.0.1.13 - Port 11	Ingress Filtering	Off					0	No Status
10.0.1.13 - Port 11	PVID	1					0	No Status
10.0.1.13 - Port 11	Autoneg	On					0	No Status
10.0.1.13 - Port 11	Duplex	Unavailable	✓				0	No Status
10.0.1.13 - Port 11	Media Type	Copper					0	No Status
10.0.1.13 - Port 11	Name						0	No Status

Figure 57: Subcomponents of a folder/device

Status Reason

If you hover over an item in the folder pane or in the “Map“ view, then Industrial HiVision displays a status list containing the current detected warnings and errors. You can also view the status list in the `View >` Properties `> Status Reason` tab.

The “Status Reason“ tab is available for the following items:

- Folders
- Devices
- Containers - a sub-folder of a device folder
- Connections

As an example for this function, the status of a device in your network continually displays detected errors. You want to maintain a history of the status list for future reference.

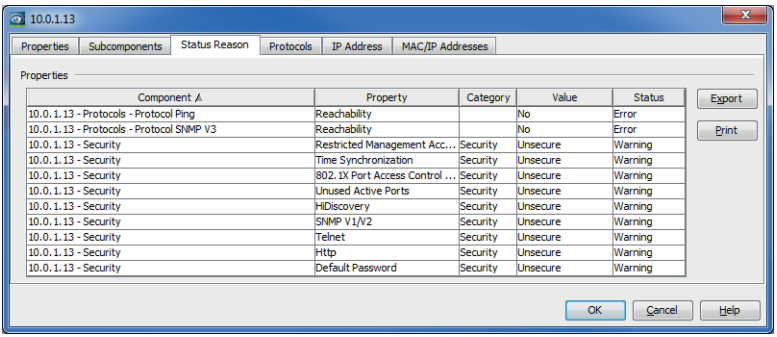
To save the status list as a PDF file, proceed as follows:

- ☐ Select the device for which you want to save the status list.
- ☐ On the tool bar, click `View > Properties`. Industrial HiVision opens the “Properties“ dialog.
  Alternatively, to open the “Properties“ dialog, right-click on the selected device. In the drop-down list, select the “Properties“ function.
- ☐ Open the “Status Reason“ tab.
- ☐ To save the status list on your PC, click the “Export“ button. The “`Save`” dialog opens.
- ☐ Navigate to the location where you want to save the file.
- ☐ In the “`Save> File name`” text field, enter an appropriate name for the file.
- ☐ In the “`Save> Files of type`” pull-down list, select “Adobe Portable Document Format“.
- ☐ Click the “`Save`” button.
- ☐ To close the “Properties“ dialog, click the “OK“ button.

You can save the status list in the following formats:

- ▶ PDF file
- ▶ HTML file
- ▶ CSV file

Note: The “Print“ button opens the status list in your default PDF program.



Component	Property	Category	Value	Status
10.0.1.13 - Protocols - Protocol Ping	Reachability		No	Error
10.0.1.13 - Protocols - Protocol SNMP V3	Reachability		No	Error
10.0.1.13 - Security	Restricted Management Acc...	Security	Unsecure	Warning
10.0.1.13 - Security	Time Synchronization	Security	Unsecure	Warning
10.0.1.13 - Security	802.1X Port Access Control ...	Security	Unsecure	Warning
10.0.1.13 - Security	Unused Active Ports	Security	Unsecure	Warning
10.0.1.13 - Security	HiDiscovery	Security	Unsecure	Warning
10.0.1.13 - Security	SNMP V1/V2	Security	Unsecure	Warning
10.0.1.13 - Security	Telnet	Security	Unsecure	Warning
10.0.1.13 - Security	Http	Security	Unsecure	Warning
10.0.1.13 - Security	Default Password	Security	Unsecure	Warning

Figure 58: “Status Reason“ of a folder or device

Scan range of a folder

The “Scan Range“ tab enables you to define IP address ranges. Industrial HiVision displays newly detected devices with IP addresses from one of these IP address ranges in this folder (see on page 406 “Scan Ranges”).

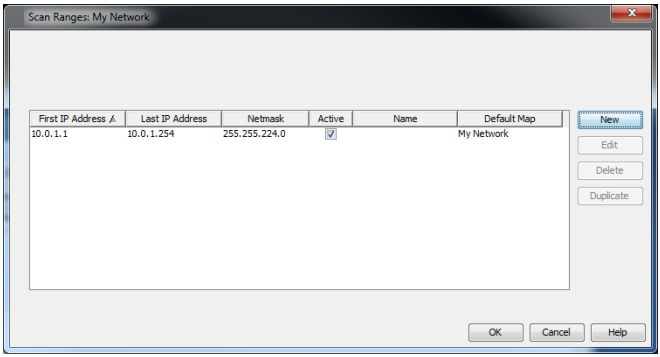


Figure 59: Scan ranges of a folder

Protocols of a device

The “Protocols“ tab displays a table of the protocols that are supported and their properties.

Depending on the devices, Industrial HiVision supports the protocols:

- Ping
- SNMP V1
- SNMP V3
- HiDiscovery V1
- EtherNet/IP
- Modbus/TCP
  Industrial HiVision supports the Modbus/TCP command `Read Device Identification (43 / 14)` exclusively.

Industrial HiVision uses the highest possible protocol (sequence: SNMP V3, SNMP V1, Modbus/TCP, Ping) to monitor a device.

You use “Reload“ to get Industrial HiVision to query protocols of the device again.

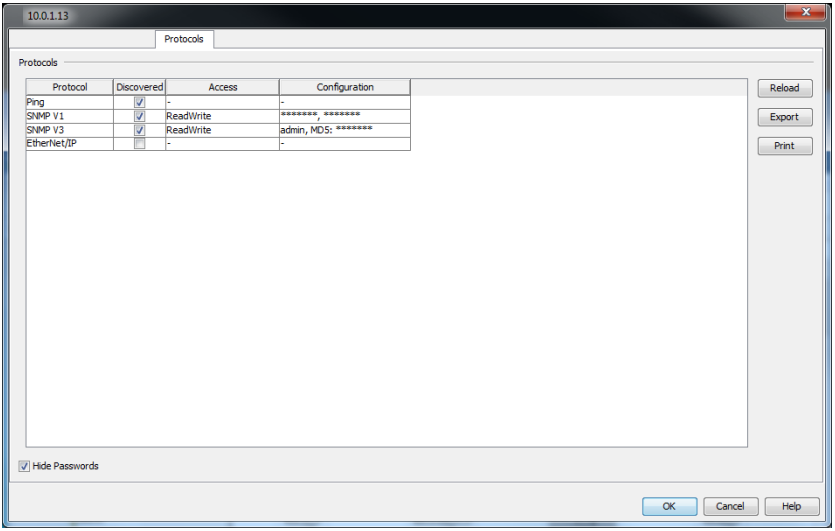


Figure 60: Protocols of a device

IP address of a device

The “IP Address“ tab allows you to change the IP address and the SNMP port number for current devices for Industrial HiVision in this dialog.
You require this function to re-access a known device with Industrial HiVision, whose IP address was changed directly on the device.
If you want to change the IP address on a device, you select the device and use the `Configuration > IP Configuration` (see on page 415 “IP Configuration”).

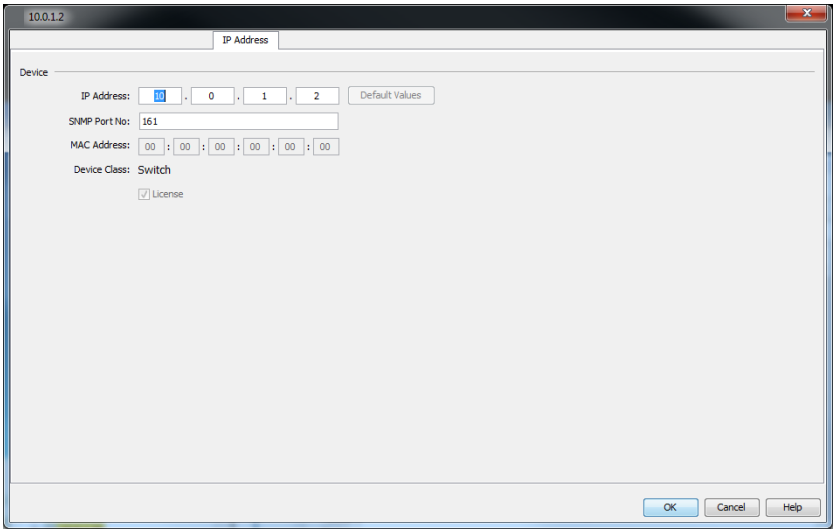


Figure 61: IP address for a current device

MAC/IP addresses of a device

The “MAC/IP Addresses“ tab displays a list of the IP addresses in the device and their related MAC addresses. The list contains:

Parameter	Meaning
MAC Address	
IP Address	
Netmask	
Host Name	Host name from the /config/hosts.txt file in the installation directory if ▶ the file exists, ▶ there is an entry and ▶ the determination of a device name is activated in the basic settings. Otherwise, the field remains empty.
DNS Name	Name from the Domain Name Service
Port No	Port number of the protocol.
Port	Device port
Management	Industrial HiVision communicates with the management of the device by means of the IP address in this row.
User Generated	The device in this row was generated by the user. Industrial HiVision has not detected this device yet.
Router Entry	The IP address in this row comes from the routing table of the device.

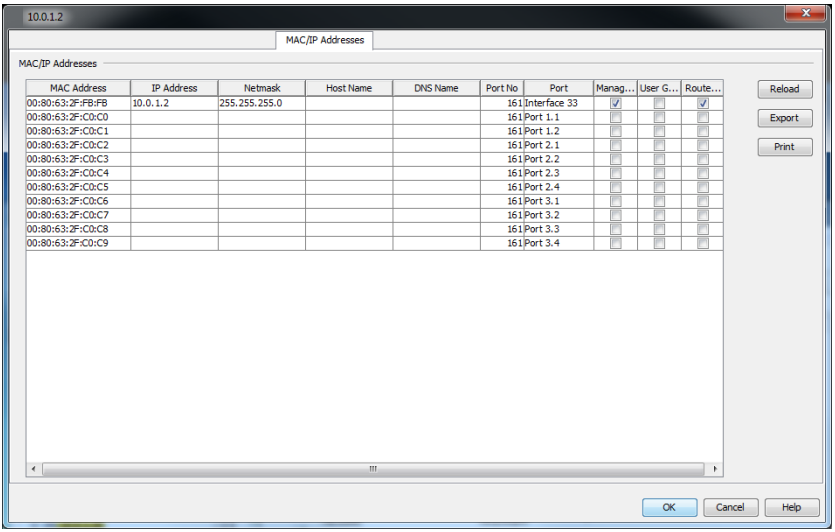


Figure 62: MAC/IP address and name of a device

8.2.24 Properties of a component detail

In the “Properties of a component detail” dialog, you are at the lowest level of the status determination. In addition to the properties that are on higher levels, this dialog contains a specifically determined value. If you want to observe this value, you can query it at freely specified intervals and log it. Value range for the polling interval: ≥5 seconds.

To set up a component detail property, proceed as follows:

- ☐ Select a device or port from the folder frame.
- ☐ Open the “List“ tab.
- ☐ To open the property dialog for the property you wish to change, double-click on the property.
- ☐ Specify the value.
- ☐ Click the “Write“ button.

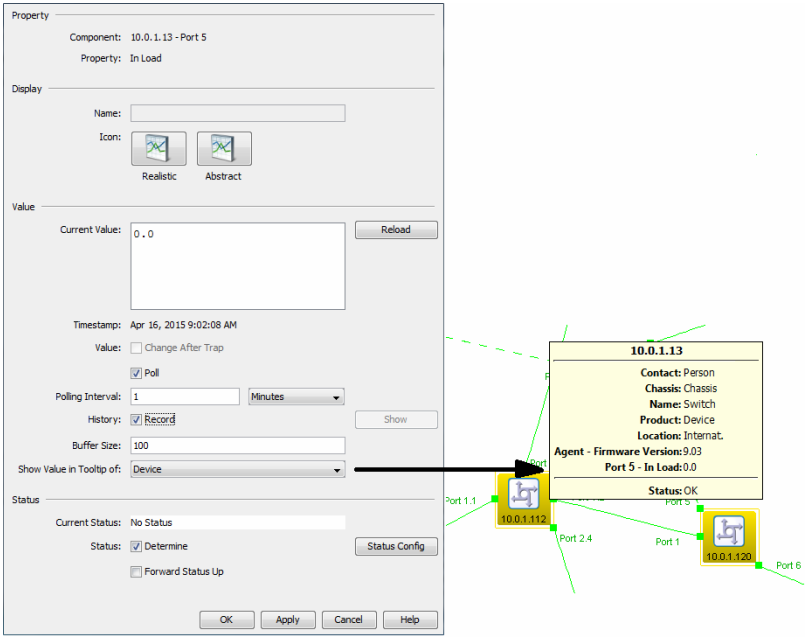


Figure 63: Detail properties

You can edit the name of the property if you have previously permitted renaming in the settings (see on page 370 “Program Access”).

- To perform logging, select `History > Record`.
  To display the history in the another window, click the “Show“ button. You can use the tab selection in this window to choose between tabular and graphic views.
  The graphic view is available if the property is of the counter type.

- With “Buffer Size“ you specify how many entries the history buffer can contain.

  Note: If you increase the “Buffer Size“ value, from the default value of `100`, then this causes the performance of Industrial HiVision to decrease.

- To display this value in the bubble help of a higher-level component, select the component in the “Show Value in Tooltip of“ drop-down list (see figure 63).

In the “Status Config“ dialog, you specify how a change in this value affects the display of the status.

Aside from monitoring your network, Industrial HiVision also allows you to set up the following properties on the component detail level, if the device supports this option:

- “Name“ of the Port
  Assign the port any readable name.
- “Admin“ for the Port Status
  Enable/disable the port.
- “Autoneg“
  Enable/disable the auto-negotiation function.
- “Name“ of the Device
  Assign the device any readable name.
- “Contact“
  Name the contact person for the device.
- “Location“
  Name the location of the device.
- “Signaling“
  To identify a specific device among several devices in the same location.

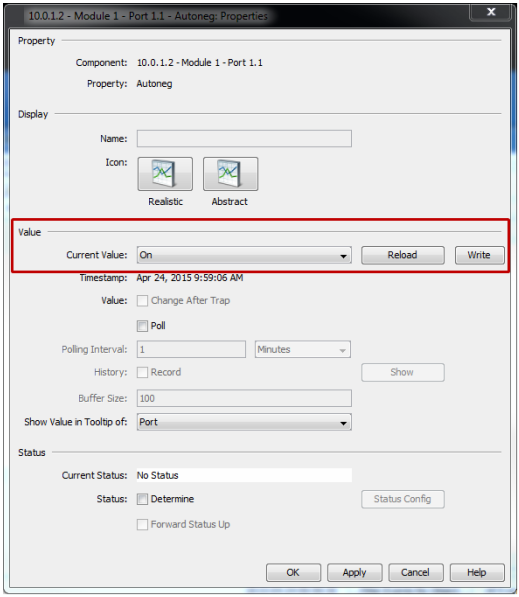


Figure 64: Configuring detail properties

Specified values

The “Status Config“ dialog displays the possible values of the component detail.
Use the drop-down list to assign the statuses you require to the values.
The operators provide you with further options for the definition of the status configuration.

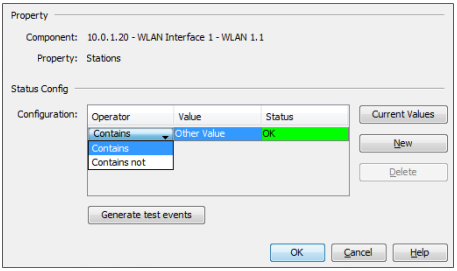


Figure 65: Example for the status display of default values

List values

The “Status Config“ dialog displays a list with current values of the component detail.
Use the drop-down list to assign the statuses you require to the values. In contrast to “Defined values”, the values are variable and you can use “Current values” to read in the currently available values, use the “New“ button to enter your own values in the list and use the “Delete“ button to delete values from the list.

Application example: You want an error message when unauthorized stations login to an access point. Enter the permitted stations in the list and set “Other Value” to “Error” (see figure 66).

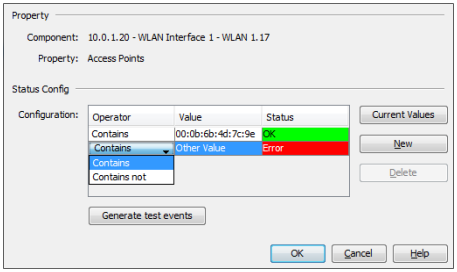


Figure 66: Status display for list values

Numeric values

The “Status Config“ dialog allows you to enter threshold values numerically.
Use the drop-down list to select the statuses which Industrial HiVision assigns to the device when these threshold values are exceeded or not reached.

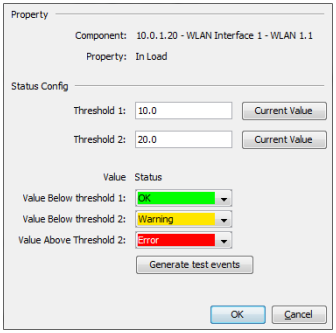


Figure 67: Status display for numeric values

Alphanumeric character string

The “Status Config“ dialog allows you to assign an alphanumeric value to the device detail.
Use the drop-down list to select the statuses which Industrial HiVision assigns to the device for other character strings.
Example: On a port enter the MAC address of the connected device. If the MAC address of the connected device is correct, assign the status “OK“. If the MAC address of the connected device is different, assign the status “Error“. As soon as the MAC address changes, you get an error message.

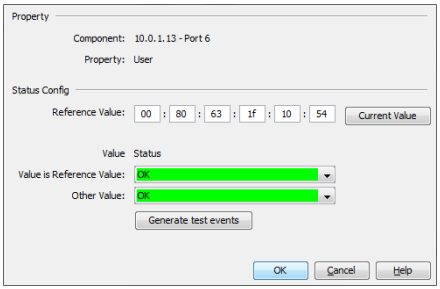


Figure 68: Status display for alphanumeric values

Generate test events

The “Generate test events“ button offers you the possibility to generate events related to properties status changes. You can then assign one of the newly generated events to an alarm.

After you click the “Generate test events“ button, Industrial HiVision opens the “Test Events“ dialog so that you can review the generated events. You can view the same generated events in the “Test Events“ tab of the “Import event“ dialog. If you select an event in the “Test Events“ tab, then you can assign it to an alarm.

Industrial HiVision does not enter the test events in the event list.

In this example, you generate test events, then assign an action to an event. To generate test events proceed as follows:

- ☐ Double-click on a device for which you wish to generate a test event.
- ☐ In the “List“ tab, right-click on the property for which you wish to generate a test event.
- ☐ In the drop-down list, select the “Properties...“ option.

- ☐ In the “Status“ frame, mark the “Determine“ checkbox.
- ☐ Click the “Status Config“ button.
- ☐ In the “Status Config“ frame, configure the property to generate the necessary event.
- ☐ Click the “Generate test events“ button.
- ☐ Click the “Close“ button.

To assign an action to an event proceed as follows:

- ☐ Open the “Preferences“ dialog.
- ☐ Select “Event Actions“ from the menu tree.
- ☐ Verify that an action is available in the “Actions“ table.
- ☐ In the “Alarms“ frame, click the “New“ button.
- ☐ In the “Filter“ frame, click the “Import...“ button.
- ☐ In the “Import event“ dialog, select the “Test Events“ tab.
- ☐ Select the event for which you wish to assign an action.
- ☐ Click the “OK“ button.
  Industrial HiVision takes the information from the event and enters it in the “Filter“ frame.
- ☐ Mark the checkbox in the “Actions“ table for the action that you wish Industrial HiVision to perform.
- ☐ Click the “OK“ button.

8.2.25 Properties of a connection

The properties dialog of a connection consists of 2 tabs: “Connection“ and “Properties“
You can access a third property, the history of the connection, by double-clicking on the connection.

To access the properties dialog, right-click on a connection and select “Properties...“ from the drop-down list.

Connection

On the “Connection“ tab you select the ports which are connected. To give you a better overview, the dialog provides you with an option of selecting the ports that will appear in the selection display.
If the speed display is activated, when the speed is increasing Industrial HiVision increases the line thickness in 2-point steps at 10, 100, 1000, 10000 MBit/s. If the speed display is activated, Industrial HiVision displays the current connection setting in the bubble help.
If the speed display is deactivated, Industrial HiVision displays the current speed setting even if you have activated the speed display in the connection properties dialog (see on page 360 “Device”).
With automatic display of the connection medium using the connection end icon, Industrial HiVision selects the respective icon. Industrial HiVision allows you to define the connection end icon for a connection yourself. This option enhances clarity when conditions prevent determination of the medium.
If observing the connection is important for you, you can query the following standard parameters at freely specified intervals:

- Link status
- Load (incoming load)
  If a terminal device on a connection does not supply a value for the incoming load, then Industrial HiVision displays the outgoing load of the other end of the connection as the incoming load at this end.
- Port redundancy
- WLAN port properties

Industrial HiVision uses “Record““Load History“ to store the value of the queried incoming load on an ongoing basis.

Properties

The “Properties“ tab for the connection allows you to give the connection any name you want and to specify the status handling.
The status display can be used for monitoring your network. Here you select whether Industrial HiVision determines the status of this connection and whether Industrial HiVision forwards the status determined to the next highest level. In the default setting, Industrial HiVision determines the status and forwards it to the next highest level, as soon as you have assigned the connected ports (see below).

Under “Availability“, you can find the fields for entering the “MTBF“ and “MTTR“ values that Industrial HiVision uses for calculating availability (see on page 442 “Calculate Availability”).

8.2.26 Adding a component detail to a port

Industrial HiVision provides the monitoring of many component details for the individual components. Industrial HiVision provides an overview of a selection of these details.

To add another component detail to a port, proceed as follows:

☐ Select a port from the folder frame
☐ Open the “List“ tab.
☐ Right-click on the empty space in the “List“ dialog.
☐ Select `New > Property`.

Industrial HiVision then provides you with a list of additional component details. A component detail is available as a “Delta“ type and “Absolute“ type.

- “Delta“: The monitoring refers to the difference between the values for two consecutive inquiries. The symbol of the delta property is a triangle in the top right corner.
- “Absolute“: The monitoring refers to the absolute value for each particular inquiry.

Figure 69: Symbols for Delta and Absolute properties

☐ You double-click on a row to select the corresponding component detail and thus create a symbol for this component detail in the detail display.

☐ Right-click on the symbol and select “Properties“ to open the “Properties of a component detail” dialog, See “Properties of a component detail” on page 285.

8.2.27 Add to reporting

The reporting function allows you to manage long-term statistics outside of the database of the network management system program.

You can add the following items to the reporting function:
- Pollable device details
- Connections between 2 devices, at both ends of which Industrial HiVision has detected a link status.

☐ To add a device detail or a connection to the reporting function, right-click on the device detail or the connection detail and select “Add to Reporting...“.
☐ To add more than 1 device detail at a time to the reporting function, proceed as follows:
  ☐ Open the “Properties“tab.
  ☐ Highlight the items that you want to add.
  ☐ Right-click on a property.
  ☐ Select the “Add to Reporting...“ option.

Note: If a device detail was previously added to the reporting function, then Industrial HiVision displays a message stating how many items were not added in the “Add Properties to Reporting“ dialog. The “Reporting“ dialog displays the monitored items (see on page 309 “Reporting”).

The dialog allows you to use “Record“ to activate/deactivate the reporting for this property or this connection. If you deactivate the reporting, the entry remains in the reporting function (see on page 309 “Reporting”). For the reporting, you have the choice of recording the value or recording the status.

“Start“ and “Stop“ allow you to define when the recording starts and when it stops. With the default setting, the recording begins right after you click the “OK“ button and continues for as long as the Industrial HiVision service is running.

If you previously activated the polling for the property or the connection, or if you changed the polling interval, this setting is kept. Otherwise Industrial HiVision activates the polling and sets the polling interval to the minimum value of `30` seconds.

Polling interval setting:

- Minimum value: `30 seconds`
- Possible values: multiples of 30 seconds

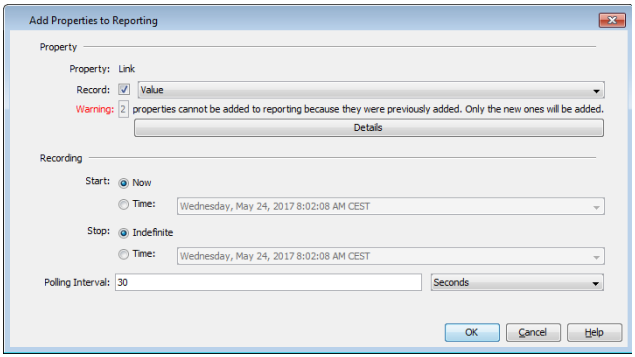


Figure 70: Add property to reporting

8.2.28 Device and Port Signaling

The signaling function lets you to identify a device or port using the LEDs of the device. When making new connections, this function allows you to verify the proper device and port.

Signaling devices and ports

To activate the signaling function on a device, proceed as follows:

- ☐ Verify that Industrial HiVision is in the “Edit Mode“.
- ☐ Double click on the device on which you wish to activate the signaling function.
- ☐ Open the “List“ tab.
- ☐ Right click on the “Signaling“ entry.
- ☐ Select “Properties“ from the pull down list.
- ☐ In the “Value“ frame, in the “Current Value“ pull down list, select the “On“ option.
- ☐ Click the “Write“ button.

The table in the “List“ tab displays the “Signaling“ function as “On“, and the LEDs on the device blink for 10 seconds. After 10 seconds the entry changes to “Off”.

The steps to activate the “Signaling“ function on a port are similar to the steps described above. The only difference is that you highlight the port for which you wish to activate the “Signaling“ function.

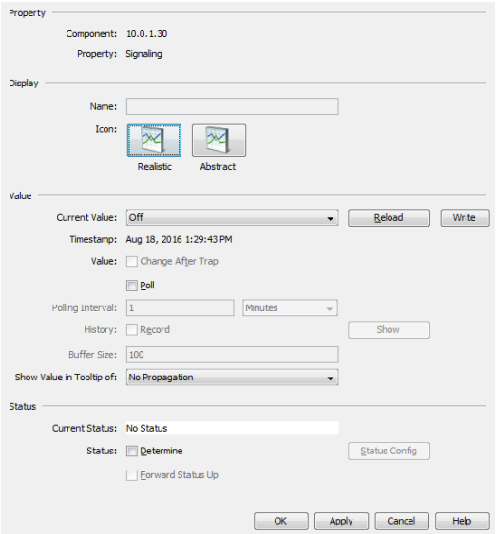


Figure 71: Signaling proprieties dialog

Signaling function support

The following list contains the devices and software versions that support the Industrial HiVision “Signaling” function:

Type of device	Since Version	Device Signaling	Port/Connection Signaling
Classic	09.0.01	X	
HiOS	04.0.00	X	X
HiSecOS	03.0.00	X	

Table 31: Signaling supported software

8.3 View

The “View“ menu contains functions to navigate through the history of the content of the detail display frame.

8.3.1 Select VLAN

This function allows you to see the VLAN membership of the detected devices and links based on the colors in which they are displayed.

☐ Select `View > Select VLAN`.
Industrial HiVision opens a dialog for selecting a VLAN.

☐ In the drop-down list, select the VLAN ID for the VLAN whose VLAN membership you want to see.
Industrial HiVision displays the devices and links that belong to other VLANs in light gray. The devices of the selected VLAN remain in color or in dark gray.

At the top of the folder frame, Industrial HiVision displays the selected VLAN.

8.3.2 Refresh VLANs

This function allows you to refresh the VLAN information on the Hirschmann devices.

☐ To refresh the VLAN information select a node in the object frame.

☐ On the menu bar, select `View > Refresh VLANs`.
Industrial HiVision refreshed the information in the subcomponents of the selected node.

8.3.3 Protocol Statistics

The Protocol Statistics give you an overview of the response time behavior of the devices with Industrial HiVision with regard to the protocol communication. This overview helps you find out whether the response time behavior is the cause if Industrial HiVision cannot set up the communication with individual devices.

You can specify the number of samples from which Industrial HiVision calculates the movable average response time for both ICMP and SNMP.

☐ Open the `Configuration > Preferences > Services` dialog.
☐ You can specify the number of ICMP samples using the “ICMP Statistics - Moving Average Number of Samples“ parameter.
☐ You can specify the number of SNMP samples using the “SNMP Statistics - Moving Average Number of Samples“ parameter.

The dialog displays the moving average as `0` until Industrial HiVision calculates the first average.

Parameter	Meaning
Device	IP address of the device to which the entries in this line apply
Protocol	Relevant protocol via which Industrial HiVision communicates with the device
Requests	Number of requests from Industrial HiVision since the last reset
Responses	Number of responses from the device since the last reset
Timeouts	Number of cases in which the device required longer for a response than was entered in the settings
Errors	Number of packets deviating from the standard
Msg Loss [%]	Pkt. loss [%] = packet loss [%] = 1-(replies/requests) * 100
Avg Resp [ms]	Average value of response times
MAvg Resp [ms]	Movable Average value of response times.
Min Resp [ms]	Minimum wait period for a response
Max Resp [ms]	Maximum response time for a reply
Std Dev	Standard deviation of the response times = measurement for the variation
Try 1	Number of responses received after the first request attempt. Depending on your settings in the SNMP configuration in Industrial HiVision, Industrial HiVision creates columns with “Try“ 2, “Try“ 3, etc. The “Try“ 2 column then only contains the number of responses received after the 2nd request attempt.

