User Manual

Basic Configuration
HiProvision Management Operation

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.

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 the Hirschmann product site (www.hirschmann.com).

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

Contents

List of figures

List of Tables

1. INTRODUCTION

1.1 General

This document is valid as of Dragon PTN Release 4.3DR.

This manual describes the general set-up of the HiProvision PC. HiProvision is the Dragon PTN management software. The HiProvision PC must be connected to the Dragon PTN MPLS-TP network. See the figure below for an example. This manual also describes the general operation on the HiProvision PC to connect, configure and monitor the Dragon PTN network.

- A detailed description to setup the core Dragon PTN network: see Ref. [2Net] in Table 1;
- A detailed description to setup pure Ethernet services: see Ref. [2Eth] in Table 1;
- A detailed description to setup Legacy services: see Ref. [2Leg] in Table 1.

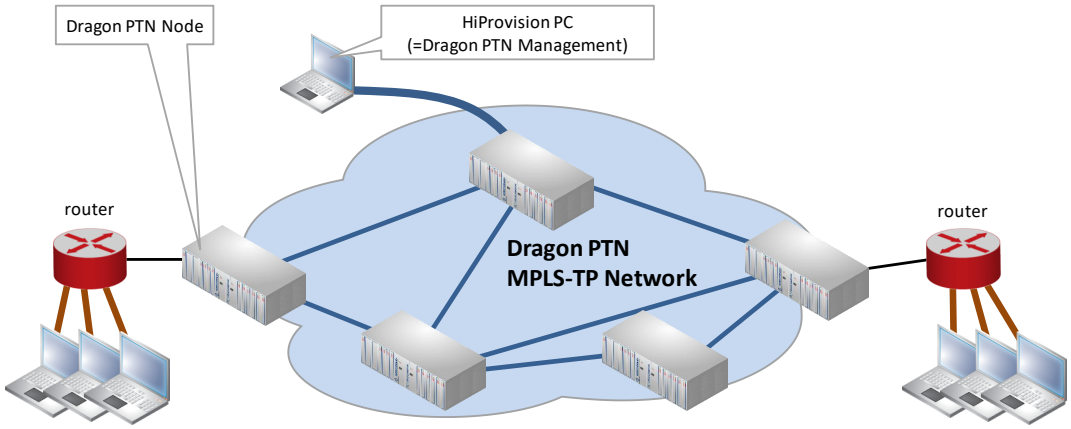


Figure 1 Dragon PTN Network Example

Prerequisites for a Dragon PTN solution setup:

- a PC or laptop with a NIC is available that can be used as a HiProvision PC;
- you are Administrator of the PC or laptop;
- have your serial key and purchased vouchers ready before going online (see §4);
- a network plan:
  - How many nodes? See also Ref.[2Eth], [8], [9] in Table 1;
  - How many links per node?
  - Optical fiber or electrical links?
  - Which node numbers and node names must be used?
  - Which front ports within the node will act as WAN port?
  - Which front ports within the node will act as LAN port?
  - How does my network look like? Network topology? Node interconnections?
  - How do my customer applications connect to the network?

1.2 Supported Hardware, Firmware, Software

The supported hardware, firmware and software within this Dragon PTN release can be found on the Portal https://hiprovision.hirschmann.com via Shortcuts → Downloads.

1.3 Manual References

Table 1 is an overview of the manuals referred to in this manual. '&' refers to the language code, '*' refers to the manual issue. All these manuals can be found in the HiProvision Help Tile.

Table 1 Manual References

Ref.	Number	Title
[1]	DRA-DRM801-&-*	Dragon PTN Installation and Operation
[2Eth]	DRA-DRM831-&-*	Dragon PTN Ethernet Services
[2Leg]	DRA-DRM832-&-*	Dragon PTN Legacy Services
[2Net]	DRA-DRM833-&-*	Dragon PTN Network Operation
[8]	DRB-DRM802-&-*	Dragon PTN Aggregation Nodes: PTN2210, PTN2206, PTN1104, PTN2209
[9]	DRB-DRM840-&-*	Dragon PTN Core Nodes: PTN2215
[10]	DRD-DRM803-&-*	Dragon PTN Central Switching Module: CSM310-A/CSM540-A
[15]	DRA-DRM812-&-*	HiProvision User Management
[19]	DRA-DRM822-&-*	HiProvision Alarms List
[20]	DRG-DRM824-&-*	HiProvision Add-on: CAR IP
[21]	DRG-DRM825-&-*	HiProvision Add-on: SNMP Northbound
[25]	DRG-DRM826-&-*	HiProvision Add-on: Generic Reporting Engine
[26]	DRG-DRM829-&-*	HiProvision Add-on: Permanent Monitoring

2. STEPS FOR A BASIC SETUP

Prerequisites: make sure that

- your network (nodes, NSM, CSM, PSU, IFMs, SFPs, …) has been installed, see Ref. [1];
- Node numbers have been set on the NSMs, see Ref. [1];
- CSMs have been factory reset, see Ref. [1];
- your network LAN/WAN network cables have been connected, see Ref. [2Net].

Following major steps are necessary to set up a basic Dragon PTN MPLS-TP solution. After having completed all the steps below, customer applications in the access networks will be able to communicate via a service over the Dragon PTN MPLS-TP network. Further on, these steps are worked out in more detail.

1. (§2.1) Prepare and Install the HiProvision PC
2. (§2.2) Connect the HiProvision PC to the Dragon PTN Network
3. (§2.3) Start Up HiProvision / Dashboard
4. (§2.4) Initialize HiProvision
5. (§2.5) HiProvision: Discover and Approve the Dragon PTN Network Topology (DCN)
6. (§2.6) HiProvision: Network Database Configuration
7. (§2.7) HiProvision: Check Network Hardware
8. (§2.8) HiProvision: Load Configuration into the Network
9. (§2.9) HiProvision: Set the Node Timing via an NTP Server

2.1 Prepare and Install the HiProvision PC

HiProvision is the software that manages the Dragon PTN network. Follow the steps below for further installation of HiProvision.

2.1.1 PC Requirements

The HiProvision PC requirements are listed in the ‘Quick Installation Guide’, see next paragraph.

2.1.2 Install HiProvision

HiProvision and a serial key can be downloaded from the Portal.

1. Surf to the Portal (= https://hiprovision.hirschmann.com) and log in;
2. Click on Shortcuts → Downloads;
3. Select the latest release or select another release via the drop down list;
4. Expand the ‘Software’ list;
5. Download all the components as described in the ‘Quick Installation Guide’. The 'HiProvision' download automatically includes all the firmware files for the hardware and the product manuals or documentation;
6. Obtain a serial key via ‘Shortcuts → Licenses HiProvision → Serial Key‘. The Obtained HiProvision serial key will look like: ‘DRN2-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx’;
7. Installation on the HiProvision PC:
   - Make sure your PC meets the PC requirements listed in the ‘Quick Installation Guide’;

- Follow the ‘Quick Installation Guide’ to install HiProvision with its serial key. The HiProvision Agent can be installed in as a program or as an MS Windows service. During HiProvision installation, the checkbox below in the installation wizard is shown to install the HiProvision Agent. Checkbox: Install HiProvision Agent as a service:
  - Unchecked (= default): HiProvision Agent is installed as a program, with a HiProvision agent icon on the desktop. Later on, after the installation has been finished, the HiProvision agent must be started manually before starting the HiProvision Client.
  - Checked: HiProvision Agent is installed as an MS Window service: Windows start button → Services → HiProvision Agent. No HiProvision Agent icon is installed on the desktop. When the HiProvision PC boots or starts up, the HiProvision Agent service will always be running by default. Only the HiProvision Client must be started manually.