Table 32: Log statistics

Industrial HiVision provides you with a portion of the protocol statistics as detailed information for each device. You will find “Avg Resp [ms]“ and “Std Dev“ in the log properties of a device.
You can use the reporting function to analyze the behavior of individual devices more precisely. To do this, you add these log details in a report.

With “Export“ you can save the complete table as a:

- PDF file
- HTML file
- CSV file (see on page 457 “CSV export”)

With “Print“ you can print the complete table. Industrial HiVision creates a temporary PDF file of the content of the list and opens this PDF file in the PDF display program, e.g. Acrobat Reader, that is installed on your management station.

With “Reload“ you get Industrial HiVision to update the values in the tables of this dialog.

With “Reset“ you get Industrial HiVision to reset the table values to “0”.

8.3.4 Filter Events for Object

With “Filter Events for Object“, you filter the events list based on the GUI object selected. You have the possibility to filter events with these types of objects:

- devices
- connections
- ports
- device properties

To filter events for object, proceed as follows:

☐ Select the number of necessary objects, on the tab or tree view. When you select at least one object, the “Filter Events for Object“ button becomes active.

☐ Click the “Filter Events for Object“ button.

Figure 72: List generated with the "Filter Events for Objects" function

The event list displays the object-based filtered events. The “Filter“ section on the event list info-bar displays information about the objects used for filtering. Here are a few scenarios:
When you filter events based on a connection between two devices, the “Filter“ section displays this information:

- IP addresses and labels, if the devices are renamed, of the connected devices, in the “Source“ column
- Port number and label, in the “Component“ column
- Component path, if the port is part of a WLAN interface or a module, in the “Component“ column.

When you filter events based on folders, the “Filter“ section displays this information:

- IP addresses and labels, if the devices are renamed, of the devices in the folder, in the “Source“ column.

Note: If you rename the property of a device, Industrial HiVision will search only for the new label. The rule does not apply to the ports.

8.3.5 Back

You use “Back“ to return to the previous view of the detail display frame.

8.3.6 Forward

You use “Forward“ to go to the next view of the detail display frame.

8.3.7 Up

You use “Up“ to go to the next highest level of the detail display frame.

8.3.8 Home View

The “Home View“ button allows you to return the window size and detail view parameters to the settings that you defined with the “Set Home View Settings“ button.

The following parameters are permanent default settings:
- VLAN “All“
- Event Filter “Last 24 Hours Events“
- Tab view “Map“

For an example of the function proceed as follows:
- ☐ Click the “Home View“ button.
- ☐ Note the parameter settings and window size.
- ☐ Specify the VLAN to monitor VLAN 1 only.
- ☐ Specify the window size as full screen.
- ☐ Select a different folder in the menu tree.
- ☐ Select a device in the “List“ tab.
- ☐ Filter the events for “Unacknowledged Warnings & Errors“.

Industrial HiVision now displays the events for the selected settings in the full screen mode. Industrial HiVision also displays the devices that are members in VLAN 1 with the status color for each device. To reset the display to the previously save configuration, click the “Home View“ button.

8.3.9 Set Home View Settings

The “Set Home View Settings“ function allows you specify the window size and content of the detail view that Industrial HiVision displays when you click the “Home View“ button.

For an example of the function proceed as follows:

☐ Verify that the “Edit Mode“ is active.

☐ Specify the view as you wish.
Industrial HiVision allows you to save the following settings:
- Specify a different folder in the menu tree.
- Specify a different screen size.
- Specify either the maximize or normal view.

☐ Click the `View > Set Home View Settings` function.

You can also specify the settings in the `Configuration > Preferences >` Display `> Appearance > Home View Settings > Home Folder` list (see on page 363 “Appearance”).

8.3.10 Geographical Location View

Industrial HiVision allows you to display the location of a device on a map.

☐ Right-click on a device in the detail view and select “Geographical Location View“.

If you have met the following conditions, Industrial HiVision shows you the location of the device on a map.

- The coordinates are entered in the “Location Coordinates“ property of the device.
  See “Properties of a component detail” on page 285.
- Under `Configuration > Preferences > Advanced > External Applications`, the map display application for the URL is entered under “Geographical Location View“.
  See “External Applications” on page 393.

8.3.11 Zoom

Use “Zoom“ to increase the size of the display in the detail frame in steps of 10 %.

8.4 Configuration

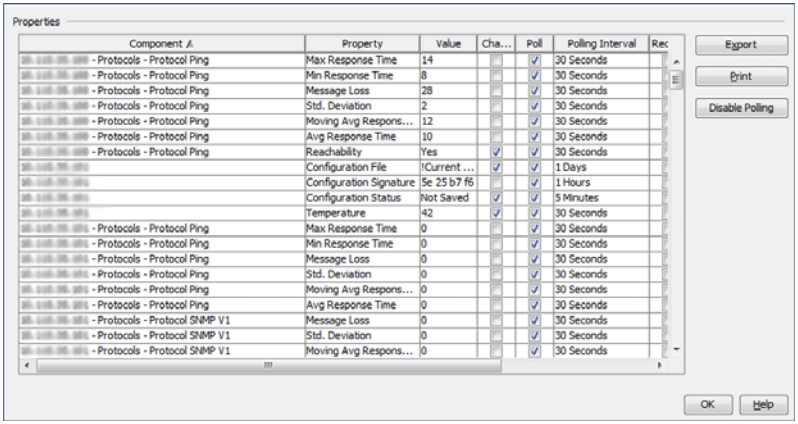
8.4.1 Monitor

The “Monitor“ dialog lists in a table the monitoring functions for the components currently being monitored:

- Property
- Value of the property
- Take the value from an alarm message (trap) relating to this property
- Query the value of this property periodically from the device
- Query interval
- Record history for this property
- Size of the Ring memory for the history recording (number of entries)
- Derive status of property from the value of the property
- Propagate status to the next highest level

Double-click on a row in the table to edit the status configuration of the property.

Note: Before you click the “Disable Polling“ button save your project See “Save” on page 259. The button disables polling for the current properties and deletes the list. The button also deactivates the default polling function in the dialog `Preferences > Default Polling`.



Component	Property	Value	Cha...	Poll	Polling Interval	Rec
[redacted] - Protocols - Protocol Ping	Max Response Time	14		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Min Response Time	8		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Message Loss	28		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Std. Deviation	2		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Moving Avg Respons...	12		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Avg Response Time	10		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Reachability	Yes	✓	✓	30 Seconds	
[redacted]	Configuration File	!Current ...	✓	✓	1 Days	
[redacted]	Configuration Signature	5e 25 b7 f6		✓	1 Hours	
[redacted]	Configuration Status	Not Saved	✓	✓	5 Minutes	
[redacted]	Temperature	42	✓	✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Max Response Time	0		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Min Response Time	0		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Message Loss	0		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Std. Deviation	0		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Moving Avg Respons...	0		✓	30 Seconds	
[redacted] - Protocols - Protocol Ping	Avg Response Time	0		✓	30 Seconds	
[redacted] - Protocols - Protocol SNMP V1	Message Loss	0		✓	30 Seconds	
[redacted] - Protocols - Protocol SNMP V1	Std. Deviation	0		✓	30 Seconds	
[redacted] - Protocols - Protocol SNMP V1	Moving Avg Respons...	0		✓	30 Seconds	

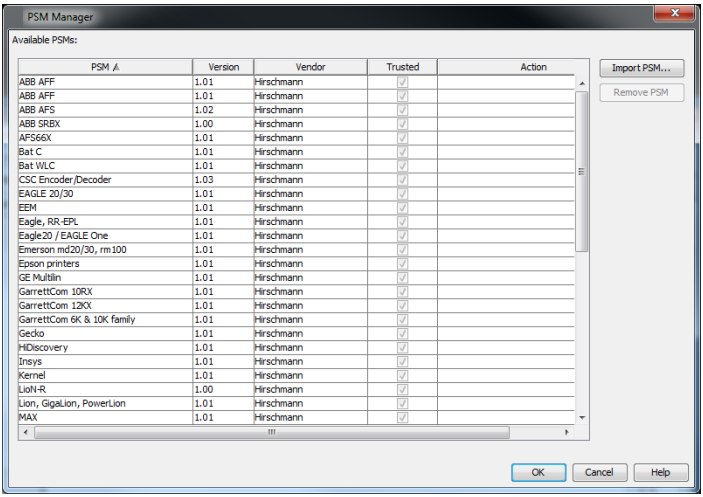
Figure 73: `Configuration > Monitor`

8.4.2 PSM Manager

Product-Specific Modules (PSMs) describe the properties of a device which Industrial HiVision can read for monitoring or write to for configuration.
The PSM Manager gives you the opportunity to update PSMs or import additional PSMs beyond the ones included with delivery and remove them again.

- Industrial HiVision assigns the device class “Switch” to devices for which Industrial HiVision has no PSM.
- During import, Industrial HiVision compares the version of the PSM to be imported with any existing PSM. If the PSM to be imported already exists, Industrial HiVision opens a dialog. The dialog offers you the opportunity to keep or overwrite an existing PSM.

Note: Industrial HiVision accepts the changes made after a restart of the service.



PSM	Version	Vendor	Trusted	Action
ABB AFF	1.01	Hirschmann	✓	
ABB AFF	1.01	Hirschmann	✓	
ABB AFS	1.02	Hirschmann	✓	
ABB SRBX	1.00	Hirschmann	✓	
AFS66X	1.01	Hirschmann	✓	
Bat C	1.01	Hirschmann	✓	
Bat WLC	1.01	Hirschmann	✓	
CSC Encoder/Decoder	1.03	Hirschmann	✓	
EAGLE 20/30	1.01	Hirschmann	✓	
EEM	1.01	Hirschmann	✓	
Eagle, RR-EPL	1.01	Hirschmann	✓	
Eagle20 / EAGLE One	1.01	Hirschmann	✓	
Emerson md20/30, rm100	1.01	Hirschmann	✓	
Epson printers	1.01	Hirschmann	✓	
GE Multilin	1.01	Hirschmann	✓	
GarrettCom 10RX	1.01	Hirschmann	✓	
GarrettCom 12KX	1.01	Hirschmann	✓	
GarrettCom 6K & 10K family	1.01	Hirschmann	✓	
Gecko	1.01	Hirschmann	✓	
HiDiscovery	1.01	Hirschmann	✓	
Insys	1.01	Hirschmann	✓	
Kernel	1.01	Hirschmann	✓	
LioN-R	1.00	Hirschmann	✓	
Lion, GigaLion, PowerLion	1.01	Hirschmann	✓	
MAX	1.01	Hirschmann	✓	

Figure 74: `Configuration > PSM Manager`

8.4.3 Reporting

The reporting function allows you to manage long-term statistics outside the database of the network management system program.

Monitor

This table lists the properties that you selected for monitoring (see on page 295 “Add to reporting”).

- ☐ To change an entry in this table, select the entry and click the “Edit“ button.
- ☐ To delete one or more entries in this table, select the entry or entries and click the “Delete“ button.
  If entries are contained in templates, Industrial HiVision refuses the deletion of these entries.
  Delete these entries in the template table so that you can delete the entries in the monitoring table.
- ☐ To check whether the entries are still valid, as they could have changed during the editing in this dialog, click the “Refresh“ button.

An entry is valid if Industrial HiVision can access and query the component.

Parameter	Meaning
Record	Activate this entry. If you close this dialog, then click “OK” or “Apply” in the “Monitor” dialog, Industrial HiVision starts the recording according to the settings below.
`Recording > Start > Now`	If you close this dialog, then click “OK” or “Apply” in the “Monitor” dialog, Industrial HiVision starts the recording.
`Recording > Start > Time`	If you close this dialog, then click “OK” or “Apply” in the “Monitor” dialog, Industrial HiVision starts the recording at this time.
`Recording > Stop >` Indefinite	After the recording starts, Industrial HiVision continues the recording indefinitely until this entry is deleted or changed.
Polling Interval	Time interval at which Industrial HiVision cyclically queries the value from the device.

Table 33: Editing an entry in the monitoring table

Note: Industrial HiVision can record values as long as Hirschmann Industrial HiVision 8.4 Service is active. When you stop Hirschmann Industrial HiVision 8.4 Service, the recording also stops until Hirschmann Industrial HiVision 8.4 Service is started again.

Templates

This dialog allows you to define the format of reports.

☐ Click the “New“ button to define a new template.
☐ Click the “Edit“ button to change a template.
☐ Click the “Delete“ button to delete one or more templates.
☐ Click the “Display Report“ button to check how a template looks.

Parameter	Meaning
`Report > Name`	Name to identify this template.
`Report > Title`	Header that Industrial HiVision writes above the report.
`Report Type > Type`	Output format of the report. Options: “PDF“, “Excel“
`Report Type > Layout`	Layout of the report. Possible: “Chart“, “Table“
`Report Type > Chart Type`	Options for layout of diagram. Possible: “Line“ (for presenting numeric values), “Bar“
Data	Selection of properties that you previously added to the reporting (see on page 295 “Add to reporting”)

Table 34: Defining a new template

☐ To avoid gaps in line graphs, combine only properties with the same polling intervals.

▶ To improve the appearance of diagrams, Industrial HiVision fills the gaps between the data with repetitions of the latest data. You can recognize the values inserted for filling-out purposes in table reports and Excel files by their grey color.

Scheduling

This dialog allows you to get Industrial HiVision to generate reports for defined time periods.

☐ Click the “New“ button to define a new time period.
☐ Click the “Edit“ button to change a time period.
☐ Click the “Delete“ button to delete one or more time periods.

Industrial HiVision distinguishes between 3 different time period types:

– Absolute start and end times (“Absolute“)
– Absolute start and relative end times (“Relative Stop“)
– Relative start and end times (“Relative“)

▶ Absolute start and end times (“Absolute“)
Industrial HiVision generates a report from the data that lies between the start time and the end time.

Parameter	Meaning
Name	Industrial HiVision provides a selection of existing templates.
From	The first time this dialog is opened, Industrial HiVision displays the time at which Industrial HiVision began recording the data for the selected template. If the report to be generated should start with data from a later point in time, you enter this time here. Possible: Point in time after recording has started and before report generation.
Until	End time of the reporting period. Possible: Point in time after the start time.

Table 35: Scheduling with absolute start and end times

▶ Absolute start and relative end times (“Relative Stop“)
Industrial HiVision generates several reports.
The report period begins at the same start time in each case.
The report period ends at a later time in each case and thus comprises increasingly large periods.

Parameter	Meaning
Begin of report period	The first time this dialog is opened, Industrial HiVision displays the time at which Industrial HiVision began recording the data for the selected template. If the report to be generated should start with data from a later point in time, you enter this time here. Possible: Point in time after recording has started and before report generation.
Offset to execution	Designates the relative end of the data to be included in the report. The relative end of the data to be included in the report relates to the time at which the report was generated. The offset to execution is the amount of time between the relative end of the data to be included in the report and the time at which the report is generated. Possible: Amount of time between the start of recording and the first report generation.

Table 36: Scheduling with absolute start and relative stop times

Parameter	Meaning
First Execution	Time at which Industrial HiVision is to generate the first report.
Schedule every	Amount of time between the generation of a report and the generation of the following report.

Table 36: Scheduling with absolute start and relative stop times

▶ Relative start and stop times (“Relative“)
Industrial HiVision generates several reports.
Each report starts after the end of the preceding report.
The reports contain data from successive periods of equal length.

Parameter	Meaning
Duration	With the duration you set the relative start of the data to be included in the report. Possible: Period smaller than the repetition interval minus the offset between successive executions
Offset to execution	Designates the relative end of the data to be included in the report. The relative end of the data to be included in the report relates to the time at which the report was generated. The offset to execution is the amount of time between the relative end of the data to be included in the report and the time at which the report is generated. Possible: Amount of time between the start of recording and the first report generation.
First Execution	Time at which Industrial HiVision is to generate the first report.
Schedule every	Amount of time between the generation of a report and the generation of the following report.

Table 37: Scheduling with relative start and stop times

Generated reports

This dialog lists the generated reports. Industrial HiVision stores the generated reports in the installation directory in the directory `\var\report_files`.

- ☐ To display a report, select the report and click the “View“ button.
- ☐ To save a report, select the report and click the “Save“ button.
- ☐ To delete one or more reports, select the reports and click the “Delete“ button.
- ☐ To refresh the list, click the “Refresh“ button. After refreshing, Industrial HiVision adds to the list those reports generated since the last refresh.

Industrial HiVision displays the path where Industrial HiVision stores the reports below the table. For remote connections, the specified path refers to the file system on which Hirschmann Industrial HiVision 8.4 Service is running.

The data recorded by the reporting function are snapshots of a moment in time. They represent the value of a property as saved by Industrial HiVision at a particular point in time. Individual values have no bearing on the values from other points in time.

8.4.4 Export to InfluxDB®

The “Export to InfluxDB®“ dialog lets you configure the InfluxDB® server export policy.
The “Categories“ table contains the properties that Industrial HiVision can export to the InfluxDB® server. These properties are classified in different categories.
To select the desired categories of properties, perform the following steps:

☐ Mark the checkboxes related to the desired categories in the “Export“ column.
Default setting: `unmarked`

Note: You can only select a category of properties, and not an individual property to be exported.

☐ To accept the changes and close the window, click the “OK“ button.

Note: When you click the “OK“ button, Industrial HiVision starts the data export to InfluxDB® independent of the export interval you set previously.

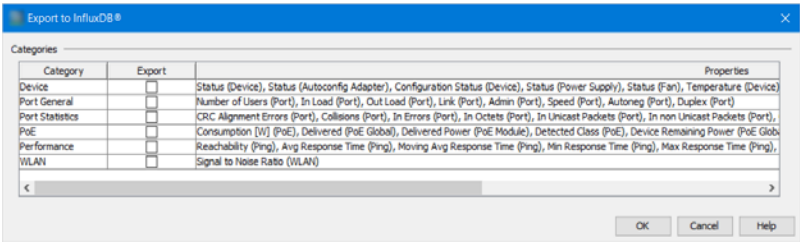


Figure 75: `Configuration > Export to InfluxDB®`

8.4.5 Scheduler

The “Scheduler“ dialog offers the possibility of having repeating tasks of Industrial HiVision carried out automatically.

Task

This table shows you already defined tasks that Industrial HiVision carries out according to the stored schedule.

☐ To define a new task, click the “New“ button.
☐ To change a task, click the “Edit“ button.
☐ To delete one or more tasks, click the “Delete“ button.

Parameter	Meaning
Task Name	Any name to identify this task.
Device	Selection of the device on which Industrial HiVision will run the task.
Task Type	Industrial HiVision makes the following types of tasks available: ▶ “Standard“ ▶ “Advanced“ ▶ “Save Device Configuration“ ▶ “Save Project“ Depending on the selection, the subsequent part of this dialog changes.

Table 38: Defining new tasks

Parameter	Meaning
Standard	Standard belongs to task type SNMP action. As SNMP actions, Industrial HiVision offers the following actions: – Switching a port on/off – Switching the PoE voltage of a port on/off After you have selected the action, the table below provides the port selection of the device and the corresponding parameter (On/Off).
Advanced	Advanced belongs to the task type script action. As script actions, Industrial HiVision offers the following actions: – Cisco: show running config – Cisco: show running config all – HiOS: show running config – HiOS: show running config all Under Executable you have the option to use the built-in Telnet client for executing the action, or you can select your own program with parameter transfer.
Save Device Configuration	The option allows you to schedule saving device configurations. You can select multiple devices, then specify the path and rules for saving the files.
Save Project	Use the option to schedule a task to save the project database to a location of your chose. The database contains the following device information: – The location of the devices as displayed in the “Map“ tab – The device connections as displayed in the “Map“ tab – The device credentials – The Industrial HiVision device status configuration

Table 38: Defining new tasks

Scripts

The “Scripts“ dialog offers you the opportunity to add your own scripts to the selection of scripted actions.

☐ To define a new script, click the “New“ button.
☐ To change or import a script, click the “Edit“ button.
☐ To delete one or more scripts, click the “Delete“ button.
☐ To duplicate a script, click the “Duplicate“ button.

Parameter	Meaning
Script Name	Any name to identify this script.
Content	Import script or enter script as text.

Table 39: Define new scripts

Note: Industrial HiVision uses Telnet or SSH sessions to run scripts on a device. After a successful login, the session waits for a specific output from the device. Wireless devices do not send the output which results in a timeout. To work around this behavior, you can schedule Industrial HiVision to open a command-line tool for example, Putty and then run your script.

Schedules

The “Schedules“ dialog offers you the opportunity to define a schedule for carrying out a task.

☐ To define a new task, click the “New“ button.
☐ To change a task, click the “Edit“ button.
☐ To delete one or more tasks, click the “Delete“ button.

Parameter	Meaning
Task Name	List of defined tasks for selection in the “Tasks“ dialog.
Execution	Type of execution: once or several times with entry of the start date and repeat interval for repeated execution.
Repetition	Entry of the repetition conditions for repeated execution: Number of repetitions, end date.

Table 40: Define a new schedule

Note: You can only schedule 1 task for a device.

Results

The “Results“ table lists the results of the executed tasks.

☐ To view a marked result, click the “View“ button.
☐ To delete a result, click the “Delete“ button.
☐ To refresh the results list, click the “Refresh“ button.

Example of Scheduling an Event for a Single Device

This example demonstrates how to schedule an event to save a device configuration. If Industrial HiVision detects an error during the configuration saving process, then the detected error is entered in a log.

Industrial HiVision saves the log file in the following location: `\log\services\HiVisionKernelDb.0.stderr.log`.

Note: If the “Save Device Configuration“ task fails during device configuration retrieval, then proceed as follows:
- ☐ Verify that Industrial HiVision can reach the selected device.
- ☐ Verify that the protocols, SNMP and HTTP or HTTPS, are active on the device.
- ☐ Verify that Industrial HiVision has administration rights for SNMP, HTTP, and HTTPS on the selected device.
- ☐ Verify that the selected device supports the “Save configuration to PC”, or “Export configuration” functions.

To schedule an event in Industrial HiVision for saving the configuration file for a single device, proceed as follows:
- ☐ Open Industrial HiVision.
- ☐ Verify that the “Edit Mode“ is active.
- ☐ To open the “Scheduler“ dialog, click `Configuration > Scheduler`.

The following work steps pertain to the “Tasks“ tab:
- ☐ To open the “New Entry“ dialog, click the “New“ button.
- ☐ Enter a name that describes the event for example, “Save Device Configuration“.
- ☐ Select a device from the “Device“ list.
- ☐ In the “Task Type“ field, select the “Save Device Configuration“ option from the drop down list.
- ☐ When the selected device supports the function the fields in the “Save Config“ frame are active. In the “Save Config“ frame, enter the appropriate information in the following fields:
  - In the “Destination folder“, enter or browse to the location where you wish to save the configuration.
  - Industrial HiVision enters `IP_Address` in the “File name“ field.
  - The “On multiple task execution“ field allows you to select how Industrial HiVision handles multiple files. To maintain a history of the configuration changes, select “Add timestamp to target file name“.

- ☐ Industrial HiVision keeps a record of detected failed tasks. If you wish to also keep a log entry for every successful task, then unmark the checkbox “Suppress report creation for successfully completed task“.
- ☐ Click the “OK“ button.

The following work steps pertain to the “Schedules“ tab:

- ☐ To open the “New Entry“ dialog, click the “New“ button.
- ☐ Open the “Name“ drop down list, in the “Task“ field.
- ☐ Select the task created in the previous work steps.
- ☐ To have Industrial HiVision save the device configuration multiple times, in the “Execution“ field, select “Multiple execution“.
- ☐ You can leave the current date and time in the “Start Date“ field (default setting).
- ☐ Change the “Interval“ setting to `1` and the units to “Days“.
- ☐ To have Industrial HiVision save the device configuration every day until you change this setting, in the “Repetition“ field, select the “Repeat indefinitely“ option (default setting).
- ☐ Click the “OK“ button.

Example of Scheduling an Event for Multiple Devices

You can also schedule an event to save the configuration of multiple devices. If Industrial HiVision detects an error during the configuration saving process, then the detected error is entered in a log.

The log file is in the following location:
`\log\services\HiVisionKernelDb.0.stderr.log`.

Note: If the “Save Device Configuration“ task fails during device configuration retrieval, then proceed as follows:

- ☐ Verify that Industrial HiVision can reach the selected device.
- ☐ Verify that the protocols, SNMP and HTTP or HTTPS, are active on the device.
- ☐ Verify that Industrial HiVision has administration rights for SNMP, HTTP, and HTTPS on the selected device.
- ☐ Verify that the selected device supports the “Save configuration to PC”, or “Export configuration” functions.

To schedule an event in Industrial HiVision for saving the configuration file for multiple devices, proceed as follows:

☐ Open Industrial HiVision.

☐ Verify that the “Edit Mode“ is active.
☐ In the “Map“ tab, select the devices that you want to save the configuration. You can also select devices from the “List“, “Devices“, and “Security“ tabs.
☐ Right-click a device.
☐ In the drop down menu, select the “Schedule Saving Device Configuration“ option. The “Schedule Saving Device Configuration“ dialog opens. In the “Device“ field, Industrial HiVision highlights the devices that you selected in the “Map“ tab.
☐ In the “Save Config“ field, enter the appropriate information in the following fields:
  – In the “Destination folder“, enter or browse to the location in which you wish to save the configuration.
  – Industrial HiVision enters `IP_Address` in the “File name“ field.
  – The “On multiple task execution“ field allows you to select how Industrial HiVision handles multiple files. To maintain a history of the configuration changes, select “Add timestamp to target file name“.
☐ Industrial HiVision keeps a record of detected failed tasks. If you wish to also keep a log entry for every successful task, then unmark the checkbox “Suppress report creation for successfully completed task“.
☐ The “Reporting“ field also contains the “Schedule Execution“ function. The function allows you to schedule a save configuration file event. When the function is active, Industrial HiVision saves the configuration of the devices in a single file.
☐ To have Industrial HiVision save the device configuration multiple times, in the “Execution“ field, select “Multiple execution“.
☐ You can leave the current date and time in the “Start Date“ field (default setting).
☐ Change the “Interval“ setting to `1` and the units to “Days“.
☐ Verify that the “1 minute delay between start of tasks“ function is active. The function allows Industrial HiVision to add a delay between saving the configuration of the devices.
☐ To have Industrial HiVision save the device configuration every day until you change this setting, in the “Repetition“ field, select the “Repeat indefinitely“ option (default setting).
☐ Click the “OK“ button.

Example of Scheduling an Event for Save Project

The “Save Project“ task gives you the opportunity to schedule a backup of your project database.

Note: The backup files made with the “Save Project“ task are version specific.

To schedule an event in Industrial HiVision to save a backup of your project database, proceed as follows:

☐ Verify that the “Edit Mode“ is active.
☐ To open the “Scheduler“ dialog, click `Configuration > Scheduler`.

The following work steps pertain to the “Tasks“ tab:

☐ To open the “New Entry“ dialog, click the “New“ button.
☐ Enter a name that describes the event for example, “Save Project“.
☐ In the “Task Type“ field, select the “Save Project“ option from the drop down list.
☐ In the “Save Project File“ field, enter the following information:
  – Enter a path to the location where you wish to save the file in the “Destination folder“ field.
  – Enter a name that describes the file in the “File name“ field.
  – The work steps that follow make multiple files in the same location. Use the “On multiple task execution“ drop down list to select either “Overwrite target file“, or “Add timestamp to target file name“.
☐ Industrial HiVision keeps a log entry of detected failed tasks. If you wish to also keep a log entry for every successful task, then unmark the checkbox “Suppress report creation for successfully completed task“.
☐ Click the “OK“ button.

The following work steps pertain to the “Schedules“ tab:

☐ To open the “New Entry“ dialog, click the “New“ button.
☐ In the “Task“ field, open the “Name“ drop down list.
☐ Select the task made in the previous work steps.
☐ To have Industrial HiVision save the project database multiple times, in the “Execution“ field, select “Multiple execution“.
☐ You can leave the current date and time in the “Start Date“ field (default setting).
☐ Change the “Interval“ setting to `1` and the units to “Weeks“. The minimum value for the “Save Project“ task is `1` hour.

- ☐ To have Industrial HiVision save the project every week until you change this setting, in the “Repetition“ field, select the “Repeat indefinitely“ option (default setting).
- ☐ Click the “OK“ button.

8.4.6 Preferences

The “Preferences“ window enables you to enter basic program settings. These settings relate to monitoring functions, management functions, display options, access rights and others.

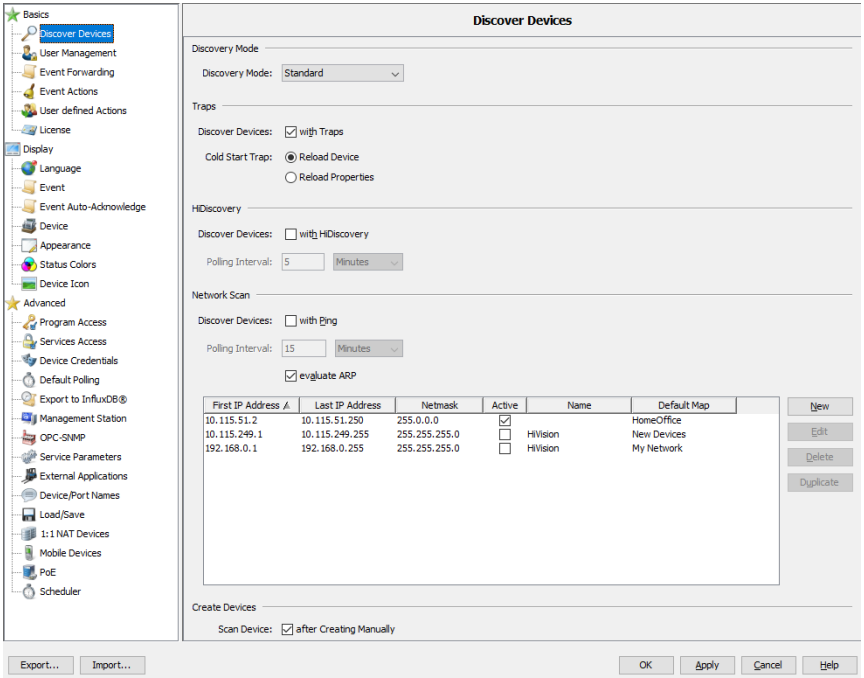


Figure 76: `Configuration > Preferences`

- ☐ To accept changes in the dialogs and close the window, click the “OK“ button.
- ☐ To accept changes in the dialogs before you switch to another dialog, click the “Apply“ button.
- ☐ To close the window, click the “Cancel“ button. Changes not written using the “Apply“ button are lost.

Importing and Exporting the Preference Settings

Industrial HiVision allows you to import and export the preference parameter settings. Industrial HiVision exports the preference file with a .prefs extension. You can use the file for a backup or importing the preference settings to a new management station. The application restarts after importing preferences settings.

For security reasons, Industrial HiVision excludes the following parameters from the export file:

- Passwords
- Password dependent preferences
- User Management settings
- Licenses
- Device Credentials
- Mobile Device Credentials

Note: Industrial HiVision displays an information message allowing you to apply the settings before you export the preference file.

[Basics]

Discovering devices

You use this dialog to specify which way Industrial HiVision should detect the devices in your network structure. Industrial HiVision enters newly detected devices in the default map. If you have not entered an activated default map in the network scan table (see below), then Industrial HiVision displays newly detected devices in the “New Devices“ folder
The search function in the tool bar helps you to find devices already detected.

Industrial HiVision provides the following options for the “Discovery Mode“:

- “Standard“
  Industrial HiVision uses the option you select to detect devices.
- “Monitoring Mode“
  Industrial HiVision exclusively evaluates cold start “Cold Start Trap“ and ARP answers to discover devices.
- “Rogue Device Detection“
  Industrial HiVision uses the option you select to detect devices and places newly discovered devices in the “Rogue Devices“ folder.

Industrial HiVision provides the following options for discovering devices:

- Detecting devices using traps
- Detecting devices using the HiDiscovery V1 protocol
- Detecting devices using a defined IP address range (“Network Scan“)
- Detecting newly created devices
- Detecting devices using a list

Detecting devices using traps.
After they are switched on, the devices send a switched-on message to the network management station entered in the device.
Then Industrial HiVision reads the properties of the devices:

– Read device again: Industrial HiVision treats the device like a new device and reads in the entire properties and the structure of the device (new/removed model or power unit) again.
– Read properties again: Industrial HiVision reads the known properties in again.

Example: You switch on a device with 2 power supplies for the duration of some maintenance work. How does Industrial HiVision behave after the device is switched on if a voltage supply is missing?
– With the “Reload Device“ setting, Industrial HiVision represents the device with one power unit and the color green.
– With the “Reload Properties“ setting, Industrial HiVision represents the device with two power units, with one power unit in red.

Industrial HiVision displays the newly detected devices in the corresponding folder.
This method of detecting devices is suitable for use during ongoing monitoring in networks where you need to manage the bandwidth.

Detecting devices using the HiDiscovery V1 protocol
The HiDiscovery V1 protocol uses the MAC address to communicate with Hirschmann devices in the subnetwork on which the HiDiscovery V1 protocol is active.
You can find information as to which devices support HiDiscovery V1 in the user manual of the device.
This method enables you to detect devices in your network to which you have not yet assigned a valid IP address.
Industrial HiVision displays the devices in the corresponding folder.
This method is suitable for when you start up a newly installed network and want to assign the IP address to the new devices. Select this method for a limited time in order to spare your network an unnecessary network load.

☐ For the polling interval you enter the desired value in the “Polling Interval“ field and select the units for this value – seconds, minutes, hours or days – in the pull-down list.
Default setting: 5 minutes.
Keep in mind how this affects your system resources (see on page 228 “Effect on system resources”).

Detecting devices using a defined IP address range
Using the “Network Scan“ function, Industrial HiVision periodically sends ping requests to the devices with an IP address in the defined IP address ranges and displays the new devices that respond in the destination folder entered.
A firewall blocks the ping requests.

In order for Industrial HiVision to be able to discover devices behind a transparent firewall, mark the “evaluate ARP“ checkbox. A transparent firewall forwards an ARP response. If the ping response does not come within a predetermined time, Industrial HiVision evaluates the ARP response.
The “Network Scan“ method is suitable for monitoring a running network. Adapt the frequency of the requests to the bandwidth of your network.

☐ For the request interval you enter the desired value in the “Polling Interval“ field and select the units for this value – seconds, minutes, hours or days – in the pull-down list.
Default setting: 15 minutes.
Keep in mind how this affects your system resources (see on page 228 “Effect on system resources”).

☐ To enter an IP address range, click the “New“ button. Entering the IP address range includes:
- the first IP address of the query range
- the last IP address of the query range
- the related network mask
- the activation/deactivation of this range for the query
- the name you want to give the range
- the default map in which you want Industrial HiVision to display a newly detected device.
  You can enter overlapping IP address ranges, then Industrial HiVision enters a copy of a device in each of the relevant folders.

The table displays the IP address ranges already created.

☐ To edit an IP address range, select a row in the table and click on the “Edit“ button.

☐ To delete a row from the table, select the row in the table and click the “Delete“ button.

☐ To duplicate an IP address range so that you can then modify the copy, select a row in the table and click the “Duplicate“ button.

Detecting newly created devices
Here you enter the initial setting for the dialog for entering the IP address which appears when you create a new device (see on page 132 “Creating new devices”).

Discover device from a list of IP addresses
Industrial HiVision allows you to scan IP addresses using a text or an Microsoft Excel csv file. The “Create Devices from List“ dialog allows you to search for and upload the file to Industrial HiVision. If a device in the list is unreachable, then Industrial HiVision displays the device in the topology map as a generic device. (see on page 257 “Devices from List”)

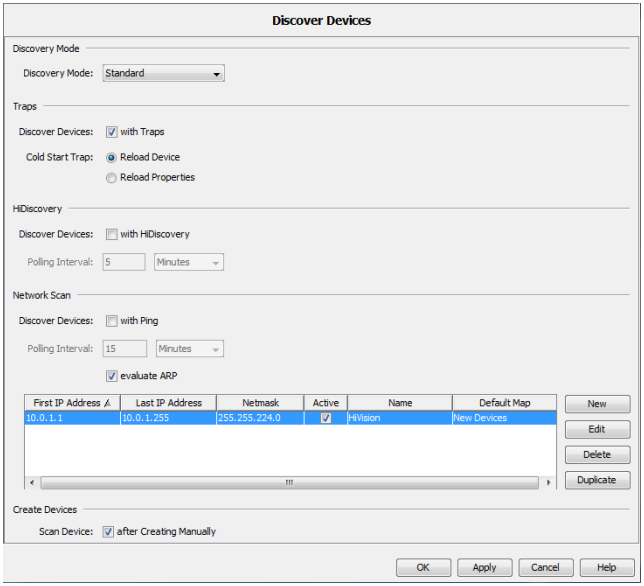
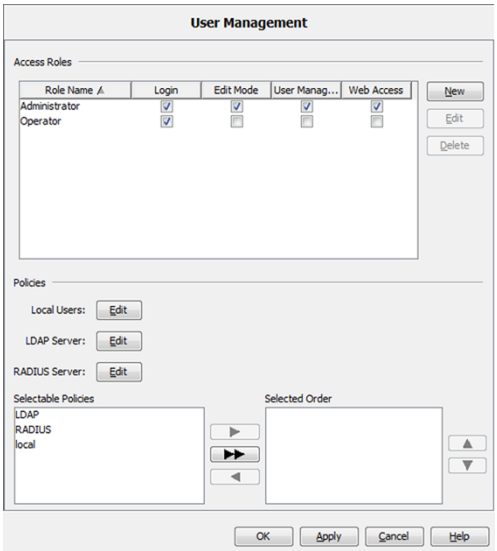


Figure 77: `Configuration > Preferences > Basics > Discover Devices`

User Management

User management is based on a role model.
You specify role names in the “Access Roles“ frame. You assign these roles the permissions of this role using the assignment of the access authorizations. You can naturally assign the available rights to an administrator, whereas an observer can only login, they cannot receive rights with which they are able to change anything.
Industrial HiVision provides the following permissions:

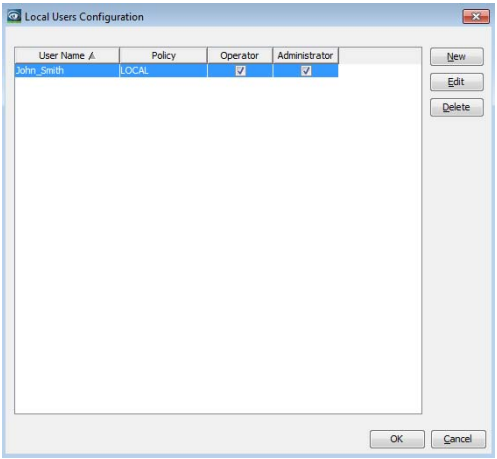
- “Login“
- “Edit Mode“
- “User Management“
- “Web Access“



Once you have made the access roles, create the users and allocate them one or more of the roles made above. This assignment depends on the method Industrial HiVision is supposed to use to verify a user's authorization.

Industrial HiVision uses three “Policies“ to verify the authorization of a user:

– “Local Users“, local user name with role assignment.
  Industrial HiVision transfers the role names created above into the user table header. Thus allowing you to easily assign roles to a user name.



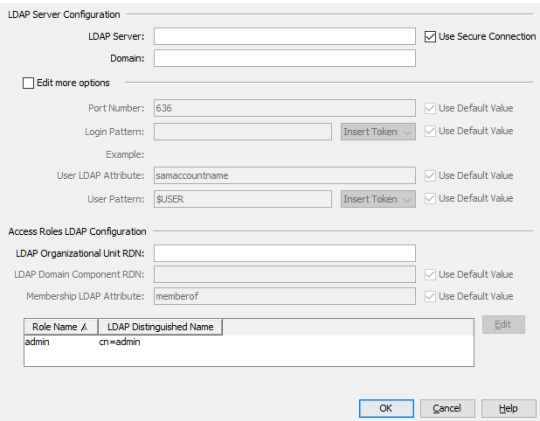
– The Lightweight Directory Access Protocol (LDAP) lets you authenticate and authorize the users at a central point in the network. Give the administrator of your LDAP server information about the Industrial HiVision users and their access roles. The necessary information includes the following user data:
  – “User Name“
  – “Password“
  – “Access Roles“

  The `Preferences > Basics > User Management > LDAP Server Configuration` dialog contains an “LDAP Server“ field. Specify the IP address or DNS name in the “LDAP Server“ field. The field lets you specify more than one “LDAP Server“. Industrial HiVision sends the log on data to the first authentication server. If the first server does not

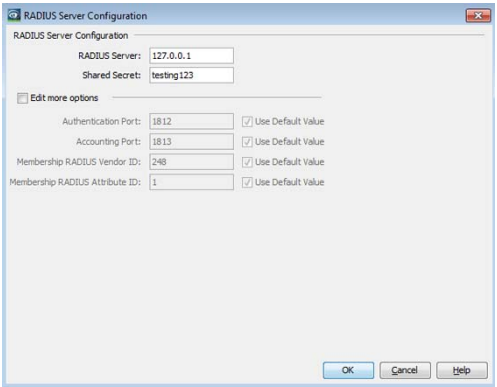
respond, then Industrial HiVision attempts to contact the other servers, one after the other, until it receives an answer. To specify more than one server, separate the IP addresses or host names with either a comma or a space. For example, 192.168.10.10 LDAP_Server_1 or 192.168.10.10,LDAP_Server_1.

The “LDAP Server Configuration“ dialog also contains the “Use Secure Connection“ checkbox. When using an LDAP server to authorize an Industrial HiVision user, the checkbox lets you choose between a secure or an unsecure connection.

- When you mark the checkbox, the user authenticates using an SSL connection to the server. The data exchanged between Industrial HiVision and the LDAP sever is encrypted.
- When the checkbox is unmarked, the connection is unsecure and data such as passwords are sent as plain text.



– “RADIUS Server“, central user control using the Remote Authentication Dial-In User Services.
  Give your RADIUS server administrator the following user data to enter into the RADIUS server:
  – “User Name“
  – “Password“
  – “Access Roles“



In the “Selected Order“ field you can specify, which methods Industrial HiVision uses to verify the authorization of a user. As long as the “Selected Order“ field is blank, the “User Management“ function is disabled and Industrial HiVision is freely accessible.
Industrial HiVision uses the first entry in this field for an authorization check. If the test for the 1st method is unsuccessful, Industrial HiVision verifies the authorization according to the 2nd method. If Industrial HiVision cannot verify any of the authorization checks successfully, Industrial HiVision denies access.

Event Forwarding

This dialog gives you the option of making settings for forwarding events to a syslog server.
With “Forward events to syslog server“ you enable/disable the event forwarding function globally. When event forwarding is enabled, Industrial HiVision sends a syslog message to the syslog server entered in this dialog as soon as an event occurs.
With “Forward internal events“ for example, “Industrial HiVision Started“, Industrial HiVision also sends syslog messages for Industrial HiVision internal events.
With “Forward events of all devices“, Industrial HiVision sends syslog messages to the syslog server for every available device. When you mark the “Forward events of all devices“ checkbox, the “Forward events for devices“ table is hidden.
With “Event Type“, you specify at what evaluation level of an event Industrial HiVision sends a syslog message.
In the “Forward events for devices“ table, you enter the device whose events should lead to a syslog message.
In the “Syslog servers“ table, you enter the data of the syslog server to which Industrial HiVision sends syslog messages.
Industrial HiVision sets the communication with the syslog server through the following transport protocols:

- User Datagram Protocol (UDP)
- Transport Layer Security (TLS)

When the TLS protocol is used, Industrial HiVision accepts the certificate of the syslog server without additional validation.
In some cases, a syslog server can require a two-step validation process which includes the validation of the client certificate. If a syslog server requires a two-step validation process, then the communication with the syslog server is not possible.

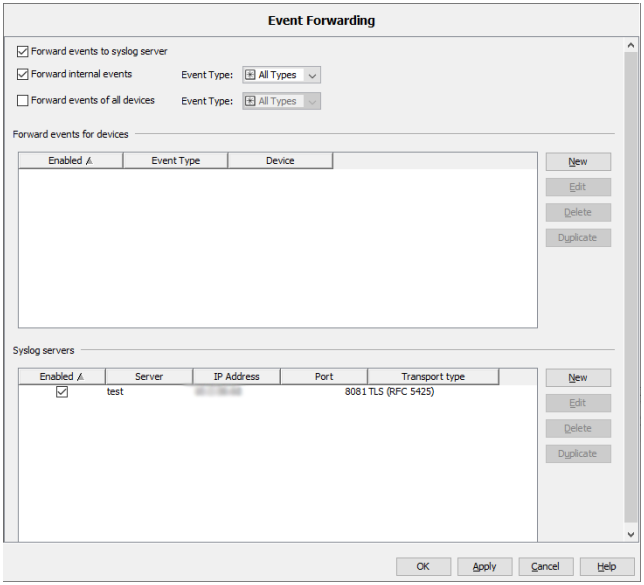


Figure 78: `Configuration > Preferences > Basics > Event Forwarding`

Event Actions

In this dialog you define the actions you want Industrial HiVision to perform when particular events occur.

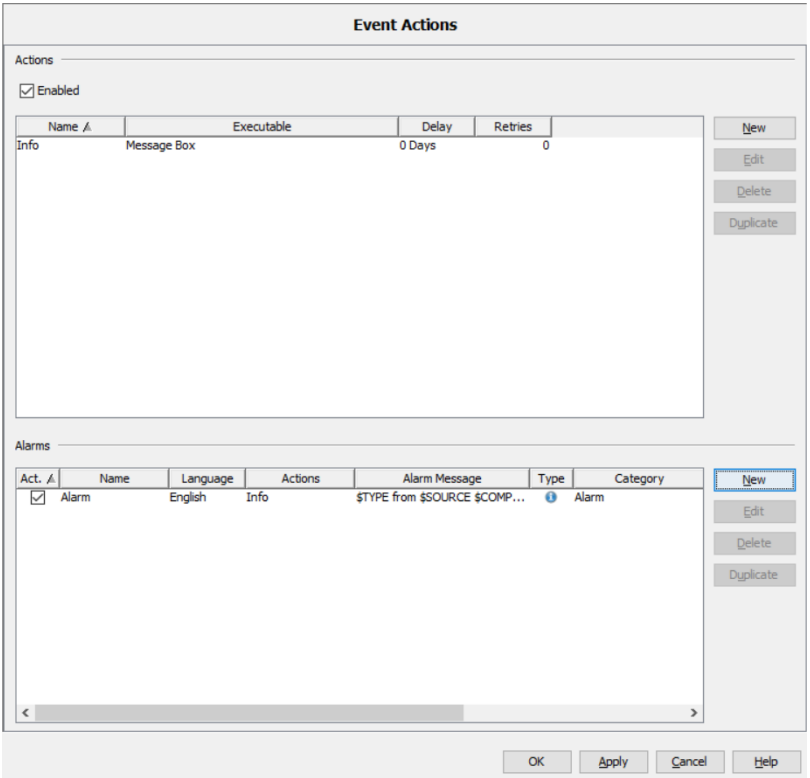


Figure 79: `Configuration > Preferences > Basics > Event Actions`

The “Actions“ frame describes what Industrial HiVision can carry out:

- Open the message window on the screen
- Send an SMS
- Play Sound
- Play Notification

- Send an e-mail
- Execute a program (see note in “Installation under Windows”). In the figure below (see figure 80), you will find the user program “siren.exe” as an example.

☐ To enable the “Event Actions“ function, mark the “Enabled“ checkbox. When enabled, Industrial HiVision completes the actions defined in the “Actions“ table.
The checkbox is enabled in the following situations:
- You open a new project.
- You open an existing project that has no event actions defined.
- You load the backup of an existing project that has no event actions defined.

The checkbox is disabled in the following situations:
- You open an existing project that has minimum `1` event action defined.
- You load the backup of an existing project that has minimum `1` event action defined.

☐ To specify the action you want to assign to the events, click the “New“ button.
For actions that might not execute on the first try, such as a busy line when sending an SMS, Industrial HiVision gives you the option of repeating the action.

The “New Entry“ dialog contains the “Test Action“ button. The “Test Action“ button gives you the possibility to test your configuration.

The “Send SMS“ action requires
– that your network management station is connected to the telephone network for example, using a modem and
– that the SMS program is configured correctly.

Enter the telephone number of the recipient under “Recipient“.
If you enter the telephone number of your modem as the “Sender“, then Industrial HiVision sends it with the message. You can thus recognize Industrial HiVision as the sender in the display of your mobile phone.
As the “Service Provider“ you enter the available service which you configured in your SMS program (if available).

Under `Preferences > Advanced > External Applications`, check that the entries for the required external applications are present and that they meet your requirements.

The table displays the actions already created.

- ☐ To edit an action, select a row in the table and click the “Edit“ button.
- ☐ To delete a row from the table, select the row in the table and click the “Delete“ button.
- ☐ To duplicate an action so that you can then modify the copy, select a row in the table and click the“Duplicate“ button.

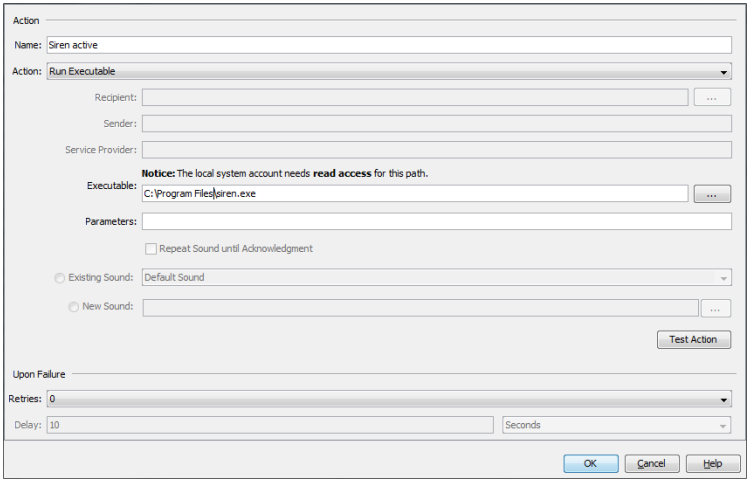


Figure 80: `Configuration > Preferences > Basics > Event Actions > Actions`, *Example for using the action “Execute program” for the user program “siren.exe”*

The “Alarms“ frame offers the possibility to perform an action when certain events occur or in the absence of confirmation of certain events.
Under “Type“, you specify when Industrial HiVision performs the action.
Under “Alarm“, enter any name for the event that is to trigger an action.
Under “Filter“, you define the event that is to trigger the actions selected below. Industrial HiVision allows wildcards for defining the filters.

Designation	Meaning
Type	Selection of the status type (error, warning, ...)
Category	Event of a particular category (status better, new device, ...)
User	Logon name from the network management station
Source	Cause of the event

Table 41: Filter criteria

Designation	Meaning
Component	Component of the cause of the event
Message	Text describing the event

Table 41: Filter criteria

To simplify things, “Import...“ provides you with the events that have already occurred from the list in the event frame.

☐ Select a row and click the “OK“ button.
Industrial HiVision copies the properties of the selected event into the filter frame.

The “Message“ row enables you to enter the message text for actions. You can use the filter keywords with a “$” sign as a prefix to a variable entry. Enter the keywords in upper-case characters. For example, if you enter “$TIME” in the message, Industrial HiVision enters the time the event occurred in the message. The keywords that Industrial HiVision provides you with are listed in the “Message“ row of the bubble help.

The following list contains words that are reserved for Industrial HiVision internal usage. If you type any of the words in the “Message“ field, then Industrial HiVision opens an error message. The words by themselves or as part of a longer word are prohibited. The reserved words apply only to the English and German graphical user interfaces (GUI).

List of reserved English words:
- Alarm
- alarm
- Alarms
- alarms
- Actions
- actions
- Message
- message
- Critical
- critical

List of reserved German words:
- Alarm
- Alarme
- Alarms

- Nachricht
- Kritisch

The “Time“ frame offers you the opportunity to set a time period during which Industrial HiVision responds to an event with an action.

In the “Actions“ frame, you have the option of selecting one or more of the actions already created. Industrial HiVision executes these actions when the event defined above occurs or when confirmation of the event is absent within the time specified in “Type“.

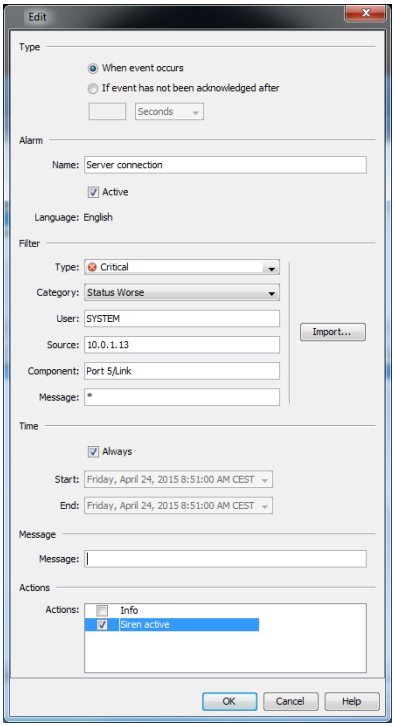


Figure 81: `Configuration > Preferences > Basics > Event Actions > Alarms >` *Message*

The following example configuration describes how you configure Industrial HiVision to send an email for an event. In this example you configure the following `Configuration > Preferences` dialogs:

- The `Advanced > External Applications` dialog
- The `Basics > Event Actions > Actions > New > New Entry` dialog
- The `Basics > Event Actions > Alarms > New > New Entry` dialog

In order for Industrial HiVision to send emails, it connects to an email server host. Get the following server information from your email server administrator:

- Host name
- The name of the email account which Industrial HiVision uses to send the email. Make the name of the email sender easily identifiable as Industrial HiVision.
- Is it necessary for Industrial HiVision to log on to the server? If so, then the following information is necessary:
  - What type of connection does the server use. Industrial HiVision connects using the following protocols:
    Normal, unsecure communication
    STARTTLS, begins a TLS session
    SSL, uses the Secure Socket Layer protocol
  - What TCP port does the server use.
  - The user name and password used for authentication.

The following items can prevent Industrial HiVision from sending an email:

- Firewall settings
- Virus protection settings

To configure Industrial HiVision to connect to an email server, proceed as follows:

☐ Open the `Advanced > External Applications` dialog.
☐ In the `Mail Server > SMTP Mail Host` field, type in the name of the email server for example, `smtp2.xxxx.com`.
☐ In the “Sender Address“ field, type in the email account from which Industrial HiVision sends the email, for example,`Industrial HiVision@xxxx.com`.
☐ Click the “OK“ button.

To send an email to the person responsible for the task, proceed as follows:

☐ Open the `Basics > Event Actions` dialog.
☐ To make an entry in the “Actions“ table, click the `Actions > New` button.

- ☐ In the `Edit > Action > Name` field, type in the value `Send_email_to_admin`.
- ☐ In the “Action“ drop-down list, select the “Send E-Mail“option.
- ☐ Type in the email address of the person responsible for the task in the “Recipient“ field.
- ☐ Click the “OK“ button.

To configure an event for which Industrial HiVision sends an email, proceed as follows:

- ☐ Open the `Basics > Event Actions` dialog.
- ☐ To make an entry in the “Alarms“ table, click the `Alarms > New` button.
- ☐ In the “Edit“dialog, type in the text that you wish to be displayed on the subject line in the “Name“ field.
- ☐ Type in the event that you wish to send as an email in the “Filter“ frame.
  When Industrial HiVision has an event in the “Event History“ that you wish to send as an email, you can have Industrial HiVision automatically enter values in the “Filter“ frame using the “Import...“ button.
  - Click the “Import...“ button.
  - Select the event from the “Application Events“ tab.
  - Click the “OK“ button.

  You can also generate test events that you can send as an email.
  See “Generate test events” on page 291.
- ☐ Type in the message that you wish to be displayed in the body of the email in the “Message“ field.
  You can type in free text or use tokens. When you hover over the text field Industrial HiVision displays a bubble help containing the tokens that you can use. The tokens represent the columns displayed in the event log. For example, $TYPE = the “Type“column, $MESSAGE = the “Message“ column.
- ☐ Mark the `Send_email_to_admin` checkbox in the “Actions“ table.
- ☐ Click the “OK“ button.

User defined Action

User-configurable actions give you the opportunity of starting actions on other devices from your network management station.

Location	Meaning
Desktop	Industrial HiVision starts the application on the computer on which the Industrial HiVision interface is running. The service can run on another computer. You select “Desktop“ when the application that Industrial HiVision starts expects an interaction. Application example: Starting a Telnet client
Service	Industrial HiVision starts the application on the computer on which the service is running. This selection gives you the option of configuring devices that only permit configuration from the IP address of the network management station. Application example: Configuration scripts which you want to call up from multiple interfaces (and also from applets) or use to run batch files (see “Example of interface”).
Browser	Industrial HiVision starts the application with the URL. Example: To open the graphical user interface of a device in the browser, enter the following value in the “Parameters“ field: `http://10.0.1.13`.

Table 42: Location of execution of a user-defined action

Example of interface: “Call up Telnet client”
You want to use a Telnet client for example, “Putty”, to access a known device such as an EtherNet switch.

- ☐ In the Industrial HiVision menu bar, select `Configuration >` Preferences.
- ☐ In the “Preferences“ dialog, select `Basics > User defined Actions`.
- ☐ To define a new user-configurable action, click the “New“ button.
- ☐ In the “Name“ field enter a name to identify calling up the Telnet client for example, “Manage Switch using Telnet”.
- ☐ In the “Available for“ row, you select the symbol with which you wish to start the action. Industrial HiVision places the action in the drop-down list according to the definition. You can find the action under “Actions“ by right-clicking this symbol.
  - As you want to call the action later at the device level, from the “Available for“ drop-down list, select “Device“.
- ☐ In the “Device Type“ drop-down list, select “All“.

- ☐ You want to start the Telnet client on a computer on which the Industrial HiVision graphical user interface is running. The Telnet client expects an interaction with the administrator of the switch. Therefore you select “Desktop“ as the “Location of Execution“ (see table 42).
- ☐ Enter the path to the application and the name of the application, in the “Application“ text filed. You can also select the application by clicking the “...“ button.
  To select the Telnet client “Putty” application, enter the following for example:
  `C:/Data/Software/putty.exe`.
- ☐ The “Parameters“ text field gives you the option of transferring parameters to the application with tokens. Enter the following in the example:
  – Call up Telnet
  – The token for the IP address of the device
  `$"-telnet $IP_ADDR"`

Example for service: “Enable/disable port”
In a room for visitors you have Ethernet connections. The room can be accessed by anybody. Therefore you would like to enable a port that is connected to this Ethernet connection only when you actually have visitors.