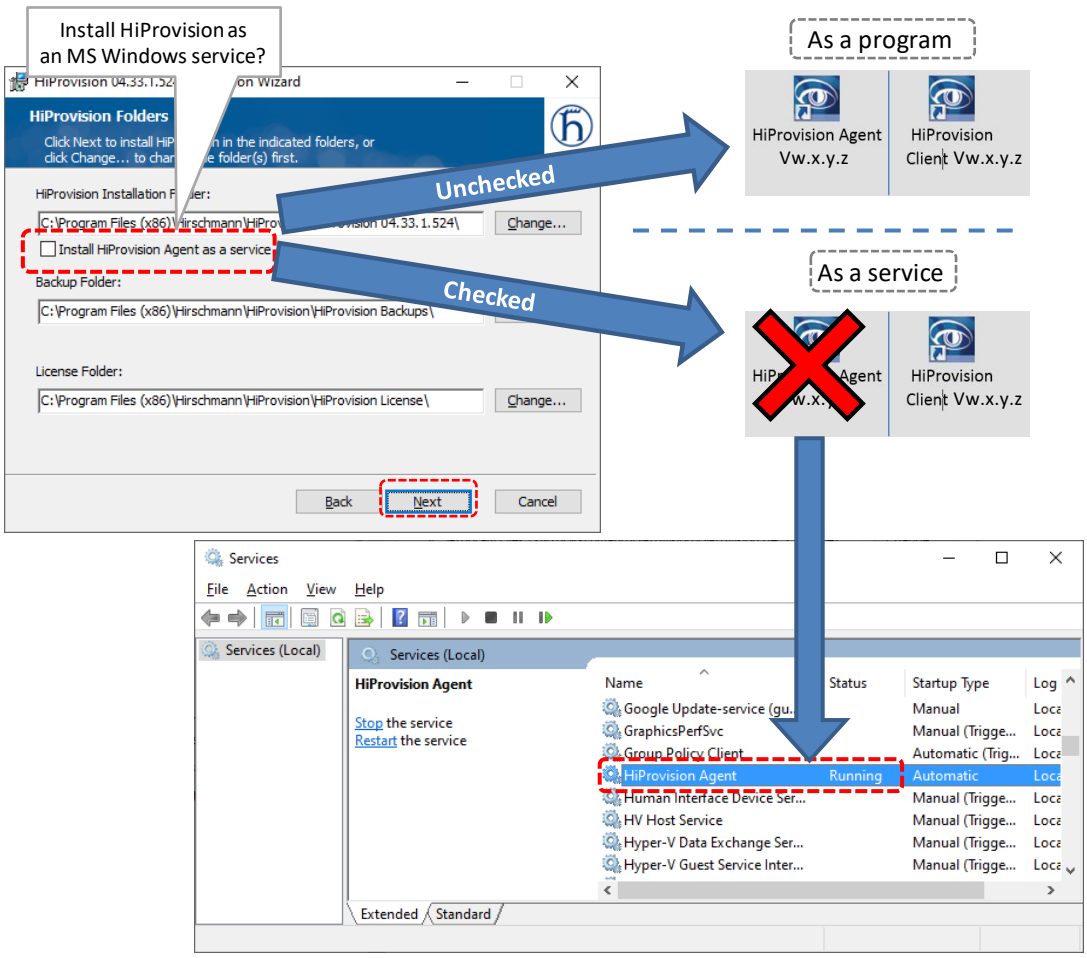


Figure 2 HiProvision Installation Wizard: HiProvision Agent: Program or as a Service

- Default installation path: `C:\Program Files (x86)\Hirschmann\HiProvision\`;
- Once the HiProvision has been installed (Complete Setup), the icons in the table below will be placed on the HiProvision desktop with X.Y.Z indicating the HiProvision version. It is also possible to install a custom installation via Custom button → Shortcuts when you don't need all shortcuts:

Table 2 Installation Shortcuts

Installer → Setup Type	HiProvision Agent VX.Y.Z (*)	HiProvision Client VX.Y.Z	HiProvision Remote Client VX.Y.Z	HiProvision LNM Client VX.Y.Z	HiProvision Remote LNM Client VX.Y.Z
Complete Button					
Complete	✓ (*)	✓	✓	✓	✓
Custom Button → Shortcuts					
Local Client	✓ (*)	✓			
Remote Client			✓		
LNM Client	✓ (*)			✓	
Remote LNM Client					✓
Note (*): HiProvision Agent icon is not visible when HiProvision Agent has been installed as a 'service'. See §3.1 for more info.					

2.1.3 Configure Static IP Address on the NIC

a. One IP Address on the NIC

The IP address that must be configured on the NIC (=Network Interface Card) in the HiProvision PC depends on the CSM in the node to which the NIC is connected. Redundant CSMs are possible in the node which might result in two NICs in the HiProvision PC. Some use cases are available in §11.

Verify to which CSM the NIC is connected. In the IP Protocol settings of this NIC on the HiProvision PC, configure the following Internet Protocol Version4 (TCP/IPv4) Settings:

- CSM Front IP address: <IP address shown on the display of the connected CSM> + [1…13]. E.g. if the IP address on the CSM display = 172.16.25.33, set the IP address of this NIC to an IP address in the range 172.16.25.33 + [1..13] = 172.16.25.34 …. 172.16.25.46. In case of redundant CSMs, both CSMs have an IP address in a different /28 subnet. Make sure to use the correct IP address in the NIC!
- Subnet mask: 255.255.255.240 (=/28 subnet mask).

NOTE: It is possible to change the IP address of the CSM, see §2.5.7.

Other fields: can be left empty;

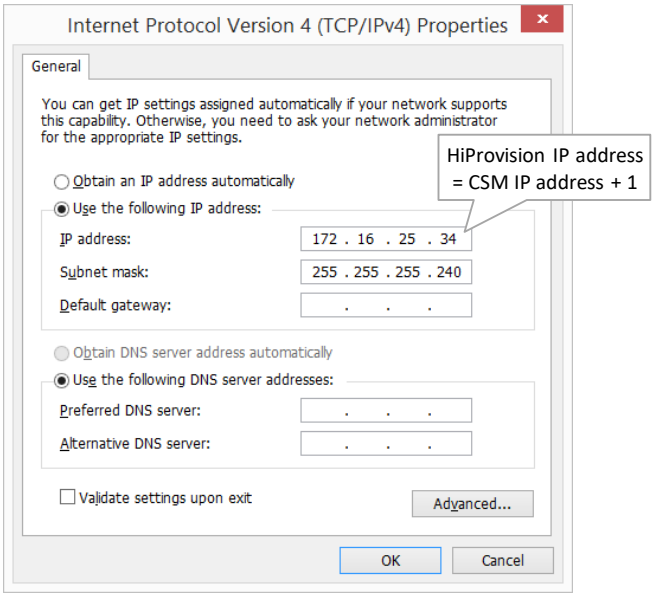


Figure 3 HiProvision IP Address

b. A Second IP Address on the NIC

A second IP address on the NIC is necessary when the HiProvision PC only has one NIC that must be connected via a switch to two different access or entry points to the Dragon PTN network (see §2.5.5).

In Figure 3, click on the 'Advanced…' button. The figure below pops up.

- Click on the Add button, the TCP/IP Address window pops up;
- Fill out the IP address and Subnet mask fields;
- Click the Add button;

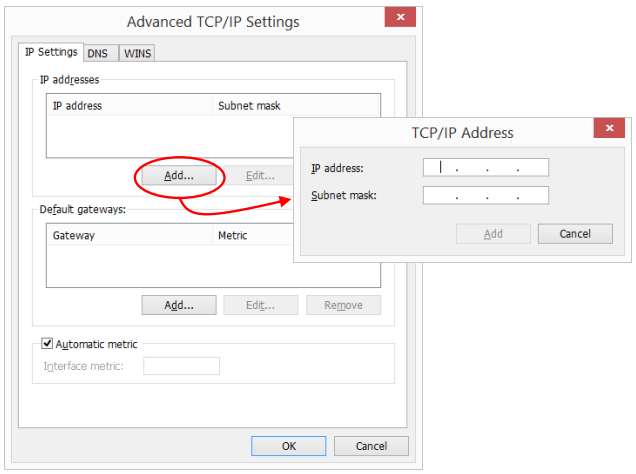


Figure 4 Second IP Address on NIC

CAUTION:
If you change your HiProvision connection e.g. from node x to node y, the IP address of the HiProvision PC must be configured with another IPv4 address. Follow the actions described in §2.5.9.