- ☐ To do this, write the following small batch files with the SNMP commands for enabling/disabling the port:

Windows users:
1st batch file: Port-on.bat

```
set IP_ADDR=%1%
set IF_INDEX=%2%
"<installation folder>\bin\SnmpSet.cmd.exe" -c private %IP_ADDR%
1.3.6.1.2.1.2.2.1.7.%IF_INDEX% integer 1
```

2nd batch file: Port-off.bat

```
set IP_ADDR=%1%
set IF_INDEX=%2%
"<installation folder>\bin\SnmpSet.cmd.exe" -c private %IP_ADDR%
1.3.6.1.2.1.2.2.1.7.%IF_INDEX% integer 2
```

Linux users:
1st batch file: Port-on.sh

```
#!/bin/bash
IP_ADDR=$1
IF_INDEX=$2
"<installation folder>/bin/SnmpSet" -c private $IP_ADDR
1.3.6.1.2.1.2.2.1.7.$IF_INDEX integer 1
```

2nd batch file: Port-off.sh

```
#!/bin/bash
```

```
set IP_ADDR=%1%
set IF_INDEX=%2%
"<installation folder>/bin/SnmpSet" -c private $IP_ADDR
1.3.6.1.2.1.2.2.1.7.$IF_INDEX integer 2
```

Mark the file as executable, `Exec-Bit`, with the command: `chmod 700 Port-On.sh`.

- ☐ Save the batch files on your network management station for example, under `C:\Data\PortOnOffBatch`
- ☐ In the Industrial HiVision menu bar, select `Configuration >` Preferences.
- ☐ In the “Preferences“ dialog, select `Basics > User defined Actions`.
- ☐ To define a new user-configurable action, click the “New“ button.
- ☐ Enter any name for the 1st batch file for example, “Enable visitor port”.

- ☐ In the “Available for“ row, you select the symbol with which you wish to start the action. Industrial HiVision places the action in the drop-down list according to the definition. You can find the action under “Actions“ by right-clicking this symbol.
  - As you want to call the action later at the device level, from the “Available for“ drop-down list, select “Device“.
- ☐ In this example the port for the connection in the visitors room is connected to a RS30 rail switch. Therefore, in the “Device Type“ drop-down list, select “Classic Switch“.
- ☐ You would like to execute the batch files on a computer on which the service of Industrial HiVision is running. Industrial HiVision passes the interface number of the port as a command parameter when calling up the batch file. Then the batch files run automatically. Therefore you select “Service“ as the “Location of Execution“ (see table 42).
- ☐ Enter the path to the application and the name of the application, in the “Application“ text filed. You can also select the application by clicking the “...“ button.
  For our example enter the following,
  “`C:\Data\PortOnOffBatch\Port-on.bat`”
- ☐ The “Parameters“ text field gives you the option of transferring parameters to the application with tokens. For our example enter the following,
  - The token for the IP address of the device
  - The token for the port

  `$IP_ADDR $USER`

  When you enter the value `$USER` in the “Parameters“ text field, Industrial HiVision opens the “User Input Prompt“ text field.

- ☐ The “User Input Prompt“ text field gives you the option to enter instructions in the “User Input“ dialog.
  For our example enter the following, “Enter the Interface Index”.

You can find further function details under “Advanced“:

- ▶ “Token Language“
  Industrial HiVision transfers the token content to the application in this language. This applies to the tokens: “Status (textual)”, “Value” and “Name”.
- ▶ Query password when calling action
  If more than 30 minutes elapse between password entry and the next call of the action, then Industrial HiVision queries the password again.

- Display settings for the content of the application event
- Display settings for the display type of the application event.
  “Only In Case Of Failure“: There has been a failure if the return value of the application has a value other than 0.

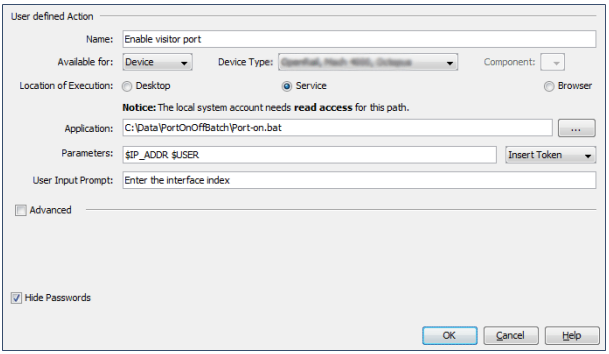


Figure 82: Example for a user-configurable action

Example for browser: “Call up web browser”
You want to access the Web server of your Industrial HiVision service to read the event list.

☐ In the Industrial HiVision menu bar, select `Configuration >` Preferences.
☐ In the settings dialog, select `Basics > User defined Actions`.
☐ To define a new user-configurable action, click the “New“ button.
☐ To call up the Telnet client, enter any name for example, “Event list”.
☐ In the “Available for“ row, you select the symbol with which you wish to start the action. Industrial HiVision places the action in the drop-down list according to the definition. You can find the action under “Actions“ by right-clicking this symbol.
  – As you want to call the action later at the device level, from the “Available for“ drop-down list, select “Device“.
☐ As the “Device Type“, select “Windows PC“.
☐ You want to view the event list in your web browser. Therefore you select “Browser“ as the “Location of Execution“ (see table 42).
☐ The “Parameters“ line gives you the option of transferring parameters to the application with tokens. Enter the following in the example:
  – Call up the Web browser
  – The token for the IP address of the computer on which the service of Industrial HiVision is running.

– The port for the Web server of Industrial HiVision
– The Web page you want to view

`http://$IP_ADDR:11208/events`

License

You require a license key to operate Industrial HiVision. The number of devices you can display depends on the license key. You thus have the option of adapting the amount you invest in Industrial HiVision to the growth of your network.
After a new installation or an update, you require new license keys. Industrial HiVision puts devices for which no license exists into the “Unmanaged” state. When you have entered a license key for these devices, you can put these devices into the “Managed” state again (see on page 269 “Manage”).
Industrial HiVision uses a seal to represent devices without a valid license.

Figure 83: Device without Industrial HiVision license key.

☐ Click the “New“ button and enter the license key in the entry window.
If you have the license key in electronic form, then you can use copy and paste to save having to type it in.
To complete the entry, click the “OK“ button.
You add new license keys and update licenses in the same way.

After you enter a license key, Industrial HiVision displays this license key in a row of the table.

Designation	Meaning
Key	Key number
Version	Software version number of Industrial HiVision
Expires	Date upon which the validity of the license ends
Type	Full version or update version
Devices	Number of devices covered by the license

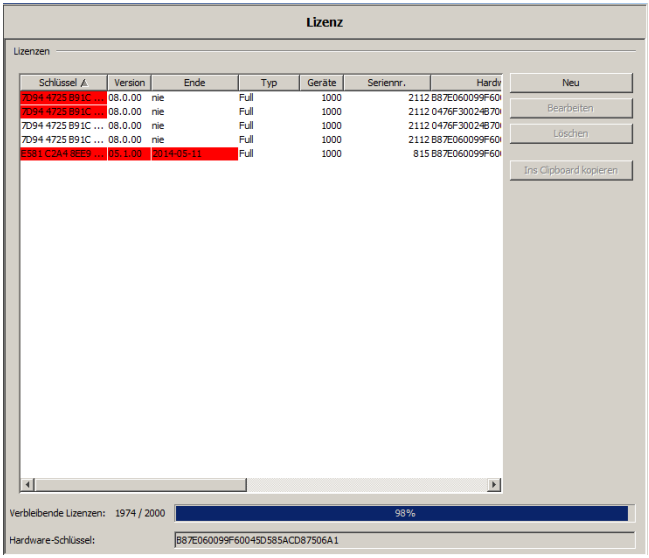
Table 43: Entries in the license table

Designation	Meaning
Hardware Key	Hardware key that you entered when requested to enter the license key. If the hardware key of this license key matches the hardware key under this license table, then you can use this license key on this network management station.
License Holder	Name that you entered when requested to enter the license key.
Registration Code	Registration code you received upon purchase of a full version, upgrade or maintenance schedule. You used this registration code to request the license key.

Table 43: Entries in the license table

A full license allows you to monitor a particular number of devices in Industrial HiVision. A full license is linked to the version of Industrial HiVision at the time of purchase.

Note: To determine the hardware key, Industrial HiVision uses a number of hardware components of its network management station. These hardware components include the network interface cards. For you to be able to replace hardware components, Industrial HiVision compares specific combinations of the hardware components in order to determine the hardware key.
As long as at least one of the network interface cards in the network management station that was installed when the license key was requested is active, Industrial HiVision detects the correct key. In this case, Industrial HiVision requires that other hardware components are still installed.
When Industrial HiVision detects that the management station is without an active interface card the “Hardware Key“ field displays this message. “The Hardware Key is not valid. It contains no network interface.” To display the hardware key, add a network interface. You can also activate a network interface for this purpose.



“Leased licenses“
When you have a hierarchical network structure and have leased licenses to subdomains, the bottom part of the “Licenses“ dialog contains a table for displaying the leased licenses.
This table contains the following columns:
– “Subdomain name“
– “IP Address“
– “Leased licenses“

Note: A superdomain requires its own license. The free-of-charge 16 nodes license cannot be assigned to the superdomain (see on page 53 “Advantages of the hierarchical network structure”).

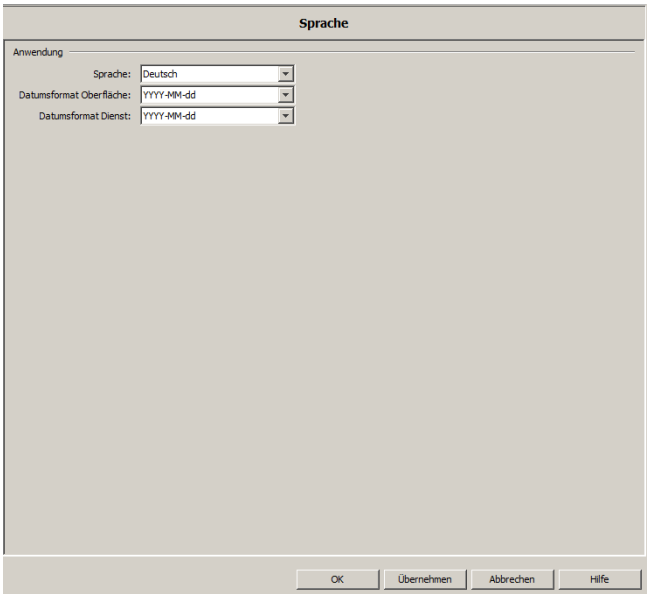
[Display]

Language

This dialog gives you the option to select the language of the graphical user interface and the date formats.

Default settings:

- Language: system language of your computer.
- Date format of the interface: year-month-day
- Date format of the service: year-month-day



Event

This dialog gives you the option of entering initial settings for the displaying of events.

Events in the event list (see figure 7):

- “Max. Number of Events“
  Use the drop-down list to select the maximum number of events which Industrial HiVision displays in the event list. If more events occur than the number specified, then Industrial HiVision discards the older events (first in, first out).
  Default setting: 1000
  Value range: ≤50000
- “Event Display“
  You use “Show Event List and Summary“ to display/hide the event list and the event summary in the main window.
  Default setting: display.
- “Event Log to File“
  With “Logging Enabled“ you can set Industrial HiVision to write every event that occurs in the event log file. Industrial HiVision writes the event log file in the language of the operating system.
  You will find the `HiVisionEvents0.csv` event log file in the installation directory of Industrial HiVision under `\log\events`.
  If the `HiVisionEvents0.csv` file exceeds a size of 1 MB, then Industrial HiVision renames the `HiVisionEvents0.csv` file as `HiVisionEvents1.csv`. Industrial HiVision writes new events in the new `HiVisionEvents0.csv` file.
  If the size of the `HiVisionEvents0.log` file exceeds 1 MB again, Industrial HiVision renames the files:
  – the `HiVisionEvents1.csv` file as `HiVisionEvents2.csv`
  – the `HiVisionEvents0.csv` file as `HiVisionEvents1.csv`
  – etc.
  Industrial HiVision can write up to 1000 log files. If other events occur, Industrial HiVision overwrites the `HiVisionEvents999.csv` file in accordance with the scheme described above.

- “Logfile path“
  As an alternative to the installation directory, this line gives you the option of selecting a path on which Industrial HiVision writes the event log file.

  Note: Delays or interruptions while writing to a network drive can block the Industrial HiVision service.

  Note: Delays and interruptions in the network can result in gaps in the content of the event log file.

  Note: As the service writes the log file, the local system account requires write permission for this directory.

- “Status Change Caused by Status Propagation“
  A status change for a property of a component/folder is an event which Industrial HiVision can display as an entry in the event list.
  Use the drop-down list to select the events that Industrial HiVision displays:
  – “No Event“, if you only want to display the status changes on the lowest level as an entry. The status changes which are propagated upwards from the lowest level are hidden by Industrial HiVision as an event entry.
  – “Info Event“, if you want Industrial HiVision to display the status changes as entries in the event list. The event entries caused by a propagated status change are assigned the type “Info” (see on page 90 “Number of events”).
  – “Similar Event“, if you want Industrial HiVision to display the status changes as entries in the event list.
  The event entries caused by a propagated status change are assigned the type corresponding to the propagated status change on this level.
  Default setting: No event.
- “Source“
  For an event that relates to a device, Industrial HiVision adds to the event list the device name with the location that you entered in the “Location“ device property.

Events on the Industrial HiVision website
(see on page 245 “Events on the website”)

- “Days in event log“
  On the event website, Industrial HiVision displays the events for the number of previous days that you enter here.
  Default setting: `7` days
- “Automatic page refresh every“
  Industrial HiVision refreshes the event website periodically. Here you enter the length of the period in minutes.
  Default setting: `5` min

“I'm alive Event“

- “Send I'm alive events“
  When you activate this function, Industrial HiVision periodically sends the event defined as the “I'm alive Event“ action.
  Default setting: `unmarked`

  Note: If you previously defined an “I'm alive Event“ category alarm and a related action, then Industrial HiVision also sends an associated “Alarm“ event (see on page “Industrial HiVision “I'm alive” event” on page 220).

- “Send interval“
  Default setting: `1` min
- “Event actions triggered by I'm alive event“
  When you activate this function, the associated “Alarm“ event also contains additional events with the “Warning“ or “Error“ status. These additional events are the ones that Industrial HiVision registered since it sent the last “I'm alive Event“.
  Default setting: `unmarked`

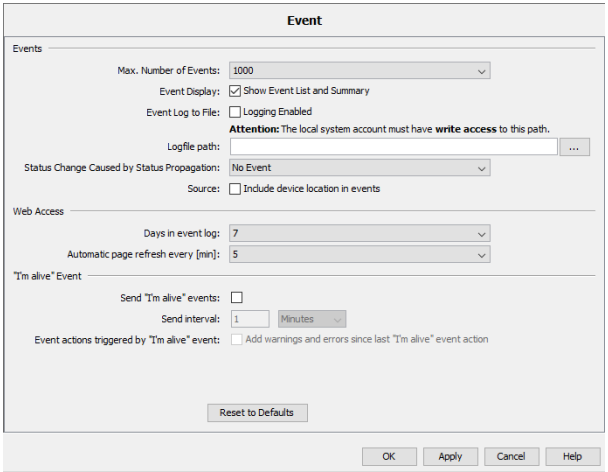


Figure 84: `Configuration > Preferences > Display > Event`

Event Auto-Acknowledge

This dialog gives you the option to set the “Status Worse“ events, that Industrial HiVision application can automatically acknowledge if a related “Status Better“ event occurs in a specified time interval.

Events in the “Event Auto-Acknowledge“ list:

- “Ping Reachability“
  An event related to a change in the reachability status of a port.
- “SNMP Reachability“
  An event related to a change in the reachability status of the SNMP protocol.
- “Port Link“
  An event related to a change in the link status of a port.
- “Port In Load“
  An event related to a change in the status of the inbound traffic load on a port.
- “Port Out Load“
  An event related to a change in the status of the outbound traffic load on a port.
- “Ring Coupling Status“
  An event related to a change in the status of the redundant ring coupling.
- “Ring Status“
  An event related to a change in the status of the “Ring Status“ property.
- “Rapid Spanning Tree Status“
  An event related to a change in the status of the Rapid Spanning Tree Protocol.
- “Spanning Tree Status“
  An event related to a change in the status of the Spanning Tree Protocol.
- “Multiple Spanning Tree Status“
  An event related to a change in the status of the Multiple Spanning Tree Protocol.

- “Interface Link“
  An event related to a change in the link status of an interface.
- “Interface In Load“
  An event related to a change in the status of the inbound traffic load on an interface.
- “Interface Out Load“
  An event related to a change in the status of the outbound traffic load on an interface.

To configure the auto-acknowledge function for an event proceed as follows:

☐ The auto-acknowledge function is disabled by default. To enable the auto-acknowledge function, mark the “Event Auto-Acknowledge Global“ checkbox.

☐ Select the event(s) for which it is necessary to enable the function. Mark the appropriate checkbox in the “Event Auto-Acknowledge“ list.

☐ To set the time interval, type the necessary value in the “Auto-acknowledge interval“ field and select the units of time for this value from the pull-down menu. You can select between seconds, minutes, hours or days.
Default setting: 3 minutes.
Value range for the “Auto-acknowledge interval“ can be specified between 1 second and 2 days.

When you configure an alarm for a “Status Worse“ event, you can also choose not to display an alarm for the event. This is possible if the event has been acknowledged beforehand.

You can create a new alarm for a “Status Worse“ event in the `Configuration > Preferences > Basics > Event Actions >` Alarms `> New > New Entry` dialog (see figure 81). In the “Type“ frame, mark the “If event has not been acknowledged after“ checkbox and select a time interval that exceeds the time interval specified in the “Auto-acknowledge interval“ field.

☐ To accept the changes, click the “Apply“ button.

☐ If you want to reset the values to default parameters, click the “Reset to Defaults“ button.

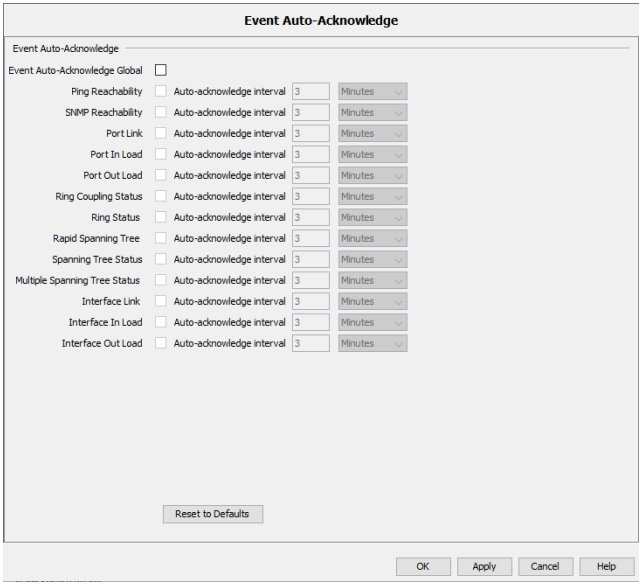


Figure 85: `Configuration > Preferences > Display > Event Auto-Acknowledge`

Device

This dialog allows you to specify the displaying of the devices in the network, the connections between the devices and the labeling.

- “Symbol“
  Click on the relevant white radio button to select the symbol that Industrial HiVision uses to display the device:
  – “Realistic“: display the device as a product image
  – “Abstract“: display the function of the device using a symbol
  Default setting: “Realistic“

- “Status Visualisation“
  Here you specify how Industrial HiVision optically displays the status of the devices or a status change on the screen.
  Industrial HiVision provides the following display options:
  – “Flash after Status Change“
  – “Acknowledged OK with Color“
  – “Status Symbol in Icon“
  – “Filled Background“
  – “Frame“
  – “Icon and Text Flash as well“
  Default setting: “Filled Background“ and “Frame“ activated.

- “Font“
  Enter the font size (in points) and the font type for the labeling of the devices and the connections between the devices.
  Default setting: font size = 13, font type = Arial.

- “Device Appearance“
  Specify the icon size and the maximum width (in pixels) with which Industrial HiVision displays the devices in the network on the screen.
  Default setting: icon size = 48, max. width = 150.

- “Connection Appearance“
  - Specify whether and how Industrial HiVision labels connections between the devices in the network on the screen.
    You use the “Draw Label“ drop-down list to select when you want Industrial HiVision to label a connection with the status of the connection.
    Options: “Always“, “Never“, “Under Mouse Pointer“
    Default: “Never“
    You use the “Draw Terminal Labels“ drop-down list to select when you want Industrial HiVision to label the terminal points of the connection.
    Options: “Always“, “Never“, “Under Mouse Pointer“
    Default: “Always“
  - The settings for “Line Thickness“ provide you with a better overview of the connection speed and the connection status in the topology view.
    If you activate the “Speed“ display, when the speed is increasing Industrial HiVision increases the line thickness in 2-point steps at 10, 100, 1000, 10000 MBit/s. If you activate the “Speed“ display, Industrial HiVision displays the current connection setting in the bubble help.
    If you deactivated the “Speed“ display, Industrial HiVision displays the current speed setting even if you have activated the “Speed“ display in the connection properties dialog (see on page 293 “Connection”).
    If you activate the “Status“ display, when the status weighting increases Industrial HiVision increases the line thickness in 2-point steps.
    Default setting: “Status“
  - The “Minimum Line Thickness“ is the minimum thickness applied by Industrial HiVision when increasing the line thickness depending on the speed.
    Possible: 1, 3, 5
    Default setting: 1

- “Preview“
  The “Preview“ frame displays how your settings affect the display.

Display	Meaning
OK Acknowledged	Status has not changed and is OK.
OK Status Changed	Status has changed and is OK.

Table 44: Preview for displaying devices and connection lines

Display	Meaning
Warning Acknowledged	Status has not changed. There is a warning message.
Warning Status Changed	Status has changed. There is a warning message.
Error Acknowledged	Status has not changed. There is an error.
Error Status Changed	Status has changed. An error has occurred.

Table 44: Preview for displaying devices and connection lines

▶ If you click on “Reset to Defaults“, the changes you made are reset to the default settings.

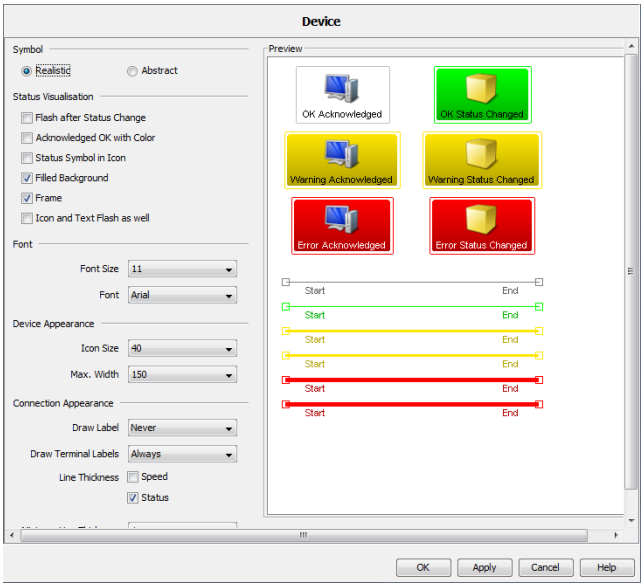


Figure 86: `Configuration > Preferences > Display > Device`

Appearance

This dialog allows you to alter the text display and the tab page selection:

- “Toolbars“
  Text placement in the tool bar
  Default setting: “Text Alongside Symbol“
- “Font Size“
  Default setting: depends on the screen resolution.
- “Security“
  Display password as stars (not readable) when dialogs are opened in which you enter or can see passwords.
  Default setting: “Hide Passwords“
- “Tab Presets“
  Depending on the context, Industrial HiVision provides you with various tabs:
  – Select “Saved settings“ to display the tab last opened in this view when you open the view.
  – Select “Default settings“ so that Industrial HiVision selects the tab with the list display below the device level.
  – Select “Don't apply“ so that when Industrial HiVision changes to another device or component detail, it keeps the current display type (list or topology display).
  Default setting: “Saved settings“
- “Home View Settings“
  Specifies the display default settings for the “Home View“ button.

Industrial HiVision allows you to save the following settings:

- Specify a different folder in the menu tree.
- Specify a different screen size.
- Specify either the maximize or normal view.

The following parameters are set as default in Industrial HiVision:

- VLAN “All“
- “Last 24 Hours Events“
- “Map“ view

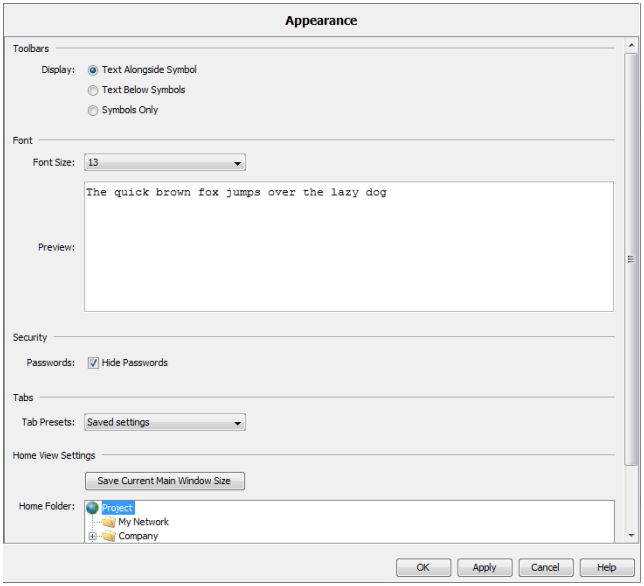


Figure 87: `Configuration > Preferences > Display > Appearance`

Status Colors

This dialog allows you to assign a color to every status. You can select the colors for the foreground and the background.

Status	Foreground	Background
OK	Black	Green
Warning	Black	Yellow
Error	White	Red
Not Available	Black	gray
No Status	Black	White

Table 45: Default setting of the status colors

- If you click on “Reset to Defaults“, the changes you made are reset to the default settings.

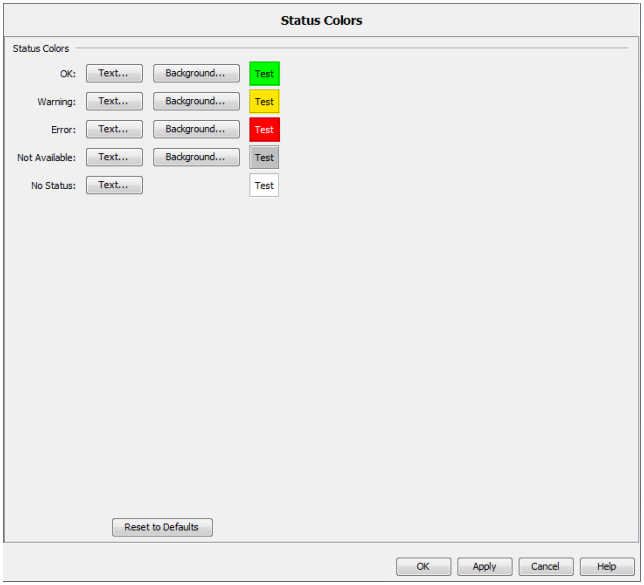


Figure 88: `Configuration > Preferences > Display > Status Colors`

Device Icon

This dialog enables you to assign defined default icons to different device types when devices are detected.

☐ To define a new default icon assignment, click the “New“ button or to edit an entry, select a row in the table and click the “Edit“ button.

Industrial HiVision provides the following methods for differentiating the device types:

▶ System Object Identifier (“SysOID“)

Type	SysOID
SysOID	Manufacturer ID
Icon	Click on “?” to search your file system for an image file for the icon.

▶ “EtherNet/IP“
Along with entering the parameters in the dialog, Industrial HiVision allows you to load the parameters from an EDS file (electronic data sheet).

Type	EtherNet/IP
Vendor Code	Manufacturer ID in the device description based on EtherNet/IP.
Product Type	Product type in the device description based on EtherNet/IP. An “*” in this field means “all product types”.
Product Code	Product code in the device description based on EtherNet/IP. An “*” in this field means “all products”.
Icon	Click on “?” to search your file system for an image file for the icon.

▶ “Modbus/TCP“

Type	Modbus/TCP
Vendor Name	Manufacturer ID in the device description based on Modbus/TCP.
Product Code	Product code in the device description based on Modbus/TCP. An “*” in this field means “all products”.
Icon	Click on “?” to search your file system for an image file for the icon.

▶ “MAC Address“

Type	MAC Address
MAC Address	The part of the MAC addresses of devices to which you want to assign a device icon using the MAC address. For example, the first 24 bits of the MAC address of Hirschmann addresses are 00:80:63.
Number of Bits	The number of bits of the MAC addresses that you want to use for the icon assignment. The first 24 bits of a MAC address indicate the manufacturer of a device.
Icon	Click on “?” to search your file system for an image file for the icon.

In the table, you can:
– add new entries
– edit existing entries
– delete existing entries
– duplicate existing entries
– add new EtherNet/IP entries using the “EDS File“ button. Industrial HiVision loads the EDS files selected together with the corresponding icon files.
  Industrial HiVision also finds icons in manufacturer-specific subfolders.

  The EDS Files are located on the device CD, or can be downloaded from the web page of the manufacturer. The EDS files contain the “Vendor Code“, “Product Type“, “Product Code“ and the name of the icon. Industrial HiVision attempts to open the icon with the specified name.

  If Industrial HiVision does not open the icon for the new device, then proceed as follows:
  ☐ Open the EDS file of the device using a text editor e.g. Notepad++.
  ☐ Verify that the icon is in the specified path, e.g. “Icon = "Icon/xxxx.ico";”.
  ☐ Save and close the EDS file.
  ☐ Click the “EDS File“ button.
  ☐ Select the EDS file for the device.
  ☐ Click the “OK“ button.

In the device detection, and for selected devices with `Edit > Set Default Device Icon`, Industrial HiVision checks the device type. Industrial HiVision assigns the device the first icon that Industrial HiVision finds in the table.

To change the sequence of the entries in the table, use the “Up“ and “Down“ buttons.
The icons already defined in Industrial HiVision for Hirschmann devices are hidden at the top of the table. Thus Industrial HiVision assigns the correct icons to the Hirschmann devices.

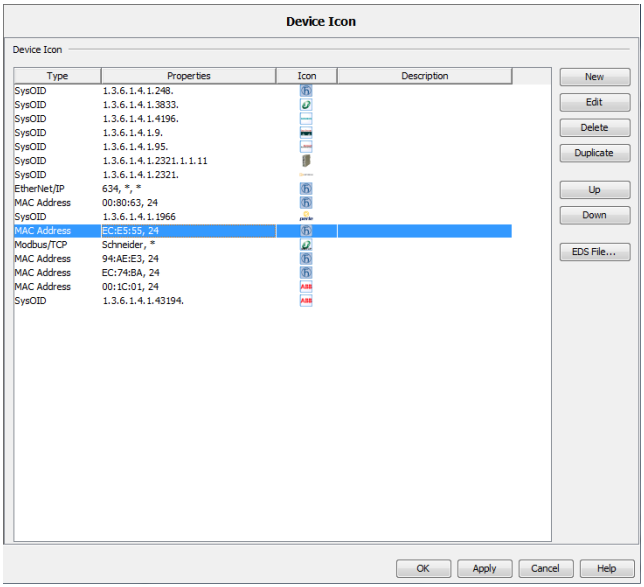


Figure 89: Assignment table for device icons

[Advanced]

Program Access

“Password for Edit Mode“
This function helps protect the edit mode from unauthorized access.

You can enable the “Password for Edit Mode“ function only when the “User Management“ function is disabled. To verify that the “User Management“ function is disabled, perform the following steps:
☐ Open the `Preferences > Basics > User Management` dialog.
☐ Verify that the “Selected Order“ window is empty.

To enable and test the “Password for Edit Mode“ function, perform the following steps:
☐ Enter the same password in the “Password“ and the “Retype Password“ fields.
☐ To save the password in the database and close the dialog, click the “OK“ button.
☐ To verify that the “Password for Edit Mode“ function is enabled, click the “Edit Mode“ button. Industrial HiVision opens the “Edit Mode Password“ dialog.

Note: When you click the “Edit Mode“ button and the “User Account“ dialog opens, this is an indication that the “User Management“ function is enabled. To access the edit mode, when the “User Management“ function is enabled, enter the password of the user that is currently logged in.

“Expire Time for Edit Mode“
With the Expire Time you specify how long Industrial HiVision stays in the Edit Mode after you have made an entry. When this time has expired, Industrial HiVision switches to the Run Mode.
Possible settings: `5` to `60` minutes or “Permanent“.

“Save Project file when Edit Mode switches“
This function lets you save the Industrial HiVision project file. You can select the moment Industrial HiVision automatically saves the project file, as follows:
▶ at the activation of the “Edit Mode“
▶ at the deactivation of the “Edit Mode“
▶ in both of the above cases

In the “Save Location“ field you can find the location where Industrial HiVision saves the project file.This location is on the hard drive of the PC that runs the Industrial HiVision kernel. You cannot change this location.
To configure the “Save Project file when Edit Mode switches“ function, perform the following steps:

☐ In the “Project File Name Prefix“ field, specify the prefix of the project file name.
Possible values: Alphanumeric ASCII character string with 1..30 characters
The following characters are allowed:
- `0..9`
- `a..z`
- `A..Z`
- `_`

The pattern of the project file name is as follows:
`prefix-YYYY-MM-DD-HH-MM-SS.ihp`

☐ To save the project file when you activate the “Edit Mode“, mark the “Save at Edit Mode Start“ checkbox.
Default setting: `unmarked`

☐ To save the project file when you deactivate the “Edit Mode“, mark the “Save at Edit Mode End“ checkbox.
Default setting: `unmarked`

Note: Industrial HiVision saves a maximum of 100 project files in the location on the hard drive of the PC that runs the Industrial HiVision kernel. If this number is exceeded, then Industrial HiVision deletes the oldest saved files.

“Web Access“
“Generate an Event for every Successful Web Access“ lets you to also generate an event for every successful Web access, in addition to unauthorized access attempts.

“Properties“
“Allow Renaming“ lets you to rename a property of the component details. For example, you can change the “In Load“ property of a connection to “Volume of Incoming Data”.

“Auto Reload“ lets you to get Industrial HiVision to perform the following task:
– query the current values for a property dialog when it opens this dialog
– query the current values of the content of the detail frame when it opens this frame.

The “if Value Older than“ function lets you to make an automatic querying of the values to be displayed depending on the age of these values.

“Device Documentation“
“Include device passwords in documentation“ allows you create the device documentation with a readable or a hidden password.
Default setting: password hidden.

	☐	☑
SNMP V1	******,******	public, private
SNMP V3	admin, MD5: ******, DES: ******	admin, MD5: private, DES: private

Table 46: Example device documentation with a readable and a hidden password.

Note: If you have forgotten your password, then quit Industrial HiVision. Logon to Windows as an administrator or to Linux as a root and start Industrial HiVision again. Restarting Industrial HiVision as an administrator or as a root enables you to make a new entry without the password being queried first.

Figure 90: `Configuration > Preferences > Advanced > Program Access`

Services Access

The “Services Access“ dialog lets you to activate and deactivate various methods of accessing network management from another computer. When a firewall separates your Industrial HiVision services from a client, add a rule to the firewall to forward data between the services and client.
See “Using Industrial HiVision with Firewalls” on page 62.

- “Web Server“
  This service allows you to access your network management server using a Web browser using another computer. The address of the Web server is:
  protocol://IP address of the network management station:port number, for example
  `http://10.0.1.159:11208`
  When setting up a secure connection using HTTPS, Industrial HiVision uses a Hirschmann certificate that classifies your browser as invalid. If you want to use this service, then you trust this connection, add an exception to your browser. Save the exception.
  If you wish to specify a different value that Industrial HiVision uses to connect to the “Web Server“, then unmark the “Use Default Values“ checkbox. Enter the desired value in the “Port“ field. If you mark the “Use Default Values“ checkbox, then Industrial HiVision resets the value in the “Port“ field to the default value `11208`.
- “Project Data Server“
  With “Remote Access“ you let Industrial HiVision interfaces running on other computers to have access to the local Industrial HiVision service. If you permit “Services Access“, then the local interface connects using the network connection, as an alternative to the internal IP address `127.0.0.1`. The local interface connects the same way as the interface of the external computer. A result of this is that the internal interface also loses the connection to the service if the network connection is interrupted.
  The “Port“ field displays the port on which Industrial HiVision interfaces, running on other computers, can access the local Industrial HiVision service.

  Note: Starting with Industrial HiVision release 8.0, you can change the value of the `Project Data Server > Port` field.

  “Subdomain interface“

If you activate the “Subdomain interface“ function, you let another network management station access the local Industrial HiVision as a superdomain.
“Password“
If you use this management station as a subdomain, then the dialog gives you the option to type in the password for access to the subdomain interface. See “Connect subdomains to superdomains” on page 56.
“Superdomain“
When a secured connection is established, Industrial HiVision lets you select the process that the superdomain uses to handle certificates provided by the subdomain:

- “Accept any subdomain certificate“
  This method permits the superdomain to accept the certificate provided by the subdomain without verification. The certificate is not added to the trust store and an event is created with the fingerprint of the subdomain in the message.
  Default setting: `marked`
- “Accept any subdomain certificate and store as trusted“
  This method permits the superdomain to accept the certificate provided by the subdomain without verification. The certificate is added to the trust store and it is used for future connections. An event is created which records the fact that the fingerprint of the subdomain is added to the trust store.
  Default setting: `unmarked`
- “Verify subdomain certificate against trusted certificates“
  This method is used to verify that the certificate provided by the subdomain is added to the trust store.
  If the certificate is not in the trust store, then the connection is rejected. An error event is created with the fingerprint of the subdomain in the message.
  Default setting: `unmarked`

- “OPC Server“
  The “OPC Server“ lets you activate the Industrial HiVision OPC server (see on page 235 “Structure of the transfer data for OPC”).
  With “Global Write“ you permit Industrial HiVision to write object values using an OPC write command (see on page 233 “Link to process visualization system”).
  To help secure communications between the OPC UA server and Industrial HiVision, use a CA certificate (see on page 241 “OPC UA Server Custom Certificates”).
  When using HTTP to connect to the Industrial HiVision OPC UA

server, configure the OPC UA client to access the server on the port displayed in the “OPC UA Server Port (http)“ field.
When using HTTPS to connect to the Industrial HiVision OPC UA server, configure the OPC UA client to access the server on the port displayed in the “OPC UA Server Port (https)“ field.

Note: When you deactivate the “OPC Server“ function, restart the Industrial HiVision kernel.

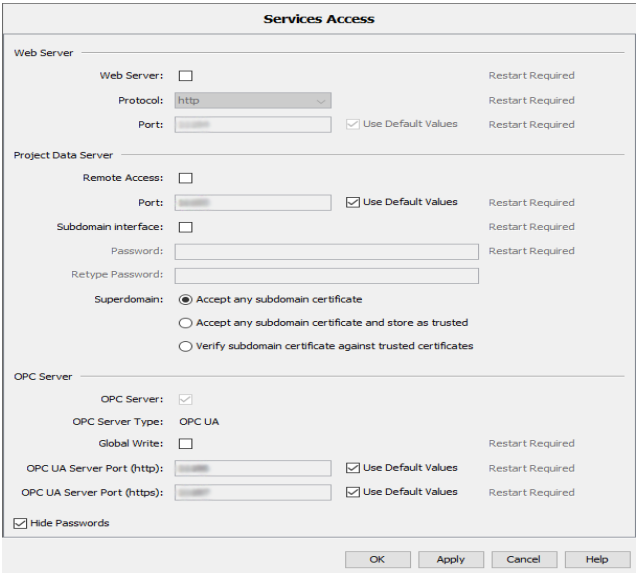


Figure 91: `Configuration > Preferences > Advanced > Services Access`

Device Credentials

Industrial HiVision supports you in communicating with SNMP devices by means of automated password usage.

“Device Credentials“
When setting up the communication with an SNMP device, Industrial HiVision tries to get access using known passwords and user names.
For an attempt with an incorrect password, Industrial HiVision gets an authentication trap from the relevant device.
For an attempt with a correct password, Industrial HiVision gets a reply to an SNMP query and enters the correct password and user name into the upper table of this dialog.

“SNMP Guess List“
When setting up the communication with an unknown SNMP device, Industrial HiVision attempts to authenticate itself with the login data from the “SNMP Guess List“.
You use the “New“ button to create a new entry in the table.
Industrial HiVision gives you the following options for table entries:
– change the entry using the “Edit“ button
– delete the entry using the “Delete“ button
– duplicate the entry using the “Duplicate“ button

“Hide Passwords“
Industrial HiVision lets you hide the passwords for this table entry. The dialog displays the passwords as asterisks.
When you open this dialog, the setting for this field depends on the setting in the `Display > Appearance` dialog.

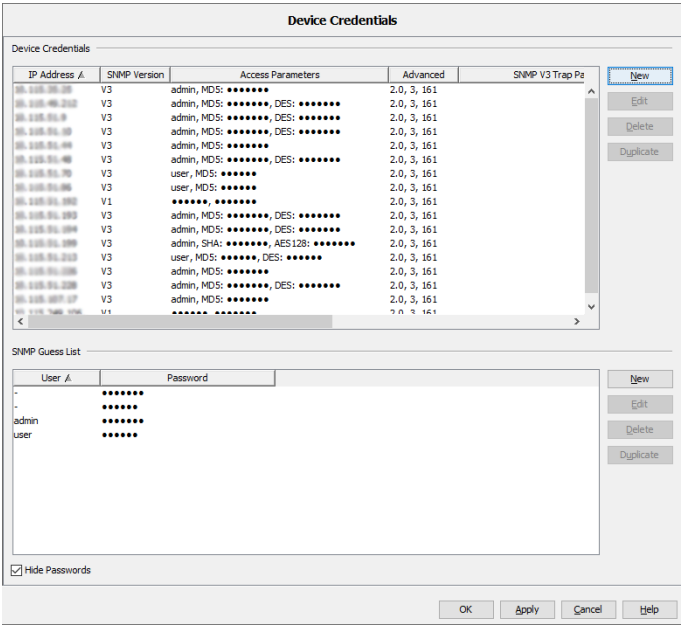


Figure 92: `Configuration > Preferences > Advanced > Device Credentials`

Along with the automatic password usage, Industrial HiVision also gives you the option of manually entering the SNMP configuration for individual SNMP devices.

- ☐ To open the “New Entry“ dialog for the SNMP configuration, in the “Device Credentials“ frame, click the “New“ button.
- ☐ Enter the IP address of the device for which you want to enter the SNMP access configuration.
- ☐ Select the SNMP version that supports the device.
- ☐ Depending on the SNMP version selected, you enter the required access information:

SNMP version	Designation	Meaning
V1	Read Password	Password with which you can get read access to the device
V1	Write Password	Password with which you can get write/read access to the device.
V3 (easy)	Username	User name with which you can access the device.

Table 47: SNMP configuration entries

SNMP version	Designation	Meaning
V3 (easy)	Password	Password belonging to the user name.
V3 (complete)	Username	User name with which you can access the device.
V3 (complete)	Authentication	SHA, MD5 method for authentication of the message
V3 (complete)	Password	Password for the authentication
V3 (complete)	Encryption	DES, AES128, symmetrical encryption algorithm
V3 (complete)	Password	Password for the encryption

Table 47: SNMP configuration entries

Under “Advanced“ you will find SNMP-specific exchange parameters. The default settings are sufficient for many requirements.

- With “Timeout [s]“ you specify how long Industrial HiVision waits for the response to an SNMP query. If there is no response, then Industrial HiVision repeats the SNMP query.
- With “Retries“ you specify how often Industrial HiVision repeats the SNMP query if there is no response.
  For each repetition, Industrial HiVision doubles the timeout time, Industrial HiVision sends a new query.
- With “Port No“ you select the protocol port of the device to which Industrial HiVision sends an SNMP query.

Note: To receive SNMPv3 Traps on Windows, disable the Windows trap service. The Windows trap service only supports SNMPv1 Traps.

In the “SNMP Trap“ frame you configure how Industrial HiVision receives SNMPv3 traps, for example, what type of encryption or authentication is used. To change the values of the devices, configure the settings in MultiConfig™ and set the user to “Active“, then write the settings to the device. Industrial HiVision automatically populates the values in the fields of this frame with the values of the active user on the device (see on page 171 “Configuring SNMPv3 traps”).

Note: For security reasons, Hirschmann recommends that you use SNMPv3 traps.

- The “SNMP Version“ field displays the SNMP version that Industrial HiVision uses to receive SNMP traps.
- The “Username“ field identifies the user profile.
- In the “Authentication“ field, set this value to the same setting as configured in the “SNMP Auth Type“ field for the `admin` user on the device. Possible values: “-” (none), `MD5` and `SHA`

- Assign a unique password for the authentication in the “Password“ field.
- The “Retype Password“ field lets you verify your password.
- In the “Encryption“ field, set this value to the same setting as configured in the “SNMP Encryption Type“ field for the `admin` user on the device. Possible values: “-” (none), `DES` and `AES128`
- Assign a unique password for the encryption in the “Password“ field.
- The “Retype Password“ field lets you verify your password.

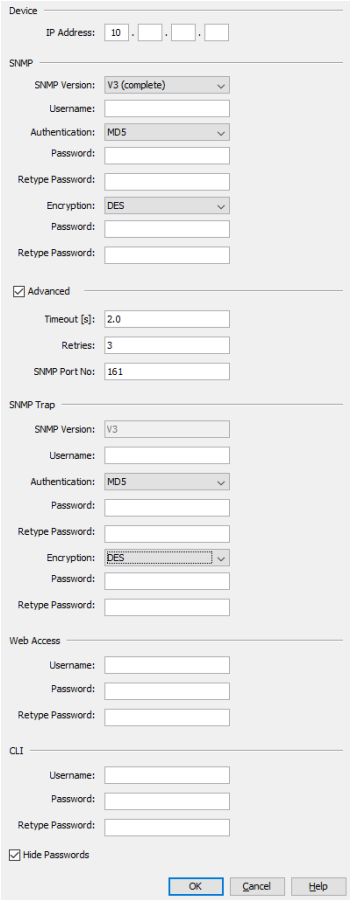


Figure 93: `Configuration > Preferences > Advanced > Device Credentials >` *New*

Export to InfluxDB®

The “Export to InfluxDB®“ dialog lets you enable or disable the export to InfluxDB®, and configure the connection parameters and the export settings. To configure these parameters, perform the following steps:

- ☐ To enable the “Export to InfluxDB®“ function, mark the “Export“ checkbox. When you mark this checkbox, the fields related to the connection parameters become editable.
  Default setting: `unmarked`
- ☐ In the “Database Server URL“ field, enter the URL for the InfluxDB® server.
  Possible values: ASCII character string with `1..1000` characters
  Default setting: `https://localhost:8086`
- ☐ In the “User“ field, enter the user name of the InfluxDB® database.
  Possible values: ASCII character string with `1..40` characters
  Default setting: empty field
- ☐ In the “Password“ and the “Retype Password“ fields, enter the same password for the InfluxDB® database.
  Possible values: ASCII character string with `1..40` characters
  Default setting: empty field
- ☐ To test the connection with the InfluxDB® server, click the “Test Connection“ button.
  When you click the “Test Connection“ button, a connection testing procedure is triggered. In order for the connection testing procedure to start, fill each field in the “Database Connection Settings“ frame.
  The connection testing procedure consists of the following verification flow:
  - ▶ The procedure checks that an InfluxDB® server is up and running at the URL configured in the “Database Server URL“ field.
  - ▶ If you use the HTTPS protocol, then the connection testing procedure prompts you to accept InfluxDB® server certificates.
  - ▶ The procedure accepts the login to the InfluxDB® server with the configured credentials.

- The procedure checks that the user identified by these credentials has write permissions to the InfluxDB® database.
- If the database does not exist, then the procedure creates the InfluxDB® database.

When the connection testing procedure ends, Industrial HiVision displays a status icon and an explanation message in the field related to the “Test Connection“ button.
When the connection is established, Industrial HiVision displays a green check mark.
If the connection is not established, then you get one of the following error messages:

- “Server not reachable“
  There is no server running at the specified URL.
  Verify that the InfluxDB® server is up or that the specified URL is correct.
- “Wrong protocol“
  The InfluxDB® server accepts an HTTP protocol but the URL specifies an HTTPS protocol or the other way around.
  Verify that the URL you provided in the “Database Server URL“ field contains the correct transfer protocol.
- “Authentication failed“
  The provided credentials are incorrect.
  Verify that you provided the correct credentials.
- “No write permissions“
  The provided credentials identify a user that does not have write permissions to the InfluxDB® database.
  Verify that the user you provided has write permissions to the InfluxDB® database.

- ▶ “Operation failed“
  The HTTPS certificate was not accepted in the “Confirm Server Certificate for Industrial HiVision Server“ dialog or an internal error occurred.
  Accept the correct InfluxDB® server certificate in the “Confirm Server Certificate for Industrial HiVision Server“ dialog.
- ▶ “Operation in progress“
  The connection testing operation is currently in progress.
  Wait for the connection testing procedure to complete.

When you use the secure HTTPS protocol and test the connection to an InfluxDB® server for the first time, the “Confirm Server Certificate for Industrial HiVision Server“ dialog opens. This dialog prompts you to confirm the InfluxDB® server certificate.

- ☐ To accept the certificate, click the “Accept“ button.
  If you do not test the connection and click the “Apply“ button, then Industrial HiVision displays the following warning:
  “After configuring a https transport testing connection is mandatory to accept server certificate“
  If you close the “Preferences“ dialog without testing the connection, then the export to InfluxDB® server is not enabled.

☐ In the “Full Export Interval“ field, enter the time interval at which Industrial HiVision sends the full set of monitored parameters to the InfluxDB® server. The values are sent whether they were changed or not. In the related drop-down list, select the unit of measurement for the time.
Minimum value: `1` h
Default setting: `1` h

When the `Preferences > Export` checkbox is enabled, the device property data export starts or restarts automatically in the following situations:

- ▶ The Industrial HiVision kernel starts.
- ▶ The connection parameters or the export settings are changed and the `Preferences > Export to InfluxDB®` dialog is closed.
- ▶ The state of the `Configuration > Export to InfluxDB® > Export` checkbox for a category is changed and the `Configuration > Export to InfluxDB®` dialog is closed.
- ▶ A value or the status of a property changes. Industrial HiVision sends each individual parameter to the InfluxDB® server immediately when its value changes.

Note: The “Database Name“ field is not editable. The default database name is `ihivision_data`.

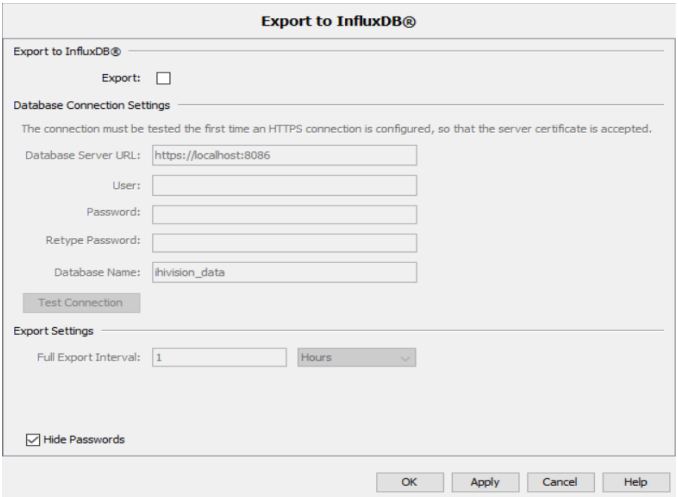


Figure 94: `Configuration > Preferences > Advanced > Export to InfluxDB®`

Management Station

In this dialog you enter the default setting for IP parameters. Industrial HiVision enters these default settings when you open dialogs where IP parameter entries are expected for example, IP configuration of devices which Industrial HiVision detected using HiDiscovery V1.

“IP Address Prefix“:
Here Industrial HiVision enters the prefix of its own IP address.

“Default Netmask“:
Here Industrial HiVision enters the network mask of its own IP address.

“Default Gateway“:
Here Industrial HiVision enters the prefix of the gateway which your network management station also uses.

“IP Address Management Station“:
If your network management station has a number of IP addresses, then Industrial HiVision enters these IP addresses in the drop-down list.
☐ Select the address you want to use as a trap destination address.

“Network Card Management Station“:
If your network management station has a number of network cards, then Industrial HiVision enters these cards in the drop-down list.
☐ Select the card which you want the HiDiscovery V1 protocol to access.

“Management Station Appearance“:
When the “Do not Change Management Station Icon“ function is active and Industrial HiVision discovers a device on which the kernel is running, then Industrial HiVision keeps the icon for the device.

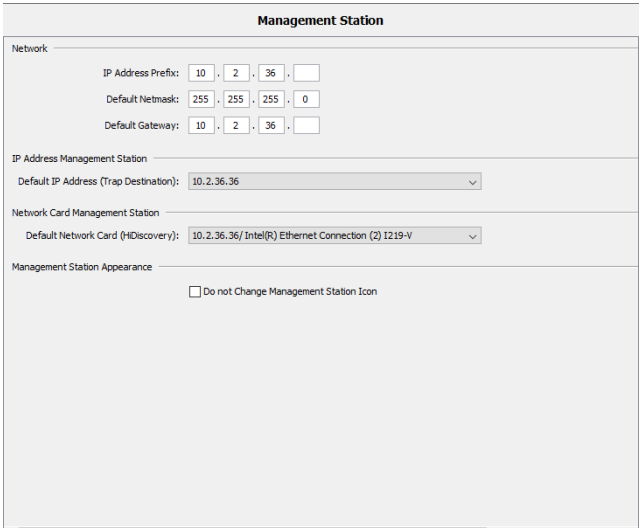


Figure 95: `Configuration > Preferences > Advanced > Management Station`

OPC-SNMP

The OPC server of Industrial HiVision allows you to use an OPC client query to determine SNMP values for devices.
In the `Advanced > OPC-SNMP` dialog you enter the SNMP attributes whose values you want to determine. In the table, you can

- add new entries
- edit existing entries
- delete existing entries
- duplicate existing entries

In the “Edit“ and “New“ dialogs, you can enter the SNMP attributes directly, or select them from an MIB.
To select an SNMP attribute from a MIB, click the “Select MIB Attribute...“ button. In the “MIB Viewer“ dialog, select an SNMP attribute. To load additional MIBs, you can use the “MIB Manager“ button.
Give the entry a brief, meaningful name, as this will be used later on for the query in the OPC tag.
If you use an Object Identifier (OID) in the OPC tag, you enter the complete OID, including any existing instance.

The OPC tag for an OPC client query is, for example:
`Industrial_HiVision.snmp.get.10:0:1:159,161,ifAdminState`

Whereby:

- `10:0:1:159` is the IP address of the device, with a colon instead of a dot as a separator
- `161` is the SNMP port
- `ifAdminState` is the name of the SNMP attribute, as configured in the settings

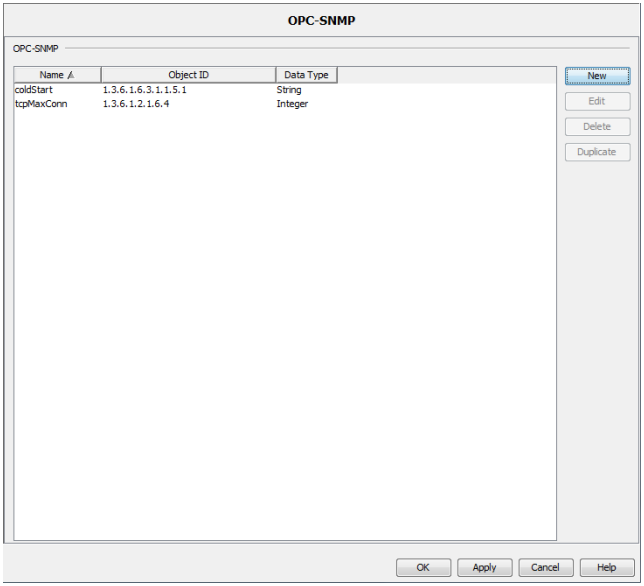


Figure 96: `Configuration > Preferences > Advanced > OPC-SNMP`

Service Parameters

The Industrial HiVision program starts its own service. Your PC operating system displays this Industrial HiVision service for you.
The Industrial HiVision service is made up of the following services:

- "Device Discovery"
  - "Scan Rate [devices/min]"
    This service performs the network scan (see on page 324 "[Basics]"). The scan rate limits the number of pings/minute.
    Default setting: `600`
  - "Simultaneously Discovered Devices"
    This setting allows you to modify the network load during the device discovery. Here you enter the number of devices that Industrial HiVision simultaneously queries during the device discovery.
    Default setting: `20`
  - "SNMP Guessing Packet Rate [pkts/s]"
    With this setting you define up to how many guess packets per second Industrial HiVision sends to an unknown SNMP device to discover the login data.
    Default setting: `100`
- "Web Server"
  - "Web Server Root Directory"
    The parameter displays the Industrial HiVision web server base directory.
  - "Web Server Session Timeout [min]"
    This parameter allows you specify the maximum idle time for web server sessions.
    Default setting: `20`

- “Device Availability“
  These settings allow you to adjust Industrial HiVision to the ping response behavior of your devices.
  - “Ping Timeout [s]“
    If the ICMP device responds to a ping request within this period, then Industrial HiVision classifies the device as still present, if it responded to the last request.
  - “Max. Ping Response Time [ms]“
    If the ICMP device responds to a ping request within this period, then Industrial HiVision detects that the device is present again, if it did not respond to the last request.

  Lower values improve the performance of Industrial HiVision. If the values are too low, the ping response may come too late and Industrial HiVision displays the device as “unreachable”. With large subnetworks that can display short term interrupts, you should use smaller values. Larger values can cause status changes to be displayed late in Industrial HiVision.
- “Reporting“
  - “Reliability Polling Intervals“
    The value queried was recorded a longer time ago than the maximum number of polling intervals x the polling interval [s] of the property query (see on page 285 “Properties of a component detail”).
  - “Replication Lock for Reporting Events [s]“:
    The retry block helps you to reduce how often repeating events are recorded in the event list.
    Default setting: `3600`
    Industrial HiVision records reporting events of the “Warning“ and “Error“ types if their last recording was further back than the duration of the retry block.
    The changed value is applied only after the Industrial HiVision server is restarted.