2.2 Connect the HiProvision PC to the Dragon PTN Network

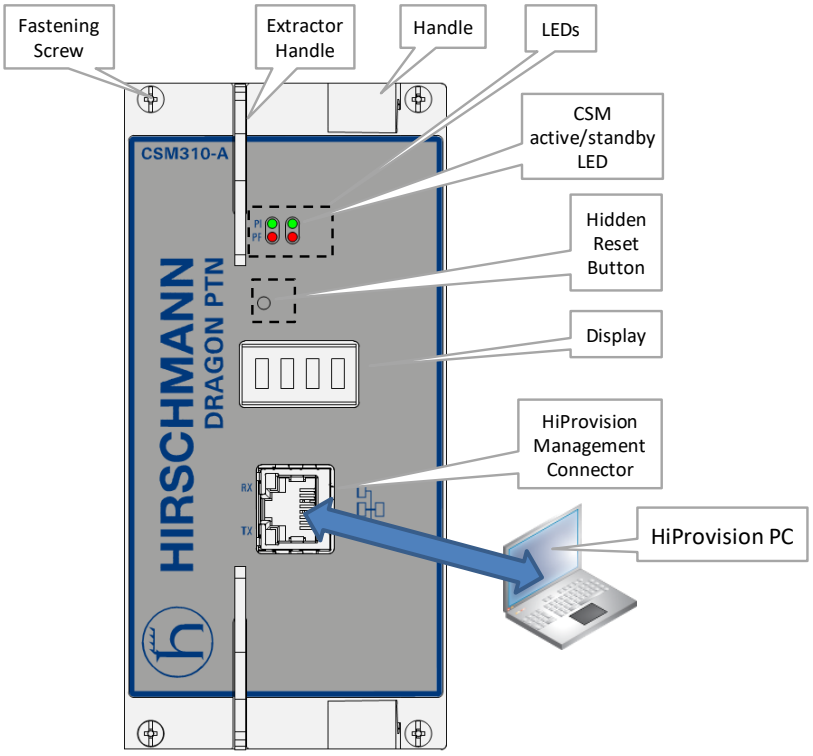


Figure 5 CSM310-A Front Panel → Connect HiProvision PC

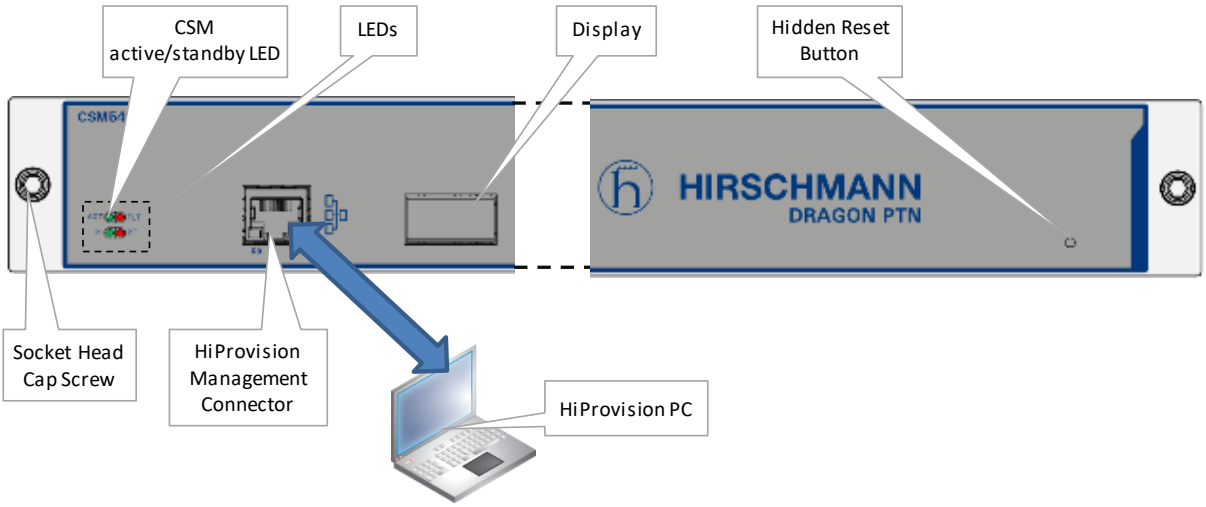


Figure 6 CSM540-A Front Panel → Connect HiProvision PC

- Make sure that the HiProvision Management Port on the CSM, to which the HiProvision PC is going to be connected, is unlocked or up. This port is by default 'up' but could be 'down' for security reasons. This can be verified via Dashboard → Network Hardware → Devices → Node → CSM → Properties (Specific) → Management Port: Up.
- Interconnect one or two NICs on the HiProvision PC with one single CSM or two redundant CSMs in a node in the Dragon PTN network. The connection(s) with the node occurs via plugging in the copper cable into the 'HiProvision Management Connector' of its CSM(s), see Figure 5;

- The IP address(es) of HiProvision directly connected to a CSM will by default be in the range of the CSM front IP address (172.16.0.1 → 172.20.100.209). This range can be different if a router is between HiProvision and the Dragon PTN network or if the CSM front IP address has been set in another IP range (see §2.5.7). The HiProvision IP addresses can be verified via the 'ipconfig' command in a command prompt on the HiProvision PC, see also §2.1.3;
- The CSM front IP address can be verified on the CSM display, see also (*) below;
- The HiProvision PC must be able to ping the connected node;

NOTE: (*) After plugging in the management cable, it can be configured in HiProvision (**) how many times ('n') the IP address must scroll on the CSM display after plugging in the management cable or rebooting the CSM. After these 'n' times, the IP address will not be displayed anymore e.g. for security reasons. If you want to show the IP address again for 'n' cycles, pull out the cable and plug it in again. By default, the IP address is always displayed in every CSM display-cycle.

NOTE: (**) 'n' can be configured via HiProvision → Network Hardware Tile → Devices → Select CSM → Display → Show IP address n Times: By default this field shows '-1' indicating that the value is displayed forever, '0' means never, 'n' with n > 0 means n times.

2.3 Start Up HiProvision / Dashboard

1. Verify if the **HiProvision Agent** is running. If HiProvision Agent was installed as a service, it is started already and runs by default. If not, is has to be started manually. See §3 to find out how it was installed and whether it is already running or not.
2. For a first time installation on the HiProvision PC, make sure to allow all the processes to pass through the Windows Firewall. Make sure that all the checkboxes are enabled in the figure below and click Allow access.

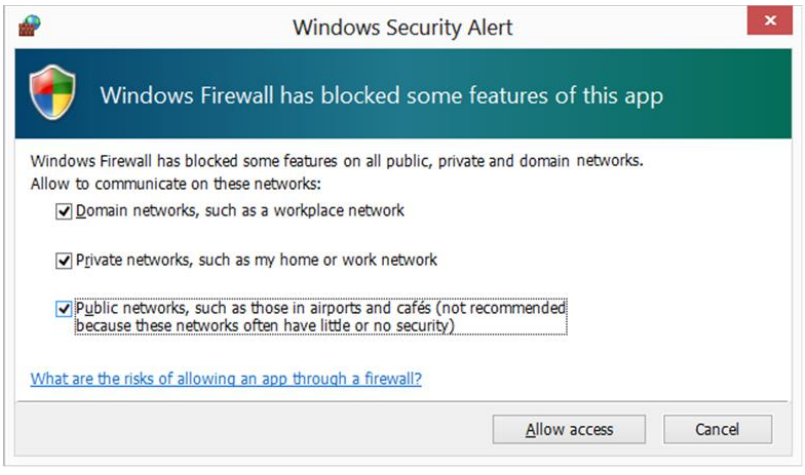


Figure 7 Allow HiProvision Processes

If the HiProvision Agent does not start up, verify the troubleshooting in §21.