- “Statistics“
  - “ICMP Statistics - Moving Average Number of Samples“
    The entry specifies the moving average which is computed based on a subset of response times.
    Default setting: `5`
    The moving average is included as a property type per device in protocol properties and can be added to the reporting tool.
  - “SNMP Statistics - Moving Average Number of Samples“
    The entry specifies the moving average which is computed based on a subset of response times.
    Default setting: `10`
    The moving average is included as a property type per device in protocol properties and can be added to the reporting tool.
- “Polling“
  - “Polling ramp-up - Start of Operations per Second (0 means unlimited)“
    This parameter allows you to specify the rate of polling operations started per second. This rate represents the number of new operations that are added to the polling engine until each polling operation is handled.
    Possible values: `0..1000`
    Default setting: `0`
    The value `0` means that the polling ramp-up is disabled and every enabled polling operation starts at the same time.
    The changed value is applied only after the Industrial HiVision server is restarted.

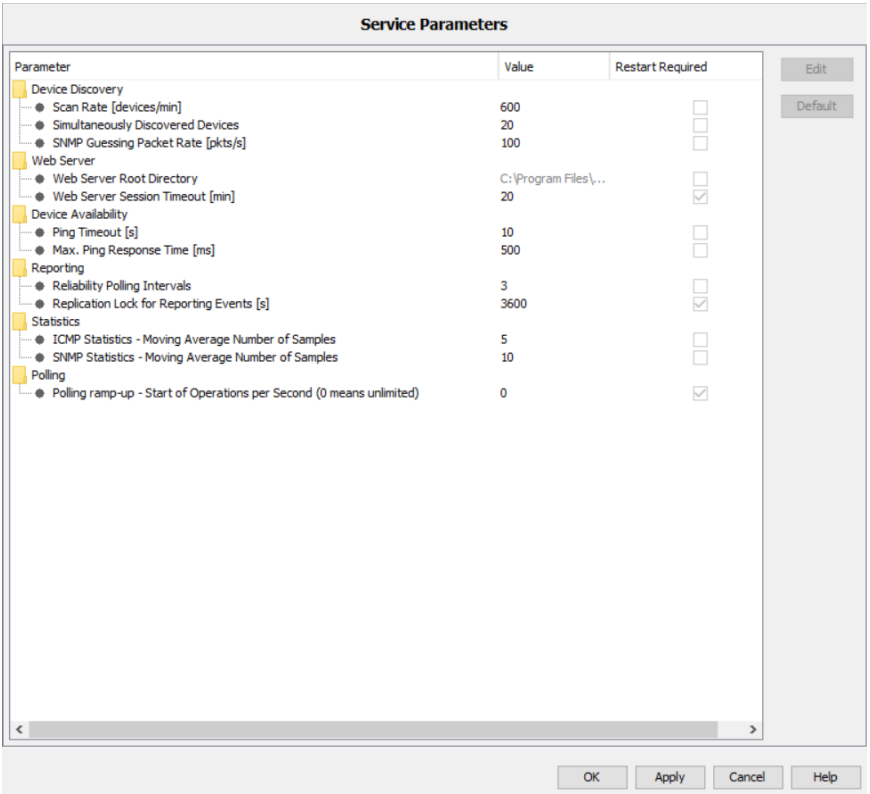
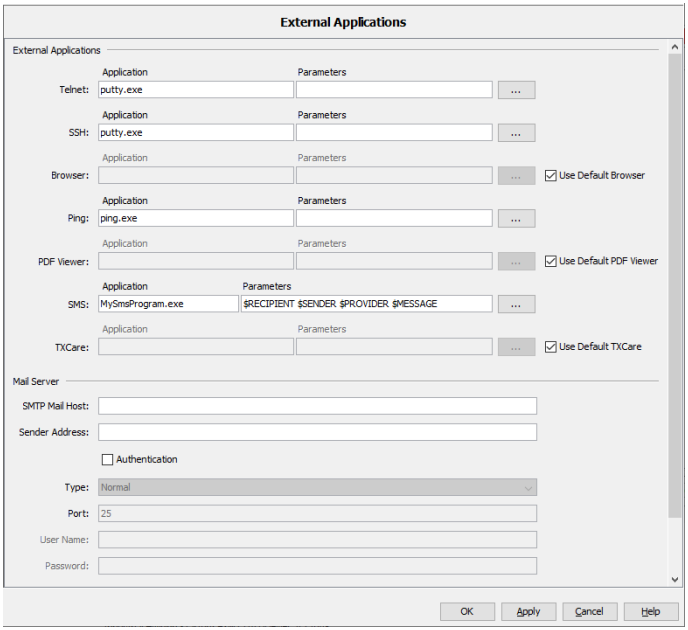


Figure 97: `Configuration > Preferences > Advanced > Service Parameters`

External Applications

Industrial HiVision uses external auxiliary programs for the following functions:

- “Telnet“
- “SSH“
- “Browser“
  On Linux systems, Industrial HiVision uses Mozilla Firefox as the standard browser. If you want to use a different browser, enter the path to your browser in the “Browser“ line.
- “Ping“
- “PDF Viewer“
- “SMS“
- “TXCare“
  If you have installed the TXCare program in the Industrial HiVision installation directory, then you can mark the “Use Default TXCare“ checkbox.
  If you have installed the TXCare program in another location, then type in the location in the “TXCare“ text field.
  For further information about the “TXCare“ program see “TXCare” on page 125
- “Mail Server“
  To carry out email configuration
- “Geographical Location View“
  URL entry for summoning the geographic location display program for example, maps.google.
  `http://maps.google.de/maps?q=$LATITUDE,$LONGITUDE($NAME)&z=19`
  See “Geographical Location View” on page 304.


External Applications
External Applications
Application
Parameters
Telnet:
putty.exe
SSH:
putty.exe
Browser:
Use Default Browser
Ping:
ping.exe
PDF Viewer:
Use Default PDF Viewer
SMS:
MySmsProgram.exe
$RECIPIENT $SENDER $PROVIDER $MESSAGE
TXCare:
Use Default TXCare
Mail Server
SMTP Mail Host:
Sender Address:
Authentication
Type:
Normal
Port:
25
User Name:
Password:
OK
Apply
Cancel
Help

Device/Port Names

With this dialog you manipulate the names of the devices and ports in the respective Properties dialog and thus their representation in the user interface.
You first select whether Industrial HiVision displays the devices and ports with their preset names, or whether Industrial HiVision determines the names from the device.

When adding new devices to Industrial HiVision, the “Device/Port Names“ frame allows you to select the method in which Industrial HiVision displays the device names.

- The “Basics“: “Use default names or entered names“ function allows Industrial HiVision to display new devices with the IP address.
- The “Basics“: “Set names from device in Industrial HiVision“ function allows Industrial HiVision to display the name of the new devices.

Note: The “Reset to Defaults“ button only resets the “Device/Port Names“ dialog to the default settings.

To change the manner in which Industrial HiVision displays the device name, proceed as follows:

- ☐ Delete the device from Industrial HiVision.
- ☐ Open the “Device/Port Names“ dialog for the desired results.
- ☐ Rescan the network for the device.

Determining device names

Request DNS	when it detects a new device, Industrial HiVision determines the device name from the Domain Name Server.
Request Now	For the devices already detected, Industrial HiVision determines the device name from the Domain Name Server. This procedure can take some time.
Use Name of Hosts File	For the devices already detected, Industrial HiVision reads the device name from the hosts file. The hosts file is the `hosts.txt` text file in the `config` subdirectory of the installation directory. The hosts file contains a row for each device with the IP address and the name, separated by a tab.
Read Now	For the devices already detected, Industrial HiVision reads the device name from the hosts file.

Industrial HiVision writes the host name and the DNS name into the MAC/IP address assignment table (see on page 412 “MAC/IP List”).

“Set Device Name“
This frame enables you to choose which name Industrial HiVision puts into the name field of the device property for the device. Industrial HiVision displays this name in the folder frame and in the detail display. Possible parameters are as follows:
– “DNS Name“
– “Host Name“
– “System Name“
– “Location“
– “Contact“

By selecting it and clicking on the arrow buttons, you move the potential names between the “Possible Parameters“ and “Used Parameters“ tables. Industrial HiVision takes the name at the top in the “Used Parameters“ table. If the relevant entry is empty for a device, Industrial HiVision takes the name in the next position. If Industrial HiVision does not find an entry for the device, then Industrial HiVision takes the management IP address of the device.

“Port Name“
The “Set Port Name“ function allows you to take the port name entered in the device into the name field of the port properties, as long as the port names are entered in the device. Industrial HiVision displays these names in the folder frame and in the detail display. If there is no setting here, Industrial HiVision displays the IP address for devices and the port number for ports.

Note: When it detects a device/port, Industrial HiVision takes the name selection that is set. If you subsequently change this selection, it becomes effective after you have reset the device/port name. To do this, you select the relevant devices and right-click “Set Device and Port Names“.

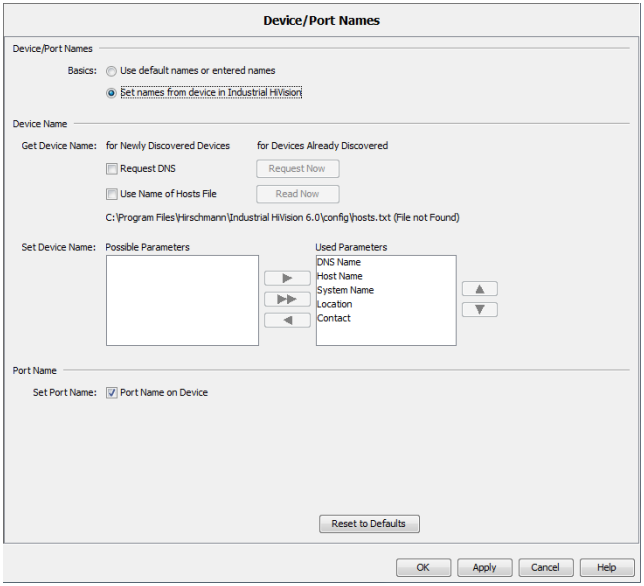


Figure 98: Assignment of device and port names

Load/Save

This dialog allows you to enter the following parameters:
– Enter the IP address of a tftp server available in the network
– File name with path
– URLs.
Industrial HiVision automatically enters this into the dialogs in which you perform file transfer actions for example, loading/saving configurations in the MultiConfig™ dialog.
This spares you having to enter the URL and the file name multiple times when you call up the “MultiConfig™” dialog.

Placeholder	Meaning
$INSTALL	Installation folder of Industrial HiVision on the network management station.
$TFTP_SERVER	IP address of the tftp server that you entered in the `Configuration > Preferences > Advanced > Load/Save` dialog.
$IP_ADDRESS	IP address of the device from which Industrial HiVision reads the configuration, or onto which Industrial HiVision writes the configuration. Industrial HiVision applies the IP addresses from the table of the Object frame.
$SYSTEM_NAME	System name of the device from which Industrial HiVision reads the configuration, or onto which Industrial HiVision writes the configuration.
$CURRENT_DATE	Current date of the network management station.
$CURRENT_TIME	Current time of the network management station.
$EXTENSION	File name extension: `cfg` for binary file `cli` for script file `html` for HTML file

Table 48: Placeholders supported

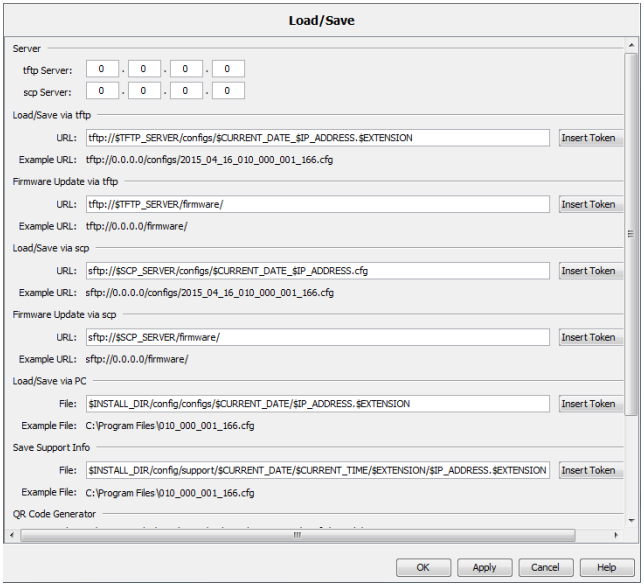


Figure 99: `Configuration > Preferences > Advanced > Load/Save`

1:1 NAT Devices

This dialog allows you to use Industrial HiVision to manage and monitor devices behind a 1:1 NAT router.
For Industrial HiVision to be able to detect the devices behind the 1:1 NAT routers, you enter the MAC addresses of the ports (of the 1:1 NAT routers) that are connected to the network management station in this list. You will find the port MAC address in the properties dialog of the 1:1 NAT router, on the “MAC/IP Addresses“ tab.

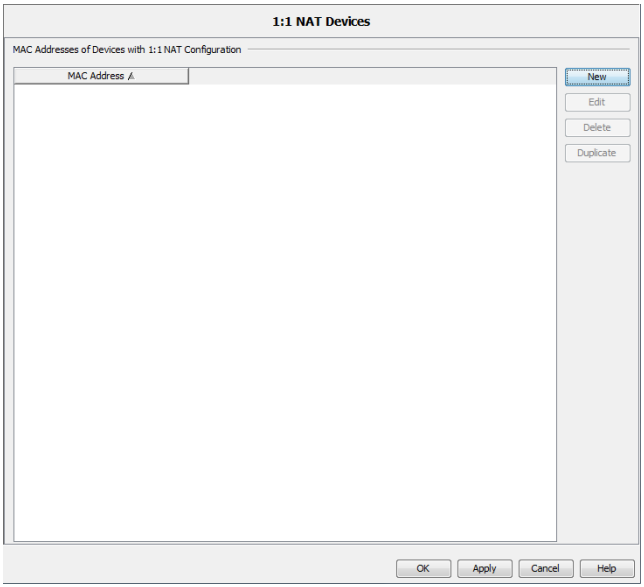


Figure 100: `Configuration > Preferences > Advanced > 1:1 NAT Devices`

PoE

- “Automate Power Limit“
  The “Automate Power Limit“ function and the “Power Limit“ function enable the device to send traps and the application to send warnings, about the power consumption at port level.
  To set the “Automate Power Limit“ function, configure the overhead percentage, which influences the “Power Limit“ value displayed in the “PoE“ tab, “Module / Port“ view.
  The overhead percentage is a configurable parameter, used in the formula, “Power Limit“ = “Max Cons“ + overhead percentage. To calculate the overhead percentage use the formula, overhead percentage = “Max Cons“ x “Automate Power Limit“. The default “Automate Power Limit“ value is 10. You configure the overhead percentage in the `Preferences > Advanced > PoE > Automate Power Limit` dialog.

To configure the overhead percentage on the PoE ports, proceed as follows:

☐ Click the “Preferences“ button.
☐ Open the `Advanced > PoE` dialog.
☐ Specify the PoE overhead in the “Automate Power Limit“ field.
☐ Click the “OK“ button.

To specify the “Power Limit“ value, see “Power Limit” on page 410

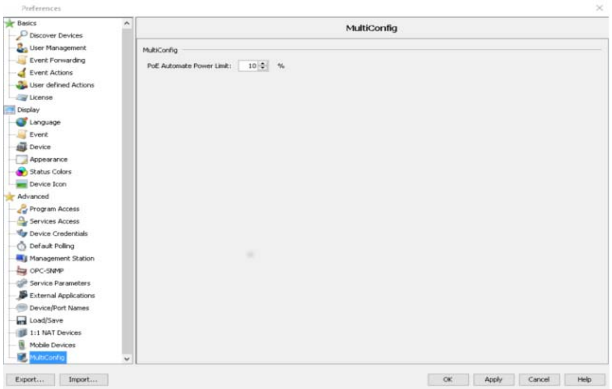


Figure 101: `Preferences > Advanced > PoE`

Scheduler

The “Scheduler“ dialog helps you delete previously saved device configuration files. Deleting the previously saved device configuration files frees up space on your hard drive. You use the dialog to configure the global settings of the “Scheduler“ function. Industrial HiVision applies the settings to every “Save Device Configuration“ task.

Whenever the “Scheduler“ function triggers a “Save Device Configuration“ event, Industrial HiVision examines the previously saved configuration files for the device. When you mark the “Delete 'Save Device Configuration' files“ checkbox, the “Scheduler“ function deletes the configuration files that are older than the value you configured in the “Older than“ field.

The “Scheduler“ function deletes only files with a valid name. A valid contains the IP address followed by a time stamp, for example, 100_100_100_100-2022-11-10_09-04. Any information after the time stamp is ignored.

The “Scheduler“ function identifies the device files and path based on the information in the `Configuration > Scheduler` dialog.

The prerequisite for this function is that you configure a “Save Device Configuration“ task in the `Configuration > Scheduler` dialog, see “Scheduler” on page 314.

- The “Delete 'Save Device Configuration' files“ checkbox, enables and disables deletion of old device files. In the default setting, the checkbox is unmarked.
- The “Older than“ field, lets you set the expiration interval. The default setting is `90` Days.The possible values are: `1..9999`.

To delete expired configuration files, proceed as follows:

- ☐ Mark the “Delete 'Save Device Configuration' files“ checkbox.
- ☐ Enter the expiration interval, in days, that you wish to delete old device configuration files, in the “Older than“ field.

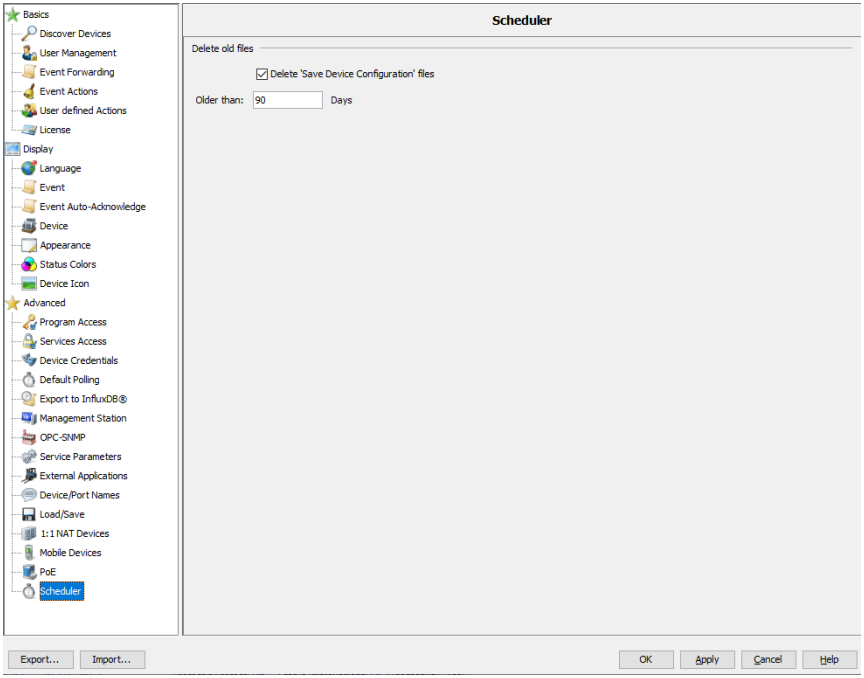


Figure 102: `Preferences > Advanced > Scheduler`

8.5 Status Configuration

This dialog allows you to configure the status of a component property for the devices of a device class across the device boundaries or for every devices simultaneously.

The dialog displays a table of the device classes and their possible properties.

☐ To display the properties of every device class, mark “Combine Entries“ checkbox. To display the property per device class, unmark the “Combine Entries“ checkbox.

☐ To specify the values of the property, double-click on a row in the table.

Industrial HiVision opens the corresponding “Status Configuration“ dialog.

☐ Assign the desired status to the values and click the “OK“ button.

☐ To change the properties of those devices that you previously configured individually, mark the “Overwrite all Properties“ checkbox.

Industrial HiVision accepts this “Status Configuration“ for the devices in this class.

This function is useful for example, if you require the highest availability within a HIPER Ring. Then the default setting, “Warning“ is too low for a loss of redundancy functionality. In the “Status Configuration“ dialog, you can use a single step to set the status for “No redundancy” to “Error“ for the devices in a class.

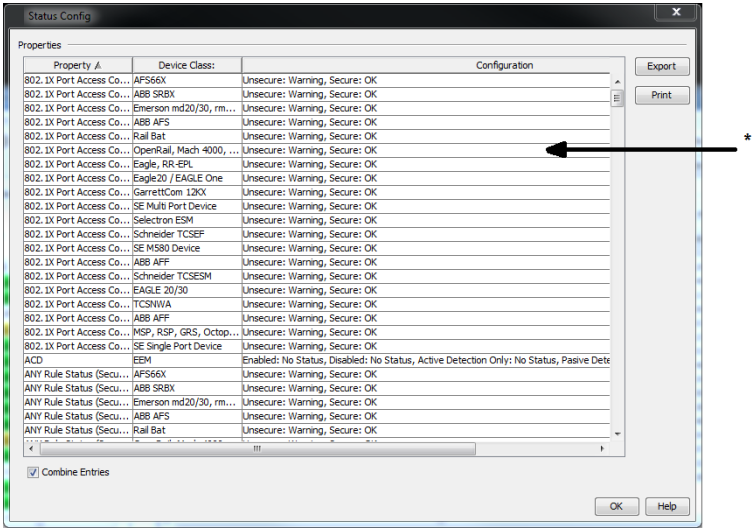


*Figure 103:“Status Configuration“ * Double-click on a row*

8.6 Scan Ranges

This dialog allows you to enter the scan range for a selected folder.

☐ After selecting a folder in the folder frame, or when the detail display is active, you select `Configuration > Scan Ranges` or right-click on `Scan Ranges` in the selection menu.

☐ To enter an IP address range, click the “New“ button. Entering the IP address range consists of the following parameters:
- the first IP address of the query range
- the last IP address of the query range
- the related network mask
- the activation/deactivation of this range for the query
- the name you want to give to the range

Industrial HiVision has already entered the selected folder or the active detail display as the target folder.

The table displays the IP address ranges already created.

☐ To edit an IP address range, select a row in the table and click the “Edit“ button.

☐ To delete a row from the table, select a row in the table and click the “Delete“ button.

☐ To duplicate an IP address range so that you can then modify the copy, select a row in the table and click the “Duplicate“ button.

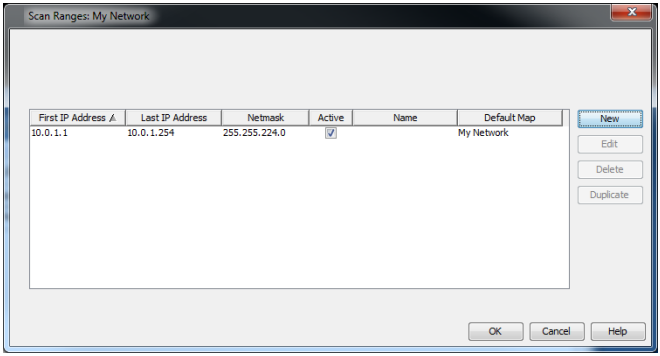


Figure 104:Scan ranges for a folder

Note: Keep in mind that the network masks in this dialog correspond with the network masks within your network, so that the detection executes properly. If the network mask within your network is bigger than the network mask of a scan range, Industrial HiVision skips the highest IP address within the network mask of the scan range during the scan network, because this IP address is a broadcast address.
If the network mask within your network is smaller than the network mask of a scan range, Industrial HiVision scans the highest IP address within the network mask of the network. Because this IP address is a broadcast address, every device replies and Industrial HiVision recognizes a device that does not exist.

8.7 User defined Properties

This dialog allows you to enhance and monitor the properties of any SNMP-capable devices in Industrial HiVision (see on page 225 “Description of user-defined properties”).

☐ In the menu bar, select `Configuration > User defined Properties` to open the “User defined Properties“ dialog.

You can edit, delete or duplicate a selected user-defined property. When you select a user-defined property, the “Delete“ button remains grayed-out if this property is assigned to a higher-level property.

8.7.1 Creating a new user-defined property

You can find an application example in the chapter “Setting up the network monitoring” (see on page 225 “Application example for user-defined properties”).

Name	Meaning
Name	A freely-selectable, unique name for this property starting with “UserDef_”, e.g. “UserDef_ICMP-Message”.
Label	A freely-selectable name that Industrial HiVision uses for the display in the user interface.
Icon	A pixel file is selected that Industrial HiVision displays as a symbol for the property in the user interface.
Parent Property	The higher-level property of the new property for example, the property “Speed” belongs to the higher-level property “Port”.
MIB Variable/OID	MIB variable/OID (object identification) that you can select by clicking on the three dots in the MIB browser.
Instance	Assignment of the MIB variants to a device detail, e.g. “0” for the time. Alternatively, Industrial HiVision determines the type itself for example, “Module Number”.

Table 49: “New Entry” dialog for a user-defined property.

Name	Meaning
Type	Industrial HiVision selects the type for example, a MAC address or an integer, automatically if Industrial HiVision can determine the type.
Mapping	Assignment of a numerical value to a meaning for example, “0 = false” or “1 = true”. Industrial HiVision determines this value from the MIB.
Factor	Factor for converting a unit for example, Celsius to Fahrenheit.
Offset	Offset for converting a unit for example, Celsius to Fahrenheit.

Table 49: “New Entry” dialog for a user-defined property.

8.8 MultiConfig™

The multi-configuration function (MultiConfig™) allows you to perform configurations on the device and in Industrial HiVision for:

- one or more devices
- one or more device properties, also device overlapping
- one or more device details, also device overlapping

You can find more information with application examples in chapter “Configuring the network” on page 157.

8.8.1 Power Limit

To configure the “Power Limit“ function on the “PoE“ ports, proceed as follows:

- ☐ Select the PoE ports in your network that need the same threshold.
- ☐ Right-click a selected port. A drop-down list opens.
- ☐ Select the “MultiConfig™“ option.
- ☐ Open the `Device Settings > PoE > Automate Power Limit` dialog.
- ☐ To configure the “Power Limit“ function, unmark the “Automate Power Limit“ checkbox.
- ☐ Specify the necessary value, in the “Power Limit“ field. When the power is above this threshold, the device sends a trap and the application sends a warning.
- ☐ To automate the “Power Limit“, mark the “Automate Power Limit“ checkbox.
- ☐ Click the “Write“ button.
- ☐ Click the “Close“ button.

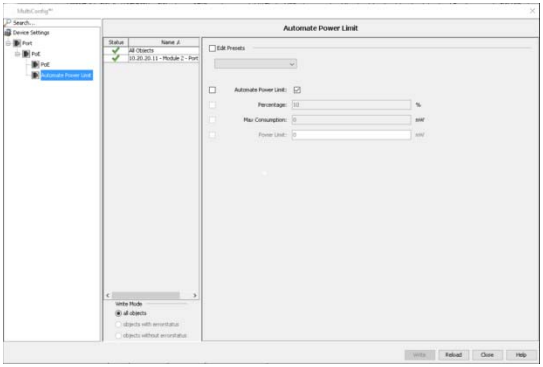


Figure 105: `Configuration > MultiConfig™ > Device Settings > PoE > Power Limit`

8.9 MAC/IP List

8.9.1 MAC/IP Addresses

This dialog displays a list of the IP addresses detected by Industrial HiVision and their related MAC addresses. The list contains:

Designation	Meaning
MAC Address	
IP Address	
Netmask	
Host Name	Host name from the /config/hosts.txt file in the installation directory if: – the file exists – there is an entry – the determination of a device name is activated in the basic settings Otherwise, the field remains empty.
DNS Name	Name from the Domain Name Service
Port No	Port number of the protocol.
Port	Device port
Management	Industrial HiVision communicates with the management of the device by means of the IP address in this row.
User Generated	The device in this row was generated by the user. Industrial HiVision has not detected this device yet.
Router Entry	The IP address in this row comes from the routing table of the device.

With the “Export“ you can save the complete list as:

- PDF file
- HTML file
- CSV file (see on page 457 “CSV export”)

With the “Print“ button you can print the complete list. Industrial HiVision creates a temporary PDF file of the content of the list and opens this PDF file in the PDF display program for example, Acrobat Reader, that is installed on your management station.

8.9.2 MAC/IP Address Pair Security

This dialog lets you monitor the assignment of MAC addresses to IP addresses and allows you to detect IP address duplicates.
Industrial HiVision is familiar with the following types of table entries.

- “Existent“
  This entry comes from an existing and discovered device in the network. If you remove this device from the topology, then Industrial HiVision removes this device from the list.
  Industrial HiVision includes this entry in the event examination.
- “User Generated“
  A user created or edited this entry at this point. This entry stays in the list until the user manually deletes it from the list.
  Industrial HiVision includes this entry in the event examination.
- “Excluded“
  A user created or edited this entry at this point. This entry stays in the list until the users manually deletes it from the list.
  Industrial HiVision excludes this entry from the event examination.

The “Display“ pull down list allows you to filter the table contents according to type.

☐ To enable monitoring, mark the “Configure Schedule for Checking“ checkbox.
As soon as you leave the dialog using the button, Industrial HiVision opens the “Scheduler“ dialog. This is where you specify the monitoring criteria.
See “Scheduler” on page 314.

8.10 Refresh

The “Refresh“ dialog enables you to have Industrial HiVision read values from properties of a previously selected device, folder or property itself. After Industrial HiVision has read in the values, Industrial HiVision refreshes the display.

- In edit mode, when you update a device, or folder within a device, Industrial HiVision reads the existing properties within and below the respective device or folder.
  Thus, for example, you can make a module visible in Industrial HiVision after adding the module to the hardware.
- In Run mode, when a device or folder within a device is updated Industrial HiVision reads in exclusively the existing properties within the respective device or folder.

When updating a property, Industrial HiVision reads in the values of the property.

8.11 IP Configuration

This dialog enables you to configure the IP parameters of a device detected by HiDiscovery V1 without an IP address, or to change IP parameters already configured.