3. Once the HiProvision Agent has started up successfully (see §3), start up the **HiProvision Client** or the **HiProvision LNM Client** by double-clicking its icon on the desktop. The HiProvision Client is a full version including all features and applications, whereas the

HiProvision LNM Client is a light or stripped version of the HiProvision Client. The differences between the two versions can be found in the table below:

Table 3 Differences HiProvision Client / HiProvision LNM Client

Tile Group	Dashboard Tile	HiProvision Client	HiProvision LNM Client
✓ = Tile or application available; --- = Tile or application not available;			
Administration	Database	✓	✓
	Servers (+Redundancy)	✓	✓
	Users (=HiProvision UM)	✓	✓
	Licenses	✓	✓
Configuration	Discovery	✓	---
	Network Hardware	✓	✓
	Connections	✓	---
	Layouts	✓	✓
	Protocols	✓	---
Monitoring	Network	✓	---
	Large Network (=LNM)	✓	✓
	Events	✓	✓
	Performance	✓	---
	Alarms	✓	✓
	Assurance	✓	---
	Protocols	✓	---
Tools	Software	✓	---
	External Devices	✓	---
	Inventory (used in HiProvision Add-on: Generic Reporting Engine)	✓	---
	Add-ons	✓	---
	Advanced	✓	---
	Help	✓	✓

NOTE: It is possible that your Client does not start because one of the two pop-ups below. Your started Client is not compatible with the already running Agent. In case of a HiProvision Agent Service, choose the version you want and click Apply. In case of a HiProvision Agent Program, either close the current Client and start the correct Client, or kill the wrong HiProvision Agent Program and start the correct HiProvision Agent Program and Client.

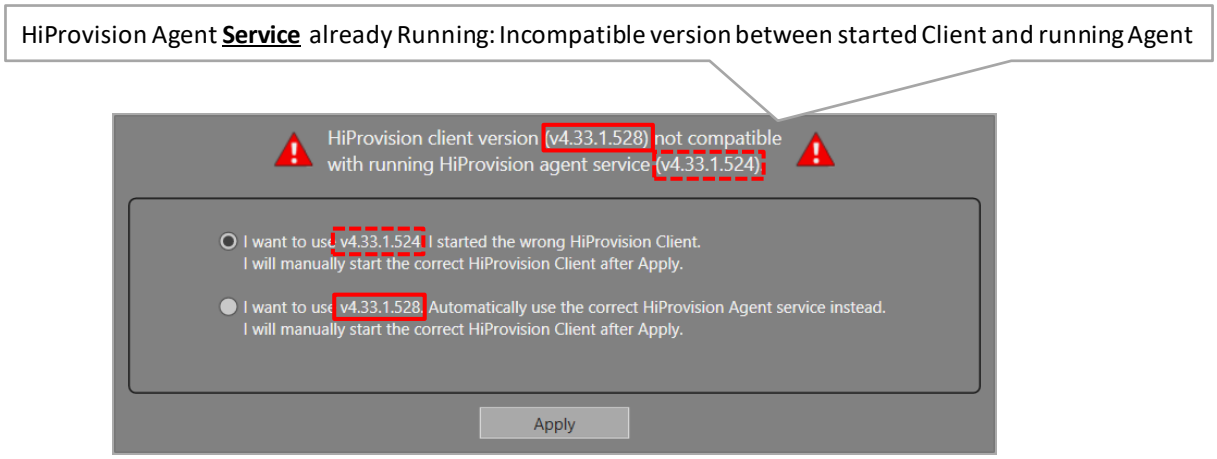


Figure 8 HiProvision Client not Compatible with Running HiProvision Agent Service

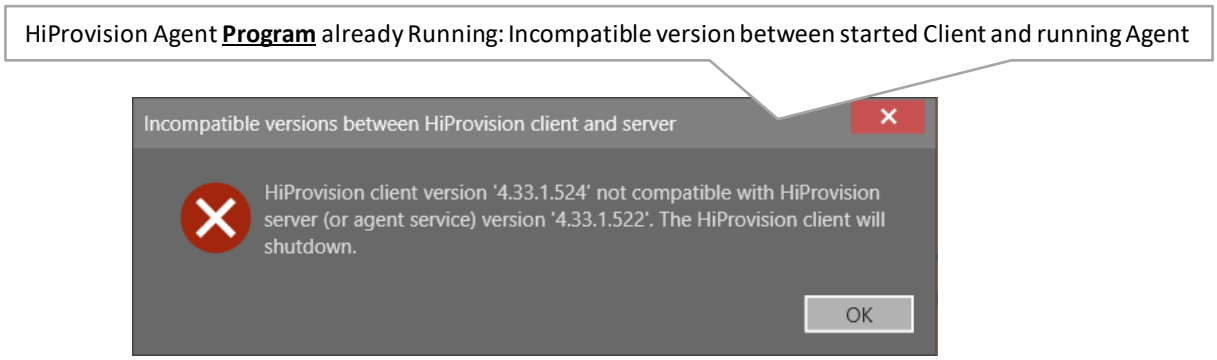


Figure 9 HiProvision Client not Compatible with Running HiProvision Agent Program

4. The HiProvision dashboard shows up including the user database pop-up below. The dashboard is divided in four main blocks, each block showing some tiles. Each tile is a shortcut to the mentioned function e.g. Database, Servers, …. Tiles with a white lock icon are currently locked or access denied.
5. From now on HiProvision must be initialized, the first step is to create/select a user database, see figure below.

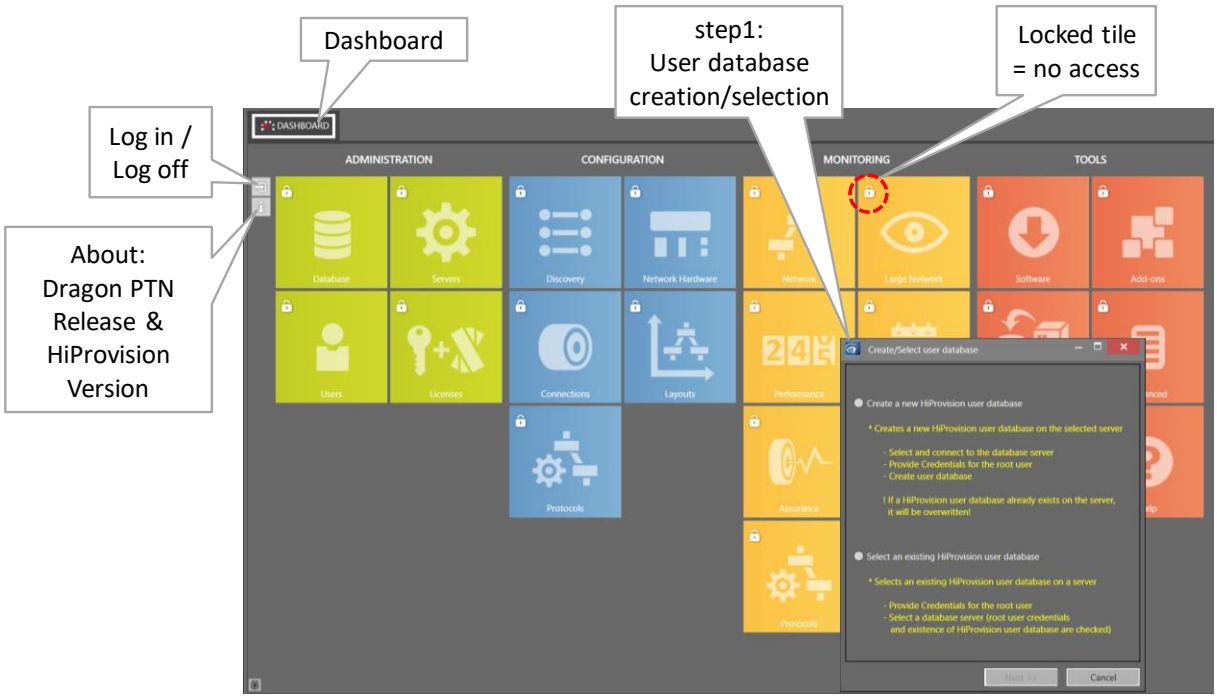


Figure 10 Dashboard View with User Database Request

2.4 Initialize HiProvision

This paragraph describes how to prepare or initialize HiProvision for a first time use. Basically following actions below must be done, find more detailed information further on:

- Create/Select User Database
- Log in
- Create Network Configuration Database
- Start Servers
- Install License Pack
- Used language

2.4.1 Create/Select User Database

1. In the user database request pop-up, select ‘Create a new HiProvision user database’.

CAUTION: if a user database exists already on the connected server, it will be overwritten with the new created one.

2. MySQL root user: Fill out the IP address of the database server on which MySQL server runs, in the 'Server IP/Host Name' field. If it runs on the own HiProvision PC, fill out 127.0.0.1. The default **User Name** = **root** and **password** = **private**. Click the Connect button. If the connection succeeds, it will be indicated by a pop-up. If the connection fails, see §21.1. The password can be modified later on via §8.2.2.
3. HiProvision administrator user: Assign a new password to the HiProvision master administrator by filling it out in the password field. Retype the password for confirmation. The password can be modified later on via §8.2.2.

4. Click the Create/Select button to create the user database, including the master administrator user with its password and some other predefined users in each group.

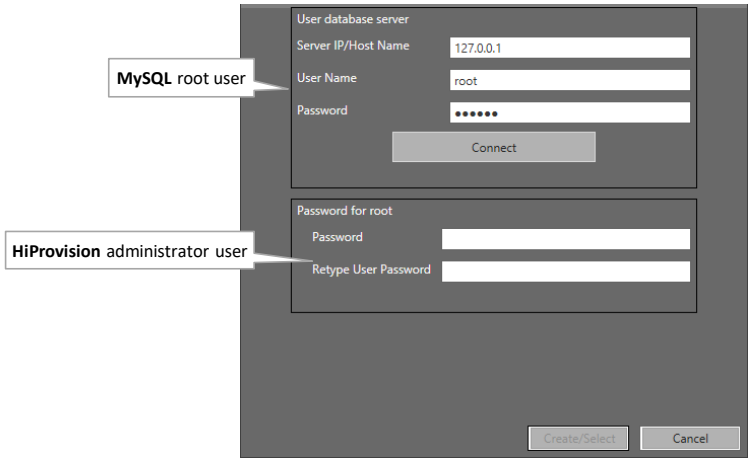


Figure 11 Configure Passwords for MySQL and HiProvision Administrator User

5. Click OK in the pop-up window indicating that the connection with the servers has failed, and restart the HiProvision Client.
6. From now on, the dashboard could look as in the figure below. This dashboard offers a compact overview of the entire HiProvision, which allows to manage the Dragon PTN network. The dashboard tab is fixed and thus cannot be closed.

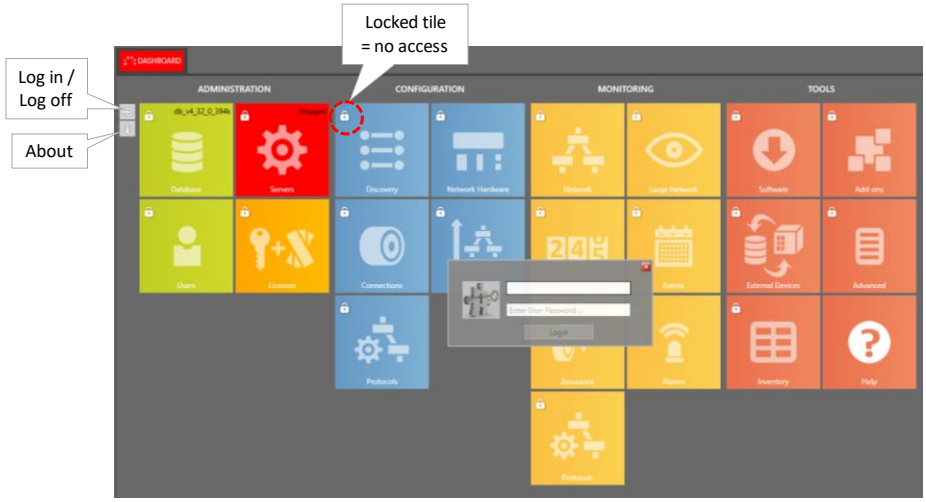


Figure 12 HiProvision Client – Dashboard

2.4.2 Log In

1. All tiles, except the Help tile, are locked (white lock icon). Log in first via the login box. If this is the first time login (e.g. after installation) or no administrators are created yet, fill out the credentials of the default admin user (user = admin, password = admin).
2. A successful login unlocks all the ADMINISTRATION tiles.

NOTE: Log in/log off can always be done via clicking / ;

NOTE: HiProvision User Management, including RADIUS authentication, is described in detail in Ref. [15] in Table 1;

2.4.3 Create Network Configuration Database

1. Click the Database tile to open the Database tab in the figure below.
2. If you have chosen a custom installation path for MySQL Server at installation, change the default path first into the custom path via the options button.
3. Create a (network configuration) database by clicking the button for a new database or by selecting an existing database from an older version and click the select button to start the migration of the older database to the newest version (see §8.6).
4. The newly created database shows up in the list and must be selected via clicking the select button. The selected database, indicated by a green border, will be used in HiProvision for further network configurations. If desired, another database can be selected by clicking the button again.

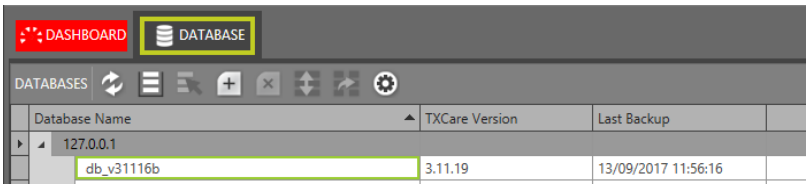


Figure 13 Network Configuration Database

2.4.4 Start Servers

NOTE: If you have installed HiProvision Agent as a service, and you start HiProvision for the first time, the Servers are already running by default, so you don't have to start them manually anymore as described below.

1. Click the Servers tile in the Dashboard to open the Servers tab in the figure below.
2. Click the button to start the HiProvision servers. A Startup Progress bar increases.

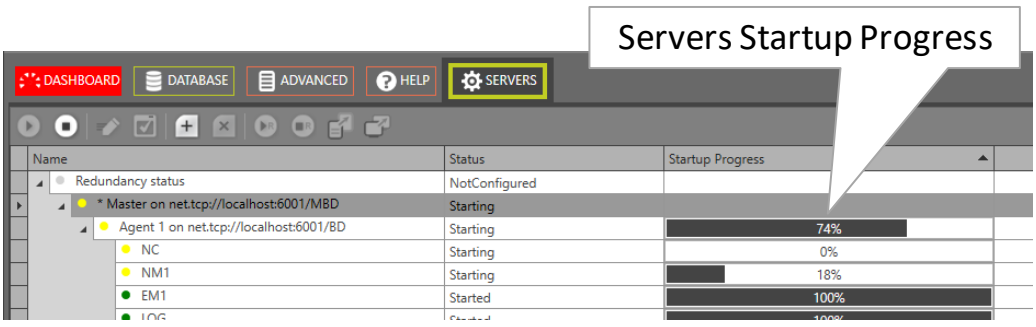


Figure 14 Servers Startup Progress

3. If this is the first time that the servers are started, the HiProvision processes must be allowed to pass through the firewall. Enable all the checkboxes for each window or process.

4. The servers are started when the Status has changed from Stopped into Started and the progress bar indicates 100%. A successful start also results in a green Servers tile. If the servers do not start, see §21.7.

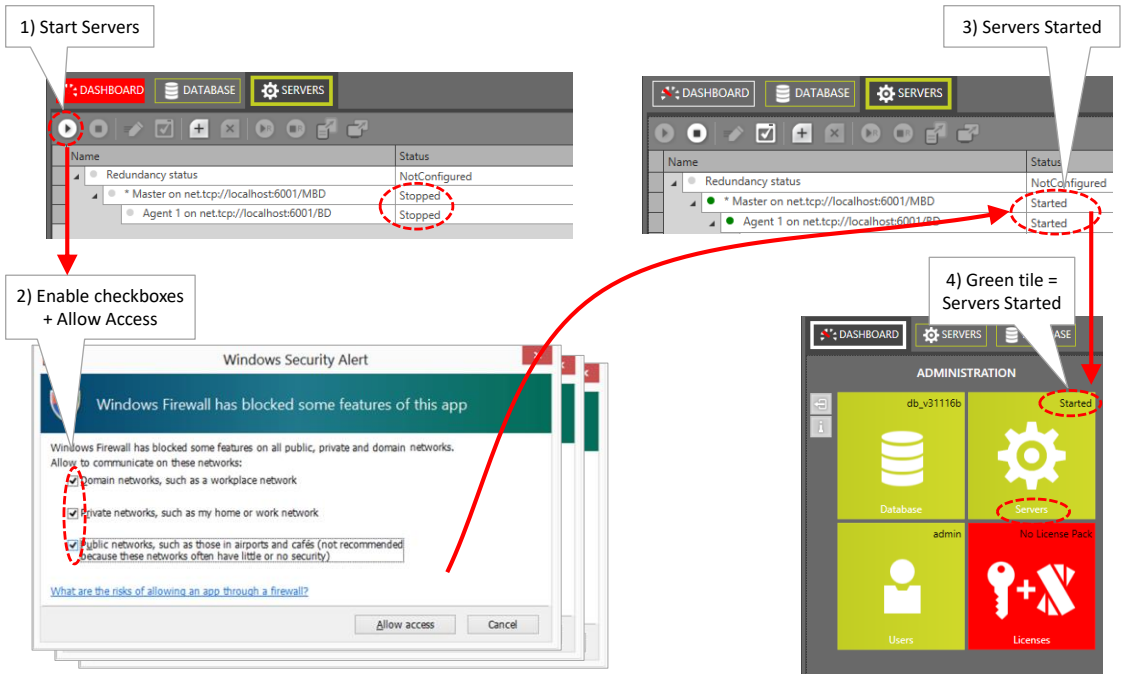


Figure 15 Start HiProvision Servers

5. Once the servers have been started, most of the ADMINISTRATION tiles turned green and most of the other tiles got unlocked (no more white lock). HiProvision is ready to discover the Dragon PTN network. Your dashboard tab could look as follows:

Figure 16 Dashboard: HiProvision Almost Ready for Management

2.4.5 Install License Pack

a. Verify Serial Key, Dragon PTN Release, HiProvision Version

Clicking the icon on the left-hand side shows ‘Dragon PTN Release a.b [HiProvision vW.X.Y.Z]’ and the serial key used for installation. See figure below.

- a.b.c = Dragon PTN Release;
  - W.X.Y.Z = HiProvision Version;

A major Dragon PTN Release upgrade requires a ‘Dragon PTN upgrade license’.In a major upgrade, ‘a’ in ‘a.b.c’ increases. A major upgrade example: from Dragon PTN Release 3.1 to 4.3. See also §4.

Figure 17 [i] Window: Dragon PTN Release, HiProvision Version, Serial Key

b. Generate and Install License Pack

1. Have your serial key ready. The serial key can be found via the 'Licenses' tile or via the Info window on the left-hand side.
2. Have your purchased voucher numbers ready. After having purchased vouchers, you have received a mail with voucher numbers in it. For more background info, read the entire chapter §4 first.
3. Follow the steps in §4.4 to install the licenses.

2.4.6 Used Language

HiProvision supports multiple languages:

- English (=default): no voucher or license required;
- German, Spanish, Chinese, Polish: voucher or license required, see §4.2.

The used language in HiProvision depends on the logged in user. If no user is logged in yet, the HiProvision tiles will be displayed in English (=default language).

A language can be configured per HiProvision user after logging on. This must be done via the Dashboard → Users tile in the 'HiProvision User Management', see Ref. [15] in Table 1.

If you want to run HiProvision in a language (e.g. Chinese, Polish, …) different from the current language (e.g. English), follow the steps below:

- If no user is logged in yet, the default start-up language is active:
  - Log in via : HiProvision will run in in the language assigned to the logged in user;
- If a user is already logged in:
  - Servers are not running:
    - Log in via : HiProvision will run in the language assigned to the logged in user;
  - Servers are running:
    - Close HiProvision and restart it (only the Client, the Agent must not be restarted) or stop the Servers;
    - Log in via : HiProvision will run in the language assigned to the logged in user. Note: When a user tries to logon with a different user language when the servers are running, following warning pops up: 'The specified language for this user cannot be used at the moment. Please restart HiProvision or login with a different user.'

NOTE: A restart of HiProvision will always run HiProvision in the default language;

2.5 HiProvision: Discover and Approve the Dragon PTN Network Topology (DCN)

2.5.1 General

Prerequisites:

- HiProvision must be able to ping the CSM front IP address (see §2.5.7) or device in the Dragon PTN network to which it is connected;
- The initial administration phase in HiProvision must have been successfully finished. See previous paragraphs.

Network Discovery will mainly do two things:

- Automatically set up a management path or DCN Channel in the live Dragon PTN network. This entire management path is called the Dragon PTN communication network. DCN = Data Communication Network. The bandwidth for this DCN Channel can be found in Ref. [1Net] in Table 1.
- Discover and visualize all the devices and links, it prepares HiProvision to approve (= to take a snapshot of) the Dragon PTN network topology.

Find more info in the paragraphs below:

- Discovery Tile / Menu Buttons / States: see §2.5.2;
- Discover Network Topology via Discovery Entry Point: see §2.5.3;
  - HiProvision connected to one Dragon PTN network;
  - HiProvision connected to multiple Dragon PTN networks;
- Approve the network topology: see §2.5.4;
- Redundant Discovery Entry Point: see §2.5.5;

- Routed DCN: see §2.5.6;
- CSM Front IP Address: see §2.5.7;
- Change the Device IP Range of the Dragon PTN Network: see §2.5.8.

2.5.2 Discovery Tile / Menu Buttons / States

Go to Dashboard → Discovery tile. A short description of the menu buttons and different discovery states are listed in the tables below.

Table 4 Discovery Menu Buttons

Button	Short Description
Discovery Entry	
	Create discovery entry point.
	Create redundant discovery entry point, see also §2.5.5.
	Delete selected discovery entry point.
	Activate the redundant or standby discovery entry point, see also §2.5.5.
	Approve the entire network topology which sets the expected Device IDs for all devices in the entire network.
	Clear the entire network approval which clears the expected Device IDs for all devices in the entire network.
	Modifies both the administration and authentication V3 SNMP passwords and applies it to the discovered devices.
	Apply the current configured V3 SNMP passwords to all the discovered devices, e.g. can be used after adding a new device into the live network.
	Deploy a new custom Device IP Range in the Dragon PTN network. This step is required if your HiProvision PC belongs to a routed network that has subnets with IP Ranges that conflict with the default Dragon PTN Device IP Range (10.255.x.y/16), see §2.5.8.
	Factory reset the Device IP Range in the Dragon PTN devices to 10.255.x.y/16.
	Refresh button. Click this button if you think the GUI has not updated the screen according to the real situation.
Devices	
	Expand/Collapse the devices treeview.
	Auto create devices: Clicking this button automatically creates the selected network element(s) in the HiProvision database. The parameters of the auto-created network elements will have default values.
	Clear neighbor approvement and IP addresses: Use this button in case of link problems or if you want to insert/remove devices. This button is only active if you select a LinkEndPoint (or port). Clicking this button clears the expected IDs from the selected LinkEndPoint and it clears the IP addresses on the link. As a result, the link will be renegotiated so it becomes up and running and ready to be Approved (state 'Not Approved').
	Search functionality to sort/group network elements in a better way.
	Refresh button. Click this button if you think the GUI has not updated the screen according to the real situation.
	Auto creation status in database, see §2.6.1 for more information.
Links	
	Expand/Collapse the links treeview.