You open the dialog for the IP configuration by right-clicking on the device and selecting “IP Configuration“.

When you open the dialog, Industrial HiVision queries the device using the HiDiscovery V1 protocol. If the query is successful, Industrial HiVision displays the parameters of the device and the “Signal“ button. If the device does not respond to the HiDiscovery V1 query, then Industrial HiVision queries the device using SNMP. If the SNMP query is successful, Industrial HiVision displays the parameters of the device.

- You click the “Signal“ button to activate the flashing LEDs on the device for the identification of the device. Click the “Signal“ button again to deactivate the flashing.
  Prerequisites for this function:
  - The device has HiDiscovery V1 activated
  - You have chosen the network interface card for this network in the `Configuration > Preferences > Advanced > Management Station` dialog under “Default Network Card“ (HiDiscovery V1).
- You can enter a name for the device, in the “Name“ field.
- You can assign a new IP address to the device, in the “IP address” field.
- You can assign a new network mask to the device, in the “Network Mask” field.
- You can assign a new gateway IP address to the device, in the “Gateway” field.
- If you click once on the “Default Values“ button, then Industrial HiVision enters the default values from “Management Station” on page 385 in the IP configuration fields.

If you click the “OK“ button, then Industrial HiVision transfers the name and the IP configuration to the device.

To close the dialog and keep the original entries, click the “Cancel“ button.

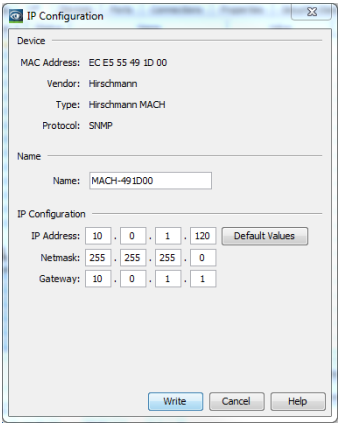


Figure 106:IP configuration of a device

8.12 SNMP V1 Trap Destination

To open the dialog for the trap destination, you right-click on the device and select “SNMP V1 Trap Destination“.

When the dialog is opened, Industrial HiVision queries the trap settings of the device and displays whether the device sends traps to the IP address displayed.

- ☐ If you want the device to send traps when defined events occur, then mark the “Send Traps“ checkbox.
- ☐ You select the IP address of your network management station, on which you are operating Industrial HiVision, in the “to IP Address“ pull-down list.
- ☐ If you want this trap configuration to be saved in the permanent memory on the device, mark the “Save Config on Device“ checkbox.

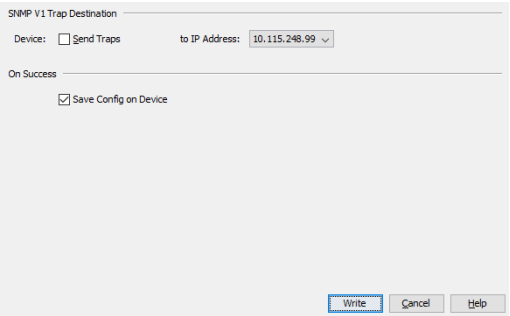


Figure 107:“SNMP V1 Trap Destination“ of a device

Note: If your Windows firewall is activated and no Windows Trap Service is installed, the firewall can block you from receiving traps. However, if you still want to receive traps, you add the `/services/HiVisionKernelDb.exe`.exe file in the Industrial HiVision installation directory to the firewall settings as an executable file.

The Windows Trap Service is installed if you find "SNMP Trap Connection: Trap Service" under `Help > Kernel Info` in Industrial HiVision.
You can configure the Windows firewall under Start> Settings> Control Panel> Windows Firewall on the Exceptions tab. Click “Program” to select the`/services/HiVisionKernelDb.exe` file in the Industrial HiVision installation directory.

8.13 Tools

In the “Tools“ menu you can find various tools allowing you to access devices in your network using Ping, graphical user interface, CLI, SNMP browser or the HiDiscovery V1 Scan.

8.13.1 Dashboard

The Industrial HiVision “Dashboard“ is a valuable fault-finding tool which allows an administrator to view the network statistics and useful information about the performance of the network in real time.

Industrial HiVision allows you to create multiple dashboards with various information, then preview the dashboards as a slide show. The function also allows you to save and load the dashboard layouts.

The main window contains a time slider. The time slider allows you to adjust how long the slide show displays each page.

When you close the Industrial HiVision application, the application saves the size and position of the dashboard. The application also saves other active dashboard options such as the full screen mode, timer slider status, and the play or pause status.

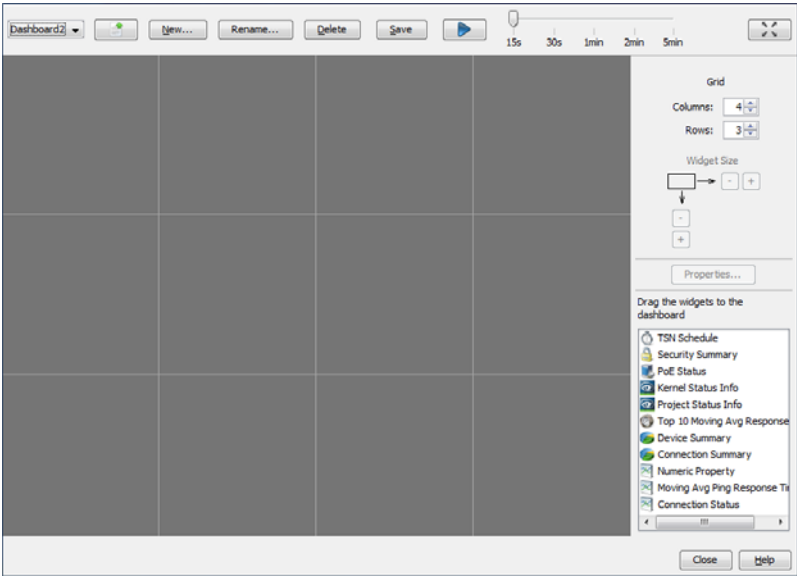


Figure 108:Industrial HiVision Dashboard

Note: If the dashboard does not display the “New“, “Delete“, and “Save“ buttons, then click the “Edit Mode“ button on the Industrial HiVision tool bar.

Widget Display and Configuration

Industrial HiVision allows you to customize the dashboards to suite your requirements. Using the drag and drop function you can specify the type and position of the widgets that a dashboard displays. You can also specify the number of rows and columns of cells for each dashboard.

The background color of the widget represents the worst state displayed in the widget. The background colors indicate the same statuses as in the Graphical User Interface (GUI) of Industrial HiVision. The user can specify the background colors (see “Status Colors” on page 365).

Widget Size

The dashboard allows you to increase or decrease the size of widgets.

To increase the size of a widget, verify that you have cells free on the right or below the widget that you wish to enlarge. If there are no free cells available, then add the required number of cells using the “Grid“ buttons.

Highlight the widget you wish to enlarge. Using the “Widget Size“ plus “+” button increases the size of the widget. The size of the widget increases one cell each time you click the plus “+” button.

Properties Button

Some widgets allow you to configure which parameters to monitor. To specify which parameters the widget monitors click the “Properties“ button, then enter the values in the “Parameters“ dialog. The widgets also allow you to drag parameters from various tabs in the GUI or the folder frame and drop them into the widget.

The following widgets allow you to specify parameters to monitor:
- “Connection Status“
- “Moving Avg Ping Response Time“
- “Numeric Property“
- “Top 10 Moving Avg Response Time“ (no drag and drop)

Viewing Modes

Industrial HiVision allows you to view a slide show of the dashboard pages using the following methods.
- When you click the “Full Screen” button , the dashboard changes to the full screen mode and the slide show is in the “Pause” mode.
- You can also open the slide show using the “Play” button . If you open the slide show using the “Play” button, then the dashboard changes to the full screen mode and the slide show begins to display the pages of the current user.

In the “Full Screen” mode the dashboard also has a tool bar containing the following control functions.

- To stop the slide show at the current page, click the “Pause” button .
- To restart the slide show, click the “Play” button .
- If you wish to open a specific page, then you can select the page from the pull down list.

Note: To display the tool bar, move the mouse to the top of the screen.

To exit the full screen mode, click the “Restore” button or press the “Esc” button on the keyboard.

Renaming

The dashboard function allows you to change the name of existing pages.

To change the name of an existing page, use the following work steps:

- ☐ Click the “Rename“ button.
- ☐ Enter the new name in the “Dashboard Name“ field.
- ☐ Click the “OK“ button.

Dashboard Order

When you have multiple dashboards Industrial HiVision allows you to display the dashboards in any order. When you have multiple dashboards or the selected dashboard is not at the top of the list, the move up button is active. The move up button moves the selected dashboard one step up.

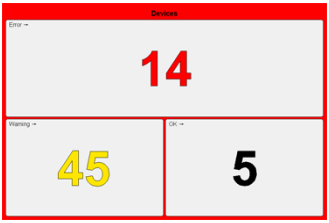
Device Summary Widget

The widget displays a summary of the devices contained in the entire project. The summary displays devices according to the state of the device. The widget only displays the state of managed and licensed devices.

Industrial HiVision includes the device and copies of devices in the summary. When you add a copy of a device to Industrial HiVision, the “Device Summary“ widget counts the device twice. The reason that the widget counts the device twice is because the status of the copy can differ from the original. The “Device Summary“ widget excludes links from the count.

The widget displays the state of the device regardless of whether the state of the device is confirmed or not (see “Acknowledge events” on page 92).

After each name in every field is an arrow. The arrow displays the trend of the field since the last update. For example: the “Warning“ field in the previous scan displayed 3, the current scan returns 2. The field displays a down arrow in this case.

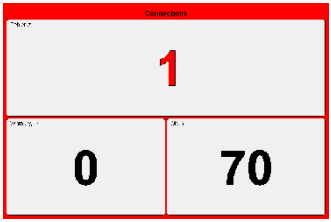


Connection Summary Widget

The widget displays a summary of the connections contained in the entire project. The summary displays connections according to the state of the connection.

The widget displays the state of the connections regardless of whether the state is confirmed or not (see “Acknowledge events” on page 92).

The arrow displays the trend of the field since the last update. For example, the “Warning“ field in the previous scan displayed 3, the current scan returns 2. In this case, the field displays a down arrow.



Connection Status Widget

You can add multiple “Connection Status“ widgets to the dashboard. The “Connection Status“ widget displays the link state and load of selectable connections as graphs. The graphs display the load values and link state in separate diagrams. The widget frame displays the color of the current connection status. The widget retrieves the connection status from the Industrial HiVision database. If Industrial HiVision detects an error on the connection for any reason, then the widget frame displays the color specified for a detected error.

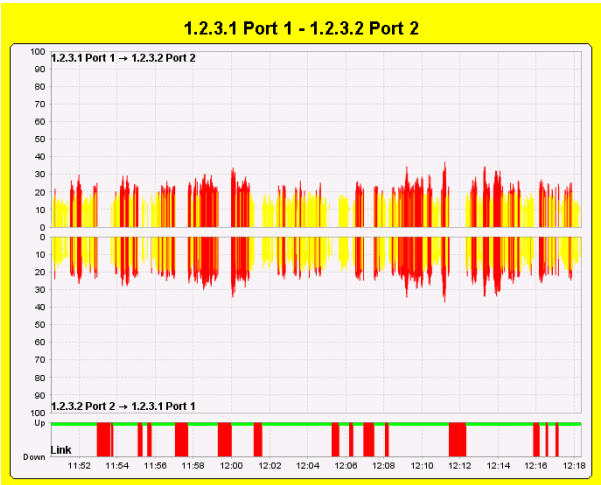


Figure 109:“Connection Status“ widget with “Top to bottom“ function activated.

When you create a new widget, the widget is in the unconfigured state. For example, you have not yet associated the widget with a connection from a project. In this state the widget displays empty diagrams.

To configure the widget, use the following steps:

- ☐ Drag and drop the widget to a cell in the dashboard.
- ☐ To open the “Widget Parameters“ dialog, click the “Properties“ button on the right side of the dashboard.
- ☐ Enter the desired history duration, in the “History Size“ field.
  The “History Size“ range is from 1 min to 2 h. Default value is 30 min.
- ☐ Using the pull-down list, select the unit of measure.
- ☐ Assign a connection to the widget. In the “Connection“ field highlight a connection.
- ☐ Click the “OK“ button.

Note: If you select an item that is not a connection, the widget displays “Widget Configuration Error“.

The widget collects the “In Load“ and “Out Load“ data from the server and displays it on a history graph. The history graph slowly scrolls across the widget allowing you to read the information. The widget displays the graph until you close the widget or specify a different connection.

The “Widget Parameters“ dialog also allows you to configure the visual aspects of the widget. To configure the widget to display the lower “Out Load“ diagram directly underneath the upper “In Load“ diagram, mark the “Top to bottom“ checkbox. To change the load graph from a solid bar type to a stacked bar type, mark the “Stacked“ checkbox. Each bar displays the status of the data set according to the diagram type for example, solid or stacked bars. The widget stores and displays the status configuration of each data set.

Note: The solid bar diagram draws the bar using the color that represents the status of the value at that time. The stacked bar diagram displays the parts of the bar that are below, between or above the thresholds in a different color. This makes it possible to display changes in the status configuration.

The widget uses the same thresholds configured in the graphical user interface. See “Properties of a connection” on page 292.

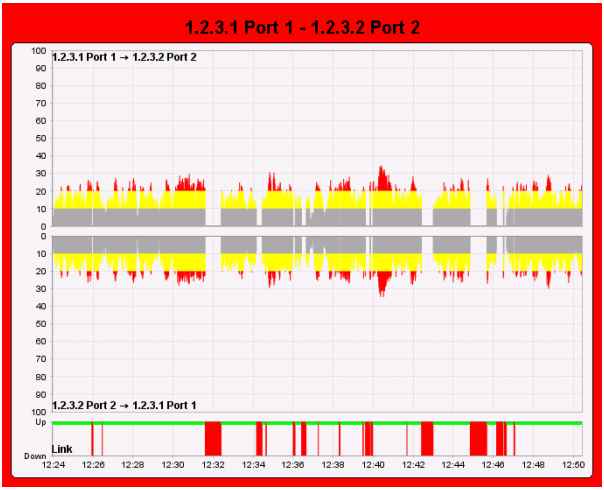


Figure 110:“Connection Status“ widget with “Top to bottom“ and “Stacked“ functions activated.

The widget attempts to determine the load in both directions using various means. The widget obtains the values from the database in the following order:

- “In Load“ property values from both end ports of the connection. The legend displays the direction of the traffic.
- If one side does not provide an “In Load“ property, then the widget uses the “Out Load“ property of the opposite side. The legend displays the direction of the traffic.
- If only one side of the connection is a port, then the widget uses the “In Load“ and “Out Load“ of this port. The legend displays the name of the end point with either “In Load“ or “Out Load“ appended.
- If the direction of traffic cannot be determined, the diagram and the legend remains empty.

If you change the connection associated with a widget, then the widget reflects the changes immediately. If you delete the connection, then the widget displays “Widget Configuration Error“.

Kernel Status Info Widget

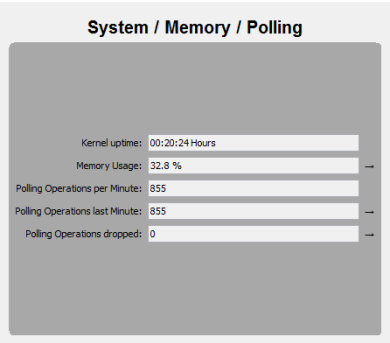
The “Kernel Status Info“ widget displays information about the Industrial HiVision kernel.

Additional information about the Industrial HiVision kernel is located in a following chapter, See “Kernel Info” on page 449.

The widget displays the following information:

- “Kernel uptime“
  The elapse time since Industrial HiVision was started.
- “Memory Usage“
  The percent of memory that the services are using. Industrial HiVision calculates the percent of memory as follows:
  `percent = actual memory used/reserved memory`
- “Polling Operations per Minute“
  The specified number of operations that the kernel can perform in a minute.
- “Polling Operations last Minute“
  The number of operations that the kernel was able to perform in the last minute.
- “Polling Operations dropped“
  The number of operations that the services dropped in the last minute. You can influence the number of polling operations dropped by changing the number of polling operations monitored or changing the polling interval.

Note: For further information about configuring the parameters that the kernel polls See “Monitor” on page 306.



Security Summary Widget

The “Security Summary“ widget displays the security relevant parameters.

The “Vulnerable Devices“ field displays the number of devices that are vulnerable to attack. Vulnerable devices have at least 1 function enabled that is recommended to be disabled, such as the http or SNMP v1/v2 protocols. The widget also counts devices which have the security functions disabled. The number displayed in the widget represents the number of devices in your project with a security status worse than OK.

The Industrial HiVision GUI “Security Status“ tab identifies which devices the widget has included in the results and the security risks. To decrease the number of devices in the count and increase network security, disable/enable the functions identified in the “Security Status“ tab. You can also use the MultiConfig™ “Security Lockdown“ function.

The “Rogue Devices“ field displays the number of devices in the rogue device map See “Detecting rogue devices” on page 212. When the number of rogue devices is more than `0`, the widget displays the color that you specified as „Warning“.

Note: The widget displays a warning triangle to the right of the “Rogue Devices“ field. The triangle is to remind you to activate the function. The widget hides the triangle after you activate the “Rogue Device Detection“ function.

The “Config. Signature Changes“ field displays the number of devices with a configuration change. The field counts every change even when the changes were returned to the original value.

In order for the widget to display the properties, specify a reference value and configure status calculation as follows:

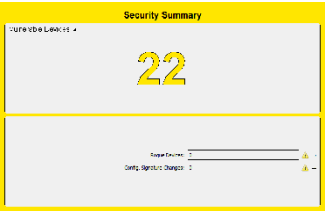
- ☐ Open the “Properties“ tab in the Industrial HiVision Graphical User Interface (GUI).
- ☐ Open the “Property:“ drop down list, select “Configuration Signature“.
- ☐ Highlight the device or devices in the table without an active “Configuration Signature“.
  The devices with an active “Configuration Signature“ have a check mark in the “Status“ column. You can filter the table to locate the devices that require activation. To filter the table, click on the “Status“ column header until the table displays the entries at the top.

- ☐ Open the “Status Config“ dialog using `Configuration >` MultiConfig™ `> Status Config`.
- ☐ Mark the “Set current to reference“ checkbox.
- ☐ Mark the “Value is Reference Value“ checkbox.
- ☐ Open the “Value is Reference Value“ drop down list, select “OK”.
- ☐ Mark the “Other Value“ checkbox.
- ☐ Open the “Other Value“ pull-down list, select “Warning“ or “Error“.
- ☐ To save the changes, click the “Write“ button.

Note: The widget displays a warning triangle to the right of the “Config. Signature Changes“ field. The triangle is to remind you to configure the function. The triangle is hidden after you configure the references for every device.

The status of the “Config. Signature Changes“ field is either OK for the value zero or the worst status of the configured “Configuration Signature“ properties.

The arrows indicate the trends of the individual fields.



Numeric Property Widget

The “Numeric Property“ Widget allows you to track the status of parameters containing numeric values. The widget allows you to track up to 10 numeric parameters.

The procedure for using the “Widget Parameters“ dialog to enter the parameters that you want to monitor is described in the following steps:

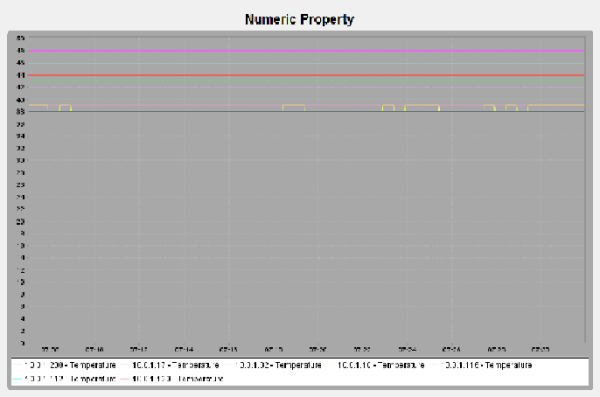
- ☐ To open the “Widget Parameters“ dialog, click the “Properties“ button.
- ☐ Specify the length of time that you want to monitor the devices in the “History Size“ field.
  Default: `30`

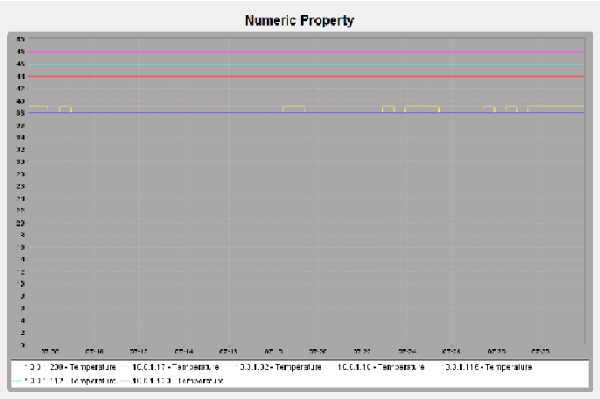
- ☐ Specify the “History Size“ units of measure for the length of time that you want to monitor the parameters.
  Default: “Minutes“
- ☐ Select up to `10` parameters from the project tree.
- ☐ You can specify a different name for the widget in the “Title“ field.
- ☐ Click the “OK“ button.

The following list contains some of the numerical parameters that the widget can monitor:

- ▶ “Ports“:
  “In Load“
  “Out Load“
  “Speed“
- ▶ Agent:
  “Number of Users“
- ▶ Protocol:
  “Moving Avg Response Time“
  “Avg Response Time“
  “Min Response Time“
  “Max Response Time“
  “Std. Deviation“
  “Message Loss“

Note: It is possible that 2 devices have the same value for a parameter for example, devices 10.0.1.10, 10.0.1.17 and 10.0.1.200 have a temperature of 38° and 39°. In this case, one trace covers the other. See the blue, yellow and orange traces in the “Numeric Property“ figure below.





Moving Avg Ping Response Time Widget

The “Moving Avg Ping Response Time“ widget allows you to display the response time of a ping request for up to 10 devices. You can enter the devices using either drag and drop or the “Widget Parameters“ dialog.

The procedure for using the “Widget Parameters“ dialog to enter the devices that you want to monitor is described in the following steps:

☐ To open the “Widget Parameters“ dialog, click the “Properties“ button.

☐ Specify the length of time that you want to monitor the devices in the “History Size“ field.
Default: `30`

- ☐ Specify the “History Size“ units of measure for the length of time that you want to monitor the devices.
  Default: “Minutes“
- ☐ Select up to 10 devices from the project tree.
- ☐ Click “OK“.

The procedure for using the drag and drop method to enter the devices that you want to monitor is described in the following steps:

- ☐ Open the GUI Map tab.
- ☐ Highlight the device or devices you want to monitor.
- ☐ Drag and drop the highlighted devices in the “Moving Avg Ping Response Time“ widget.

Note: Each time you select new devices to monitor, the widget replaces the current devices with the newly selected devices.

For further information about ICMP moving averages See “Service Parameters” on page 389.

Top 10 Moving Avg Response Time Widget

The widget displays the moving average response time of up to 10 devices. The devices with the higher moving average response time are displayed at the top of the chart.

To configure the widget, open the “Widget Parameters“ dialog using the “Properties“ button. The dialog allows you to specify which protocol the widget displays. You can select from the following protocols using the drop down list:

- `Ping` (default setting)
- `SMNP V1`
- `SMNP V3`

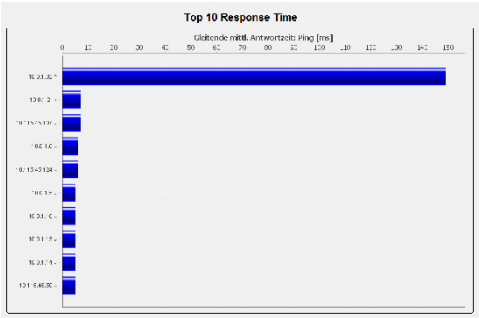
The widget displays a trend arrow next to the IP address of each device. The trend arrow indicates the movement in position of a device, with reference to the other devices displayed in the widget, since the last poll.

The information provided in the widget helps you to plan for optimal performance in your network. For example, the widget displays which device has a high average response time. A high average response time can cause a bottle neck in your network. If a device with a high response time is in the middle of your network, then the device can effect the other devices in your network. Replacing the slow device allows the data stream to be transmitted unhindered.

The following list contains some possible causes of high response times:

- Device is overwhelmed with data being sent to the CPU.
  Receiving and forwarding data is the primary task of a network device. Processing management requests are secondary tasks.
- The path to the device is slow.
  - Slow connection
  - Slow connection of neighbor
  - Old fiber or Ethernet cable

Note: When you configure the widget for the first time, there is a possibility that the widget displays high response times. In this case, allow the display to stabilize before taking action. If after `1` minute the average response time for a device remains high, then consider taking action.



PoE Status

The “PoE Status“ widget allows you to monitor the status of the PoE devices in your network.

The widget displays the sum of the warnings found in the “PoE“ tab for the following parameters:

- “Class 0 Detected“
  Displays the sum of the ports on which the device has detected that a class 0 device is connected.
- “Device“
  Displays the sum of the devices on which the “Device Limit“ is exceeded.
- “Module“
  Displays the sum of the modules on which the “Module Limit“ is exceeded.
- “Port“
  Displays the sum of the ports on which the “Port Limit“ is exceeded.

The arrow displays the trend of the field since the last update. For example, the “Class 0 Detected“ field in the previous scan displayed 3, the current scan returns 2. In this case, the field displays a down arrow.

If you disable the “PoE Class 0 Detection“ function on ports in the “PoE“ tab, then the widget displays a warning triangle next to the “Class 0 Detected“ field. Ports on which you disabled the detection function are not included in the number entered in the “Class 0 Detected“ field.

Note: If the widget displays a warning triangle next to a field, then there can be more items effected than the number indicates.

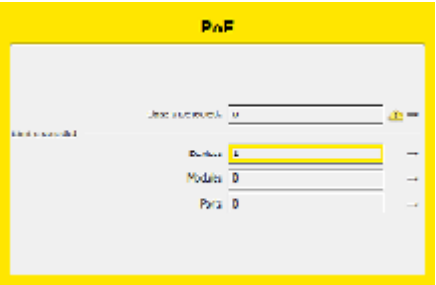


Figure 111:“PoE Status“ Widget

TSN Schedule Widget

The widget displays the TSN cycle time, and gate control of a port in a table. The table displays a row for each “Priority“ class. The columns left of the “Priority“ class display the status of each gate.
A gate is a period of time during which the port is either opened or closed for the priority class. An open gate forwards the traffic of the priority class, and a closed gate blocks the priority class traffic. A green cell displays an open gate and a gray cell displays a closed gate. The width of the column displays the length of time that the gate is either opened or closed in relation to the cycle time.
To configure the widget, click the “Properties“ button. Industrial HiVision opens the “Widget Parameters“ dialog. The dialog allows you to specify which TSN compatible port the widget displays.

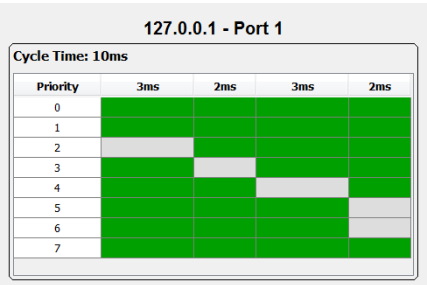


Figure 112:“TSN Schedule“ Widget

8.13.2 Web Interface

The “Web Interface“ tool enables you to open, from the Industrial HiVision interface, the Web-based interface of the device selected in the window in the web browser.

8.13.3 Device Configuration

The “Device Configuration“ tool allows you to open, from the Industrial HiVision the Web-based interface of the device selected in the window, as a Java application. Here, Industrial HiVision uses the login name and the password from the SNMP configuration settings (see on page 377 “Device Credentials”). Thus, Industrial HiVision spares you having to login and you go directly to the start page of the device.

The following series of devices support this function:

- MACH 4000
- MACH 1000
- MACH 100
- GREYHOUND
- PowerMICE
- MS20/MS30
- MSP
- RS20/RS30/RS40
- RSP/RSPS/RSPL
- RSR20/RSR30
- RED
- EES20/EES25
- OCTOPUS
- EAGLE 20/30/40
- Magnum 12KX
- TCSESM
- TCSESM-E
- TCSG
- TCSN
- TCSEFEC
- MCSESM
- MCSESP
- ESM 801-TG
- ESM 802-TG
- ERT
- AFF650
- AFS650/655
- AFS66x
- AFS670/675
- AFS677
- AFR677

Note: Industrial HiVision allows you to use the graphical user interface of Hirschmann products with the “Device Configuration“ function independent of other applications, such as a browser or an installed Java environment. Hirschmann has developed Industrial HiVision as an application that enables you to use the graphical user interface easily with the “Device Configuration“ function in a closed network.
When Industrial HiVision sets up a secure connection with HTTP or SSH, Industrial HiVision does not check the identity of the device with which Industrial HiVision is connecting. Additionally, Industrial HiVision does not display the identity of the device to the user. Someone attacking the network could take advantage of this omission of a check to access sensitive information.
Recommended actions use Industrial HiVision in a closed network. Do not use the “Device Configuration“ function and MultiConfig™ dialogs that use HTTPS in an open network. Perform an update of Industrial HiVision as soon as a newer version is available.

8.13.4 CLI

The “CLI“ tool allows you to create a connection to the selected device from the Industrial HiVision interface. Industrial HiVision opens its own window. Industrial HiVision automatically checks whether the device allows an SSH session or a Telnet session. Industrial HiVision preferably establishes an SSH session.