Button	Short Description
	Auto create links: Clicking this button automatically creates the selected links in the HiProvision database. The parameters of the auto-created links will have default values.
	Link approval: Clicking this button approves and sets the selected link to 'OK'.
	Refresh button. Click this button if you think the GUI has not updated the screen according to the real situation.
	Auto creation status in database, see §2.6.1 for more information.

Table 5 Discovery: Poll States

Poll State	Short Description
Discovering	Start of the HiProvision Discovery process.
Connecting	HiProvision is still discovering/measuring at least one network element in the network. This phase remains until all network elements have been measured.
Ready	All network elements have been discovered/measured.
Standby	Used in case of Redundant Entry points. This Entry Point is standby and ready to take over when the other Entry Point fails. See also §2.5.5.

Table 6 Devices: Neighbor Communication

Neighbor Communication	Status (*)	Priority (**)	Short Description
Not Approved (no border)			
Not Connected	Green	1 (=lowest)	No cable is plugged in on a WAN port, but not approved yet.
Connected	Green	2	The WAN port communicates with the connected device, but not approved yet.
No Communication	Red	3 (=highest)	Error: The WAN port cannot communicate with the device connected to it. It is possible that the connected device is a replaced device with an invalid IP address configuration, but not approved yet. ACTION: select the LinkEndPoint row and Clear Neighbor Approvement and IP Addresses ().
Approved (green/red border, green = OK, red = Error)			
OK - Not connected (Green border)	Green	1 (=lowest)	No cable is plugged in on a WAN port and this is desired, has been approved.
OK - Connected (Green border)	Green	2	The WAN port can communicate with the device connected to it, and this is desired, has been approved.
No Communication (Red border)	Red	3	Error: Same as 'No Communication' description above but Approved.
Missing (Red border)	Red	4	Error: In the OK - Connected state, the WAN cable has been pulled out. ACTION: put in the existing cable again or Clear Neighbor Approvement and IP Addresses on this link (Devices: ) for new links/devices and approve the new situation (Links: ).
Not Allowed (Red border)	Red	5 (=highest)	Error:

			- In the OK - Connected state, a wrong or unexpected device has been connected to the WAN port. ACTION: connect the expected device again or Clear Neighbor Approvement and IP Addresses on this link (Devices:) for new links/devices and approve the new situation (Links:). - In the OK - Not Connected state, something has been connected to the WAN port. ACTION: remove the cable or Clear Neighbor Approvement and IP Addresses on this link (Devices:) for new links/devices and approve the new situation (Links:).
(*) Status: 'orange': HiProvision is rediscovering (or connecting) this network element, e.g. due to a change in the network; (**) Priority: The Neighbor Communication is the state of the selected network element or the worst resulting state (=state with the highest priority) of its child elements, if any. Example: An IFM has a 'Missing' (=prio 4) state on port 1 and a 'Not Allowed' (=prio 5) state on port 2. The IFM will show the 'Not Allowed' state because it has the highest priority.			

Table 7 Links: Discovery

Discovery	Short Description
OK (Green border)	The link has been discovered/measured by HiProvision and approved via ;
Not Approved (Red border)	The link has been discovered/measured by HiProvision but not approved yet ;

2.5.3 Discover Network Topology via Discovery Entry Point

a. HiProvision Connected to One Network

- Configure the connection with the first CSM: Create Discovery Entry Point via clicking + in the 'Discovery Entry' section and fill out an Entry Point Name.

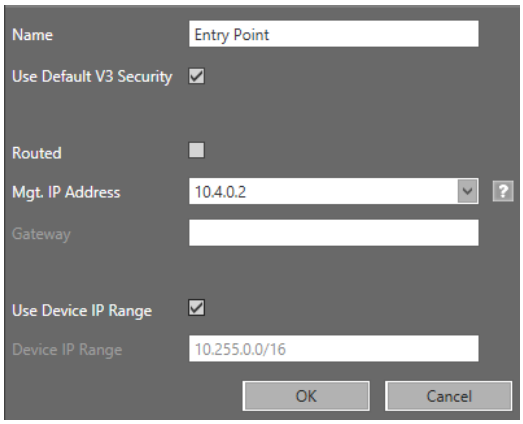


Figure 18 Create Discovery Entry

  - First CSM = CSM in node to which the HiProvision PC has been connected;
  - Entry Point = CSM management connector that interconnects a HiProvision PC with the Dragon PTN network;

- Keep the default SNMP settings ('Use Default V3 Security' = username, authentication password, private password). If your network already had a customized SNMP

authentication in the devices, uncheck ‘Use Default V3 Security’ and fill out the credentials already available in the network.

- Routed: check this if your HiProvision PC is connected to the Dragon PTN network via a routed network, see §2.5.6.
- Mgt. IP Address: fill out the CSM front IP address of the first node via which HiProvision connects to the Dragon PTN network. This address can be viewed via the display on the CSM.
- Gateway: This field becomes active when Routed has been checked, see §2.5.6.
- Use Device IP Range (default = checked) / Device IP Range:
  - Unchecked:
    - Use only when you have multiple entry points and each entry point is connected to only one node;
    - With only a single node, no Device IP Range is needed or used. Instead, only the CSM front IP address of the connected node will be used. As a result, no additional routes in the router must be configured in case of a routed network;
  - Checked (=default):
    - Must be used when the entry point connects at least to two nodes;
    - The Device IP Range is the IP address range used by HiProvision to assign a unique address to the devices and to reach the device in the Dragon PTN network. If the Mgt. IP Address is reachable (detection phase is maximum 20 seconds), the network can be detected. As a result, the detected Device IP Range is filled out automatically and greyed out. If the Mgt. IP Address is not reachable (e.g. offline), the Device IP Range can be filled out manually after the detection phase. In a detected live network, the device IP range can always be adapted, see §2.5.8. If the HiProvision PC has only one NIC, it does not matter which Device IP Range is selected. If HiProvision has more than one NIC, change the Device IP Range in such a way that the different IP networks connected to the HiProvision NICs, do not interfere with each other's Device IP Ranges.
- The network discovery starts immediately after the Entry Point has been created → **PollState = Discovering → PollState = Connecting** (see figure below);

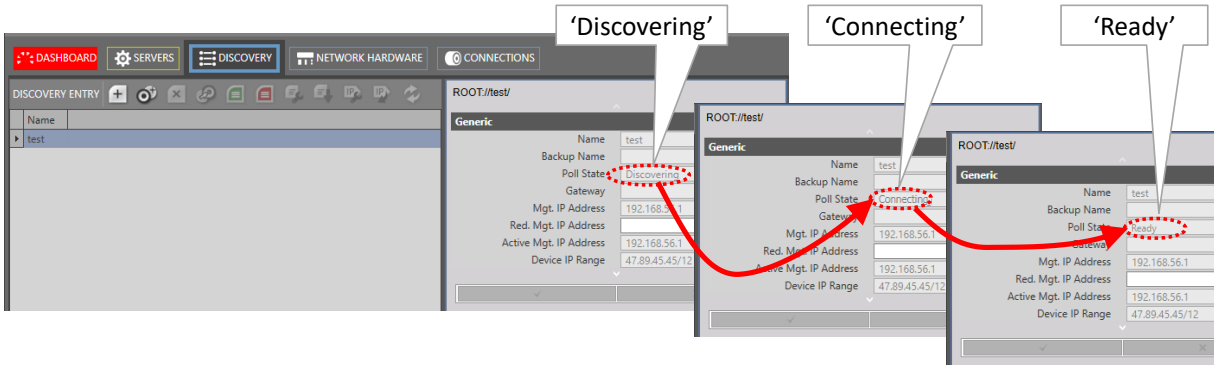


Figure 19 Discovery PollState

- In the discovering and connecting state:

- The Devices/Status column shows an orange bullet;
- The discovered devices will pop-up almost instantly within a few seconds in HiProvision. Each discovered device will automatically get a device IP address. A DCN will be set up automatically over the entire Dragon PTN network, see Ref. [1Net] in Table 1.

NOTE: DCN is an in-band Dragon PTN communication network which is only used by HiProvision to manage the Dragon PTN network.

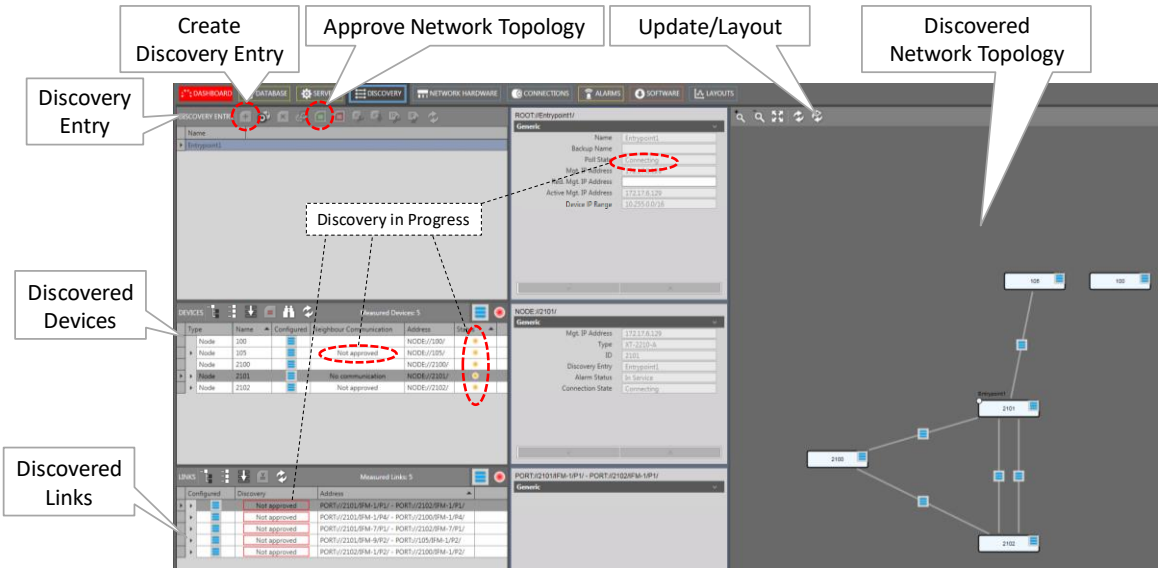


Figure 20 Network Discovery in Progress: Connecting

- Finally, the entire network (devices + links) is discovered and visualized in HiProvision: **PollState = Ready**. Also the number of discovered or measured devices and links is shown.
  - Devices:
    - Neighbour Communication column:
      - First time discovery: network elements that are discovered for the first time show 'Connected' or 'Not Connected', they still have to be approved, see §2.5.4.
      - Network element already discovered and approved before: network element cell indicates 'OK - Connected' or 'OK - Not Connected' with a green border. Any other state/color indicates that something is wrong or unexpected, see Table 5 for more info;
    - Status column:
      - Green bullet: the network element and all its underlying child elements are not approved yet or approved and OK according to the approved network expectations;
      - Red bullet: the network element or one of its underlying child elements is in 'No Communication' or in another error state with a red border meaning a violation against the approved network expectations, see Table 5 for more info;
      - Orange bullet: the network element or one of its underlying child elements is again in connecting state meaning that HiProvision is (re)discovering that network element because something has changed in the network connections of that element, e.g. a cable has been pulled out.

- Links: Discovery column:
  - First time discovery: a first time discovered link shows 'not approved' with a red border;
  - Link already discovered and approved previously: the link indicates 'OK' with a green border;
  - If an expected link is not shown in the list, it means that the link is not there and not measured. The link cable is probably pulled out, check your hardware;
- Click the Update/Layout button to update and layout the discovered devices properly;
- If the full discovered network visualization is NOT as expected, it might mean that you have forgotten some links or that you have misconnections. Verify your hardware and adapt the physical links where needed, see Ref. [1Net] in Table 1. The discovery function will automatically and almost instantly within a few seconds rediscover the modified network after changing the hardware configuration. Repeat this step until the visualization is as expected;

NOTE: The network layout in the Discovery tile is independent from the layouts available in the Layouts tile in §15.2.

NOTE: Hardware and Links Reporting information is available via the Reporting Engine Add-on, see §17.4.

b. HiProvision Connected to Multiple Networks

Per network to which HiProvision is connected, a new Entry Point must be created. Each entry point, connected to at least two nodes, must have its own unique Device IP Range. Unique means non-overlapping with the Device IP Range of the other Entry Points. A basic example is shown in the figure below. To change the Device IP Range in the Entry Point, see §2.5.8.

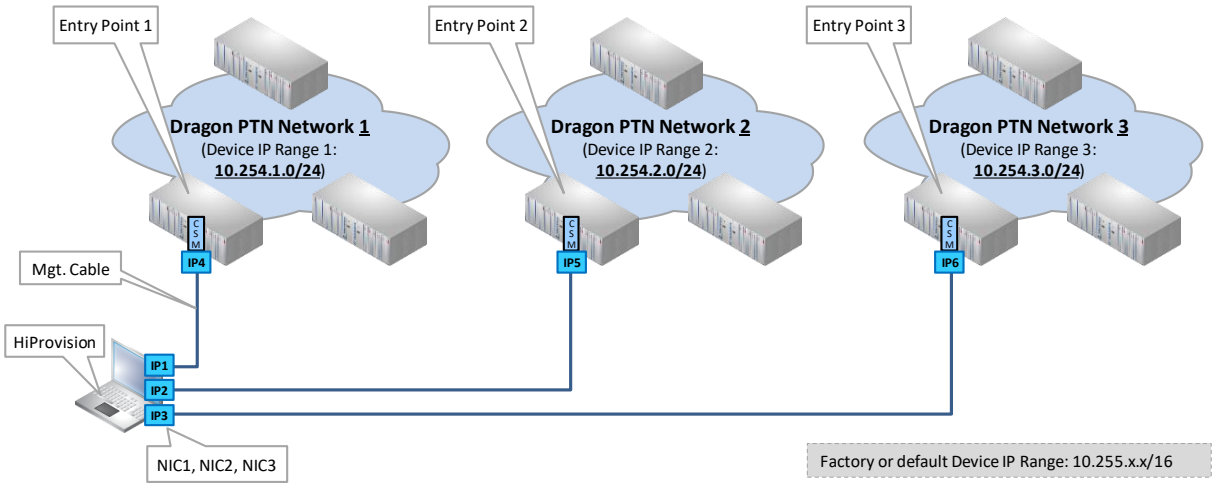


Figure 21 HiProvision Connected to Multiple Dragon PTN Networks

2.5.4 Approve Network Elements in the Network

Depending on the situation, you can either:

- Approve the entire network after a first time discovery;

- Approve one or some network elements after network modifications.

a. Approve Entire Network after First Time Discovery

Prerequisite:

- The network topology has been fully discovered (PollState = 'Ready') and its visualization is as expected;
- Understand measured/programmed (=expected)/configured values, see §9.2:

Approving the network topology means taking a snapshot of the discovered network that meets your expectations, and storing this expected snapshot into the network. As a result, every device will always expect the same neighbor device and links according to the stored snapshot.

After approving the network topology, any link alteration (e.g. broken link…) or device change (e.g. missing, unknown, intruder device….) in the network afterwards will cause a mismatch against this network snapshot and run into error states with red borders (see Table 5) and alarms in the dashboard.

- Unapproved network topology = network with no expectations, see Table 8;
- Approved network topology = network snapshot or expectations fully loaded into the network, values are according to Table 8;

Table 8 Unapproved/Approved States In Normal Situation

Section	Column Name	Column Value	
		Unapproved Network	Approved Network
Devices	Neighbor Communication	Not Approved / Not Connected	OK - Connected / OK - Not Connected
Links	Discovery	Not Approved	OK

Take a snapshot or approve the entire network topology in one click as follows:

- Click the  button in the Discovery Entry section. This action:
  - Copies all the measured values into the expected values in the devices;
  - Sets Approved values in Table 8. If a link is still 'Not approved' afterwards, select the row of this link and click the  button to set the link to 'OK'.