Note: Under Linux, the “CLI“ tool requires that Telnet and SSH clients are installed and that the environment variable PATH contains the name of the directory in which the “xterm” program is installed.

8.13.5 SNMP Browser

The “SNMP Browser“ tool enables you to read and write the MIB of a selected device. Industrial HiVision displays the MIB in a new window.

Note: The “SNMP Browser“ is a freely usable additional software. The “SNMP Browser“ is not subject to the system test.

8.13.6 Ping

The “Ping“ tool enables you to send a Ping query to the devices selected in the window. Industrial HiVision opens a separate Ping window.

Note: Under Linux, the “Ping“ tool requires that the environment variable PATH contains the name of the directory in which the “xterm” program is installed.

8.13.7 HiDiscovery Scan

The “HiDiscovery Scan“ lets you discover the devices in the network that support the HiDiscovery V1 protocol, as long as these devices have the HiDiscovery V1 v1 protocol activated.

Note: As far as HiDiscovery V1 is concerned, Industrial HiVision only supports the HiDiscovery V1 v1 protocol.

Example configuration

In this example you scan your network to discover devices which have the HiDiscovery V1 protocol active.

- ☐ Open the `Preferences > Advanced > Management Station` dialog.
- ☐ Select the adapter connected to the network that you wish to scan from the `Network Card Management Station > Default Network Card (HiDiscovery V1)` drop-down list.
- ☐ To save the values in Industrial HiVision and close the dialog, click the “OK“ button.
- ☐ To scan the network, click the “HiDiscovery Scan“ button.

8.13.8 Scan Network

The “Scan Network“ function enables you to detect every device within an IP address range of the network specified see “[Basics]” on page 324. To start a search for new devices, select the “Scan Network“ option from the drop-down list.

The “Scan Network“ tool has a toggle function. The toggle function starts and stops a network scan. If a network scan is in progress, then to stop the current network scan, click the “Scan Network“ button.

8.13.9 Demo Network

The “Demo Network“ program supplied allows you to simulate a network on your computer in order to familiarize yourself with Industrial HiVision without being connected to a network.

☐ To start the simulation of the demo network, select `Tools > Demo Network`.

In the default state, the device discovery is activated by a trap, and Industrial HiVision detects the demo devices. Industrial HiVision displays the demo devices in the “New Devices“ folder. Because the demo network functions without a network connection, the demo network is simulated using the local host interface with the IP address 127.0.0.1 and differentiates the devices through the port numbers: 127.0.0.1:9003, 127.0.0.1:9004, 127.0.0.1:9005. The simulation replicates the following management functions of the devices:

- Topology discovery based on LLDP
- Line interruptions
- Line interruption in the MRP
- Missing power unit
- Network load on device 9010
- Switch signal contact on/off
- Change device temperature

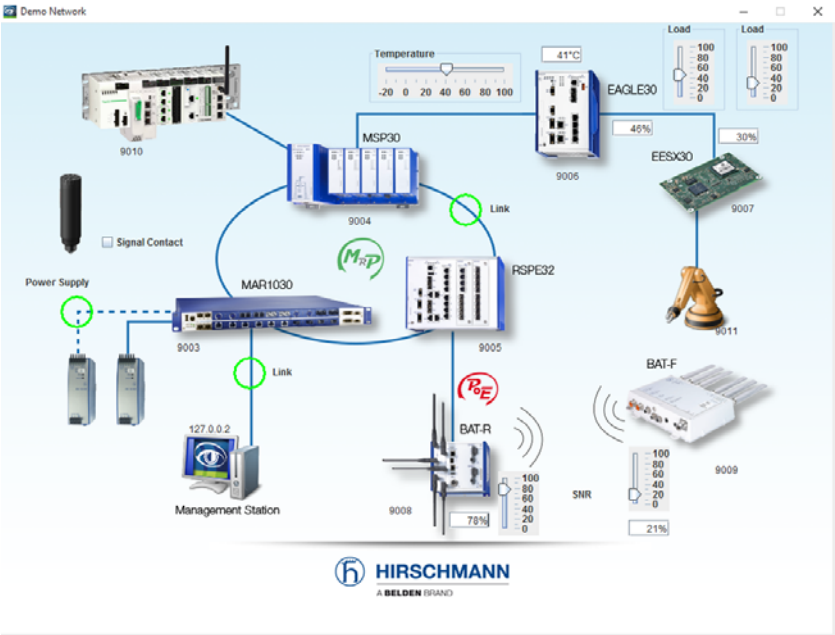


Figure 113:Demo network

8.13.10Calculate Availability

Due to their physical properties, each component in the network has a limited lifetime. The MTBF is the mean time between failures.
Repairs of the components also take a certain amount of time. The MTTR is the mean time to repair.
Industrial HiVision calculates the availability of a path based on the MTBF and MTTR values of the affected devices along that path.
Industrial HiVision also considers redundant paths here.
The type of a connected device affects the availability of the network. A redundantly connected switch/router has a bigger effect on the availability of the network than a redundantly connected terminal device.

Availability class	Designation	Availability in %	Annual downtime
1 (AEC-0)	Conventional	99.0	3.7 days
2 (AEC-1)	Highly reliable	99.9	8.8 hours
3 (AEC-2)	High availability	99.99	52.2 minutes
4 (AEC-3)	Fault resilient	99.999	5.3 minutes
5 (AEC-4)	Fault tolerant	99.9999	32 seconds
6 (AEC-5)	Disaster tolerant	99.99999	3 seconds

Table 50: Availability classes as per AEC

If the calculated availability values do not fulfill your requirements, you can carry out the following measures, among others, to increase availability:

- Set up redundant path
- Reduce downtimes by, for example, keeping replacement devices at the ready

Prerequisites for calculating availability

- For Windows operating systems:
  To calculate the availability, Industrial HiVision uses Microsoft NET Framework version 2.0 or higher.
  This program is part of the default installation of the Windows operating systems named in the system requirements.
  This software is required for proper calculation of availability on your network management station.
- For Linux operating systems:
  Install MONO 2.0.
  Check whether these programs are installed on your network management station.
- Note for Debian 6.0 and Ubuntu 12.04 (LTS):
  Install libmono2.0-cil and libmono-winforms20-cil.

Before calculating the availability, Industrial HiVision executes the following checks:

– Are the “MTBF“/“MTTR“ values of every connection greater than 0?
– Does every object (devices, clouds) have the properties “MTBF“/ “MTTR“ and are their values greater than 0?

If Industrial HiVision finds objects with missing specifications, Industrial HiVision displays them in a window. As soon as you have entered the required information, you can start the calculation again.

If you want to proceed with the calculation even though information is missing, click the “Use Default Values“ button. In this case, Industrial HiVision applies the default values wherever entries are missing.
If such objects are missing, you can start the calculation of the availability by clicking the “Use Default Values“ button. Industrial HiVision then uses any “MTBF“/“MTTR“ values entered for the calculation, and otherwise the default “MTBF“/“MTTR“ standard values.
“MTBF“ = 30000 h for devices, 100000 h for connections
“MTTR“ = 24 h for devices and connections
The actual values for the devices/connections differ from these standard values.
Using standard values allows you for example, to calculate the difference in the availability of 2 alternative routes.

Prepare calculation of availability

The following example describes how to prepare the calculation of the availability of a connection between 2 devices.
You can find the MTBF values of the Hirschmann devices in the installation path of Industrial HiVision under:
/data/doc/MTBF-Products.PDF.

- ☐ Open the “Map“ tab, at the device level.
- ☐ To enter the “MTBF“/“MTTR“ values of a connections proceed as follows:
  - Right-click on a connection and select “Properties...“.
  - In the dialog, open the “Properties“ tab.
  - In the “Availability“ frame, enter the “MTBF“/“MTTR“ values.
  - Click the “OK“ button.
- ☐ Add the user-defined properties “MTBF“, “MTTR“ and “Node Type“ to the device properties of a device.
  - Double-click on one of the two devices of the connection to go one level deeper in the detail view.
  - To add the user-defined properties “MTBF“ and “MTTR“, right-click an empty space in the detail view.
  - Select `New > Property`.
  - In the “New Property“ dialog hold down the “Ctrl” button and click “MTBF“ and “MTTR“.
  - Click the “OK“ button.
  - To enter the “MTBF“ value, open the “Properties“ dialog by double-clicking the “MTBF“ property.

- Enter the value in the “Current Value“ field and click the “Write“ button.
- Click the “OK“ button.
- Enter the “MTTR“ value in the same way.

☐ Add the device properties of the other device accordingly.

If either of the devices is a redundantly connected terminal device, then assign it the property “Node Type“ with the value “End Device“ in the same way (see above, “MTBF“ and “MTTR“).

As an alternative to individual device configuration, Industrial HiVision provides the option of MultiConfig™, which has the advantage that both devices can be configured with the “MTBF“/“MTTR“ properties at the same time:

☐ Open the “Map“ tab, at the device level.

☐ To enter the “MTBF“/“MTTR“ values of a connection proceed as follows:
- Right-click on a connection and select MultiConfig™.
- In the MultiConfig™ dialog, select “Container Properties“ in the menu tree.
  You can then find the table with the related connections in the object frame, and the table for the properties in the function frame.
- In the “Availability“ frame, enter the “MTBF“/“MTTR“ values.
- Click the “Write“ button.

☐ To add the user-defined properties “MTBF“ and “MTTR“ to the properties of the devices.
- To select both devices, hold down the “Ctrl” button and click on the devices at both ends of the connection.
- To open the MultiConfig™ dialog, right-click on a selected device and select “MultiConfig™”.
- In the MultiConfig™ dialog, select `Program Settings > New Property` in the menu tree.
  You can then find the table with the related devices in the object frame, and the table for the properties in the function frame.
- To create a new entry for the “MTBF“ value in the table, click the “New“ button.
- Select the property “MTBF“ and click the “OK“ button.
- To create a new entry for the “MTTR“ value in the table, click the “New“ button.

- Select the property “MTTR“ and click the “OK“ button.
- Click the “Write“ button.

☐ To open the dialog for entering the “MTBF“ values, open the “Properties“ tab in the detail display.

- In the “Property“ drop-down list, select the property "MTBF (Device)".
- Highlight the relevant devices.
- To open the MultiConfig™ dialog, right-click on a selected device and select „MultiConfig™“.
- To enter the “MTBF“ value, in the menu tree of the MultiConfig™ dialog, open the “Property Value“ dialog.
- In the “Value“ field, enter the “MTBF“ value.
- Click the “Write“ button.

☐ To open the dialog for entering the “MTTR“ values, open the “Properties“ tab in the detail display.

- In the “Property“ drop-down list, select the property "MTTR (Device)".
- Highlight the relevant devices.
- To open the MultiConfig™ dialog, right-click on a selected device and select MultiConfig™“.
- To enter the “MTTR“ value, in the menu tree of the MultiConfig™ dialog, open the “Property Value“ dialog.
- In the “Value“ field, enter the “MTTR“ value.
- Click the “Write“ button.

Calculate Availability

The following example describes how you can calculate the availability after you made the preparations beforehand.

☐ Open the “Map“ tab, at the device level.

☐ To select the connections of both devices, hold down the “Ctrl” key and click on both devices at the ends of the connection.

☐ To open the dialog for calculating availability, select `Tools >` Calculate Availability in the menu bar.

– If an “MTBF“/“MTTR“ property is missing for some objects, then Industrial HiVision opens the “Availability“ dialog with a table of the devices for which these properties are missing. This table also contains devices for which these properties have the value 0. Check whether the objects for example, devices or connections, for which you want to calculate the availability are missing.

– If every object in the “Map“ tab has the “MTBF“/“MTTR“ properties specified, then Industrial HiVision performs the calculation and displays the result in th “Availability“ dialog.
In the “Detail frame” of the dialog, Industrial HiVision displays the paths that Industrial HiVision included in the calculation. To display the details, mark the “Details“ checkbox.

During the calculation, Industrial HiVision writes details of the availability calculation in a log file. You can find this log file in the directory `<Installation path>/log/availability`. The name of the log file is made up of the name of the loaded project file and a time stamp.

Note: Availability calculation
Industrial HiVision performs the availability calculation under the assumption that the devices in the network are transmitting on every port. Therefore, redundantly connected terminal devices, routing, and VLANs can corrupt the results. The remedy for redundantly connected devices is to create the “Node Type“ property in the device and set its value to “Device”.

Note: Parallel connections
Industrial HiVision combines parallel connections between 2 devices into 1 path to optimize the calculation. The paths appear as a single path in the list of paths in the dialog and in the log file.

8.14 Help

In the “Help“ menu you can find the “Online Help“ and the version information for this program.

8.14.1 Online Help F1

You can access the “Online Help“ using the “F1” button on your keyboard or by selecting `Help > Online Help`.
The “Online Help“ contains the entire contents of the manual, with a table of contents, contents register, search function, and navigation help.
In the individual dialogs, you click “Help” to go directly to the page of the manual that relates to the dialog.

8.14.2 Tutorial

With `Help > Tutorial` you open an exercise with guidelines for your first familiarization with Industrial HiVision in the browser. This exercise takes you through the important and latest functions of Industrial HiVision.

8.14.3 Online

You can find further information under `Help > Online`.
You can select:

- “Hirschmann“
  to open the Hirschmann website.
- “Customer Innovation Center“
  to open the “Customer Innovation Center“ website.
- “Industrial HiVision“
  to open the Industrial HiVision product page on the Hirschmann website.
- “Order a License“
  to open an order form for ordering a license online for Industrial HiVision in the browser.
  To request the license key, you require:
  – the registration code of the product certificate (included in delivery)
  – the hardware key (see `Configuration > Preferences > Basics > License`).
    Industrial HiVision transfers the hardware key automatically when you call up the ordering page here.

8.14.4 Kernel Info

Under `Help > Kernel Info`, you can find the information that a service technician requires for a service task.

The kernel is the core of the Industrial HiVision application. The purpose of the kernel is to collect information from the network devices and the user interface. The kernel saves the information in a database. The user interface sends a request to the kernel, such as the device status. The kernel retrieves the information from the database and answers the request.

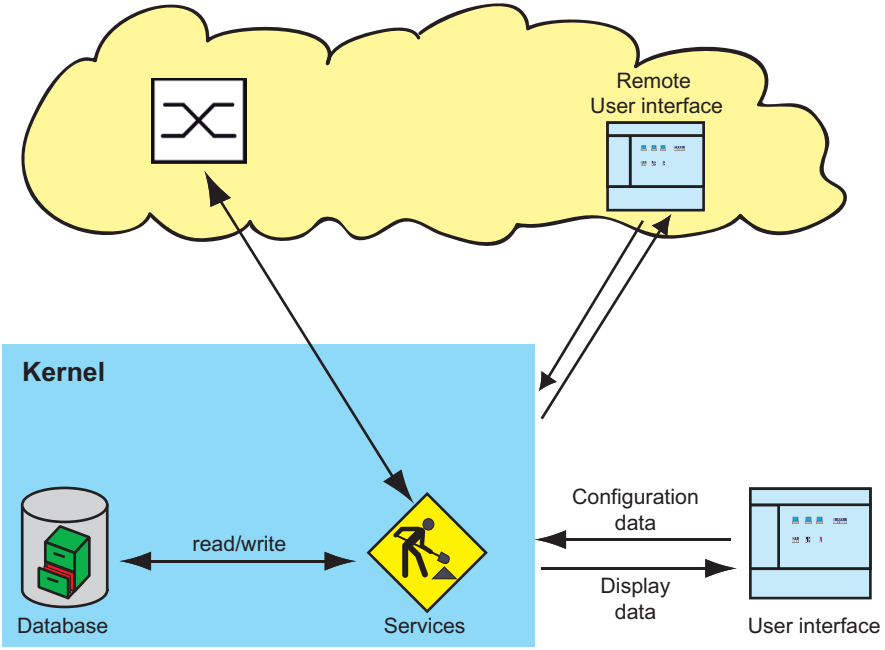


Figure 114:Industrial HiVision Kernel Architecture

8.14.5 About

Program Info

You can find information on the program version and the publisher under `Help > About > Program Info`.

EULA

You will find information on license agreements under `Help > About >` EULA

License

You can find information on program licenses under `Help > About >` License

A Appendix

A.1 FAQ

Answers to frequently asked questions can be found on the Hirschmann Industrial HiVision Website:

www.hivision.de

A.2 Monitored properties

A.2.1 Monitored properties in the basic setting

Properties that Industrial HiVision monitors using traps or polling in the basic setting you will find in the following table.

Industrial HiVision lists the traps in the event list.

Note: Keep in mind how this affects your system resources (see on page 228 “Effect on system resources”).

Property	Trap	Polling	Polling interval
AutoConfiguration Adapter status	x		
Fan Status	x		
Power Supply Status	x		
Relay Status	x		
Port Link	x	*	30 seconds
Port In Load		*	30 seconds
Port Out Load		*	30 seconds
Port Admin	x		
Port Oper Status	x		
WLAN Station	x	**	30 seconds
WLAN access points	x	**	30 seconds
Signal to Noise Ratio		x**	30 seconds

Table 51: Monitored properties
** In the default setting, polling is enabled for ports that have a cable connection in Industrial HiVision.*
*** In the default setting, polling is enabled for ports that have a wireless connection in Industrial HiVision*
**** The higher protocol supported by the device*

Property	Trap	Polling	Polling interval
Spanning Tree Status	x	*	30 seconds
Rapid Spanning Tree Status	x	*	30 seconds
Multiple Spanning Tree Status	x	*	30 seconds
Protocol Ping Reachability		x	30 seconds
Protocol SNMPv1 Reachability		x***	2 hours
Protocol SNMPv3 Reachability		x***	2 hours
HIPER Ring Status	x	*	30 seconds
HIPER Ring Coupling Status	x	*	30 seconds
Dual Homing Status	x	*	30 seconds
Ring Coupling Enabled	x		
Ring Manager Enabled	x		
Dual Homing Enabled	x		
Router Redundancy Mode	x		
Router Redundancy Status	x		
Temperature	x	x	5 minutes
Configuration Status	x	x	5 minutes
Configuration Signature		x	1 hour
Configuration File	x	x	24 hours
Http		x	24 hours
Telnet		x	24 hours
SNMP V1/V2		x	24 hours
Tftp		x	24 hours
IEC61850		x	24 hours
Profinet IO		x	24 hours
EtherNet/IP		x	24 hours
Unused Active Ports		x	24 hours
802.1X Port Access Control Enabled		x	24 hours
Outbound ANY Rule		x	24 hours
Inbound ANY Rule		x	24 hours

Table 51: Monitored properties
** In the default setting, polling is enabled for ports that have a cable connection in Industrial HiVision.*
*** In the default setting, polling is enabled for ports that have a wireless connection in Industrial HiVision*
**** The higher protocol supported by the device*

A.3 CSV export

If you are working with CSV files across different languages, you require the corresponding character sets. Industrial HiVision uses the following codes when exporting data to a CSV file:

Language	Character set
German, English, French, Spanish, Italian, Portuguese, Indonesian	Latin-8859-1
Greek	Windows-1253
Korean	Johab
Japanese	Shift-JIS
Chinese	GB2312
Russian	Cyrillic-8859-5

Table 52: Character sets for CSV export

A.3.1 Microsoft Excel before 2010

To import to Microsoft Excel, you choose:

☐ In Excel, choose the menu item
`Data:Import External Data:Import Data`

☐ Select the file and click “Open”.

☐ In the Text Conversion Assistant - Step 1, choose “Separate” for the original data type.

☐ In the Text Conversion Assistant - Step 2, choose “Tab stop” and “Semicolon” as the separators.

A.3.2 Microsoft Excel 2010

To import to Microsoft Excel, you choose:

- ☐ In Excel, select the `Data:From Text` menu item.
- ☐ Select the file and click “Import”.
- ☐ In the Text Conversion Assistant - Step 1, choose “Separate” for the original data type.
- ☐ In the Text Conversion Assistant - Step 2, choose “Tab stop” and “Semicolon” as the separators.
- ☐ In the Text Conversion Assistant - Step 3, choose the “Standard” column for the data format.
- ☐ Click “Finish”.

A.4 Language support

Language	User interface	Online help	Manual (PDF file)	Manual (printed)	Tutorial	Readme
German	X	X	X	X	X	X
English	X	X	X	X	X	X
Spanish	X	X	X			
French	X	X	X			
Italian	X	X	X			
Russian	X					
Chinese	X	X	X			
Korean	X					
Japanese	X					
Greek	X					
Portuguese	X					
Indonesian	X					

Table 53: Language support

A.5 Ports used

To communicate between the user interface and the services Industrial HiVision uses specific protocol ports in your network. The following table contains the ports and their usages.
When a firewall separates your Industrial HiVision services from a client, add a rule to the firewall to forward data between the services and client.
See “Using Industrial HiVision with Firewalls” on page 62.

Ports used	Usage
11206	CORBA Naming Service
11207	Traps from demo agent to the Industrial HiVision service
11208	HTTP/HTTPS server
11209	Communication between the interface and service. Industrial HiVision also uses this port for communication between service and subdomains.
11212	Communication with the OPC DA Server
11210	Communication with the OPC UA HTTP Server
11211	Communication with the OPC UA HTTPS Server

Table 54: Ports used

A.6 Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet.
www.hirschmann.com

A.7 Literature references

- “Optische Übertragungstechnik in industrieller Praxis”
  Christoph Wrobel (ed.)
  Hüthig Buch Verlag Heidelberg
  ISBN 3-7785-2262-0
- Hirschmann Manual
  “Basics of Industrial ETHERNET and TCP/IP”
  280 710-834
- “TCP/IP Illustrated”, Vol. 1
  W.R. Stevens
  Addison Wesley 1994
  ISBN 0-201-63346-9
- Hirschmann “Installation” user manual
- Hirschmann “Basic Configuration” user manual
- Hirschmann “Redundancy Configuration” user manual
- Hirschmann “Routing Configuration” user manual
- Hirschmann “GUI Graphical User Interface” reference manual
- Hirschmann “Command Line Interface” reference manual
- Hirschmann User Guide “Industry Protocol”
- Hirschmann Manual “Network Management System HiVision”
- Hirschmann Manual “HiOPC Server Interface”

A.8 Copyright of Integrated Software

Industrial HiVision includes a number of open source components. The creators of these components have released these components under a variety of licenses.
You will find these licenses in the installation path of Industrial HiVision under `data\doc\FOSS-BOM.html`

B Index

0-9
1to1 NAT router 276, 400

A
Absolute 294
Abstract 360
Access point 140
Access Rights 50
Access station 140
Action 337, 342
Adding rules 174
Alarm message 306
Arrange 133
Assign license 56, 58
Audit Log 48
Audit Trail 48
Authorization 46
Authorization roles 47, 329
Auto Layout 133, 277
Auto Topology 274

B
Background 360, 365
Background image 271
Bandwidth 124, 327
Basic settings 278
Browser 393
Bubble help 286, 293, 361
Buffer size 286

C
CA Certificates 241
Certificate 44, 45
Change OPC Server Type 239
Client Mode 26
Component detail 98, 236, 288, 289
Configuration signature 208
Connection 141, 292, 361
Connection line 144
Connection properties 144
Connection status 361
Contents register 448
Copy 135
Ctrl+E 79

D
Data Access V1 to V3 233
Date 91
Date format 352
DCOM 233
Debian 6.0 443
Default device icons 61
Default icon 128, 366
Default Map 325
Default setting 161, 360, 365
Delete 268
Delta 294
Device certificate 209
Device configuration 437
Device Connection 140
Device detection 128, 216, 366
Device discovering method 123
Device documentation 154, 270, 372
Device name 134, 148, 396
Device password 372
Device Signaling 297
Distributed Component Object Model 233
DNS 134
Domain 49
Domains 54
Domain Name Server 134
Draw 133
Duplex 105

E
Edit mode 46, 84, 265
Edit Mode 370
EDS 366
EDS file 367
Electronic data sheet 366
Email 393
Email configuration 393
EtherNet/IP 128, 282
EULA 451
Event 335, 337, 353, 417
Event display 353
Event line 72, 89
Event list 72, 262, 353, 390
Event log 92
Event log file 113, 353
Exit 263, 264
Export 262
E-mail 336

F
FAQ 469
FDB 273
File Selection Dialog 256
Filter 337
Fingerprint 208
Firewall rules 174
Font 360

Font size 363
Foreground 365
Forwarding Data Base 273
Free version 60, 266
Frequency of requests 124
Frequency of the requests 327

G
Gateway 385, 415
Gateway IP address 148
Geographical location 304
Geographical location view 304, 393
Graphical user interface 419

H
HiDiscovery 282
History 286, 292, 306
Hosts file 134

I
Icon 128
Icon file 367
Icon size 360
ICMP 225
Identification 415
Import 338
Important Security Note 205
Initial setting 174, 385
IP address 124, 132, 148, 326
IP address prefix 385
IP address range 124
IP Address 415
IP configuration 49, 148, 415
I'm alive Event 355

K
Key 209

L
Language 352
LDAP 46
License 49, 54, 60, 266
License Agreements 451
License files 260, 261
License key 348
Lightweight Directory Access Protocol 46
Line thickness 361
Line up 133
Link 139, 140, 222, 267
Linux Syslog Server 31
LLDP 273
Load backup 261
Location view 304
Login name 46
Log file 354
Log statistics 300

M
Main window 72
Make a folder 137
Management IP address 134
Manual 448
Map 304
MAC address 124, 129, 326, 367
Menu bar 72, 78
MIB 225, 439
MIB Manager 226, 387
MIB variable/OID 226
MIB Viewer 226, 387
Modbus/TCP 129, 282, 366
Module number 134
Monitor 306, 309
Moving 140
MONO 2.0 443
MTBF 294, 442
MTTR 294, 442

N
Name 134
Names 395
Navigation field 72
Navigation help 448
NAT 400
Netmask 415
Network card 385
Network load 222, 231, 232
Network management interface 121
Network mask 148, 327, 385, 406
Network plan 130
Network scan 124, 440
Network Scan 325, 326
NET 2.0 443

O
Object identifier 387
OID 226
Online help 82, 448
Open 259
OPC 50
OPC server 387
OPC service 233
OPC Server deactivate 376
OPC UA Client 238
OPC UA Security 241
OPC write command 375

P

password 179
Password 46, 200, 363, 372, 377, 378
Password for Edit Mode 370
PDF Viewer 393
Ping 282, 393
Ping server 389
Polling 229, 231, 296, 455
Polling interval 231, 326, 327
Port number 134, 379
Port Names 134, 396
Port security 209, 210
Power over Ethernet 108
Prefix 385
Print 263
Private Network 67
Process visualization 233
Product image 360
Product-Specific Modules 78, 308
Program 29
Project database 260, 261
Properties 278, 285, 292
Protocol 282
Protocol port 379
PSM 78, 308
PSM Manager 78, 308

R

RADIUS 47
Realistic 360
Redundant network management system 45
Refresh 216
Refresh VLAN 299
Registration code 349
Remote access 36, 374
Remote Authentication Dial-In User Service 47
Repetition 379
Reporting 78, 222, 295, 309
Request interval 327
Restart 167
Retry block 390
Roaming 140
Rogue device 212
Running mode 85

S

Save 152, 259
Save as 260
Save backup 260
Scan Network 148
Scan rate 232, 389
Scheduler 79
Scheduling 314
SCADA 233
Search function 448
Security 42, 63, 200
Security lock-down 210
Security Risk 29, 43, 45
Security status 236
Security status display 204
Security-Status 107
Send email 340
Server 36
Server IP Address 36
Server Mode 26
Service 28, 91, 256, 263, 374, 389
Service technician 449
Signal 415
Signature 44
SMS 335
SNMP 273, 282, 408
SNMP browser 439
SNMP configuration 378
SNMP MIB 225
SNMP password synchronization 177
SNMP query 379
SNMP user 377
SNMP version 378
Software Backup 33, 34
Sound 219, 335
Speed 361
SSH 393
State on delivery 214
Status 214, 360, 365
Status change 360
Status configuration 134, 140, 214
Status determination 133
Status propagation 133, 217, 278, 293
Status symbols 160
Subdomain 49
Subdomains 54, 56, 58, 375
Subdomain interface 374
Subdomain password 375
Superdomain 375
Superdomains 56, 375
Superdomain License 54, 350
Switched-on message 124, 325
Symbol 160, 161
SysOID 128, 366
System control 29
System language 352
System Object Identifier 128, 366
System requirements 24
System resources 228

T

Table of contents 448
Technical questions 469
Telnet 393, 438
Temperature 231
Temperature monitoring 231
Template example configuration 136
Template icons 138
Text display 363
Threshold value 290
Time 91
Timeout 379
Tool 419
Tool bar 72, 79
Topology 97
Topology Discovery 140, 273
Training courses 469
Trap 59, 124, 215, 306, 325
Traps 455
Trap destination 417
Trap destination address 59, 385
Trial period 60, 266
TSN Example Configuration 187
TSN time calculation 184
TXCare 393

U

Ubuntu 12.04 443
Undiscovered devices 276
Update 35
User authorizations 46, 50
User defined properties 408
User Management 329
User name 377
User-configurable action 342
User-defined property 225

V

Value 279, 285
Version 448
VLAN membership 299
VRRP 276

W

Web Access 244
Web interface 436
Wireless client 276
Wireless device scripts 316
Wireless Local Area Network 140
WLAN 140

Z

Zoom 96, 305

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

D Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

_____

_____

_____

_____

_____

_____

_____

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

Hirschmann Automation and Control GmbH
Department 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen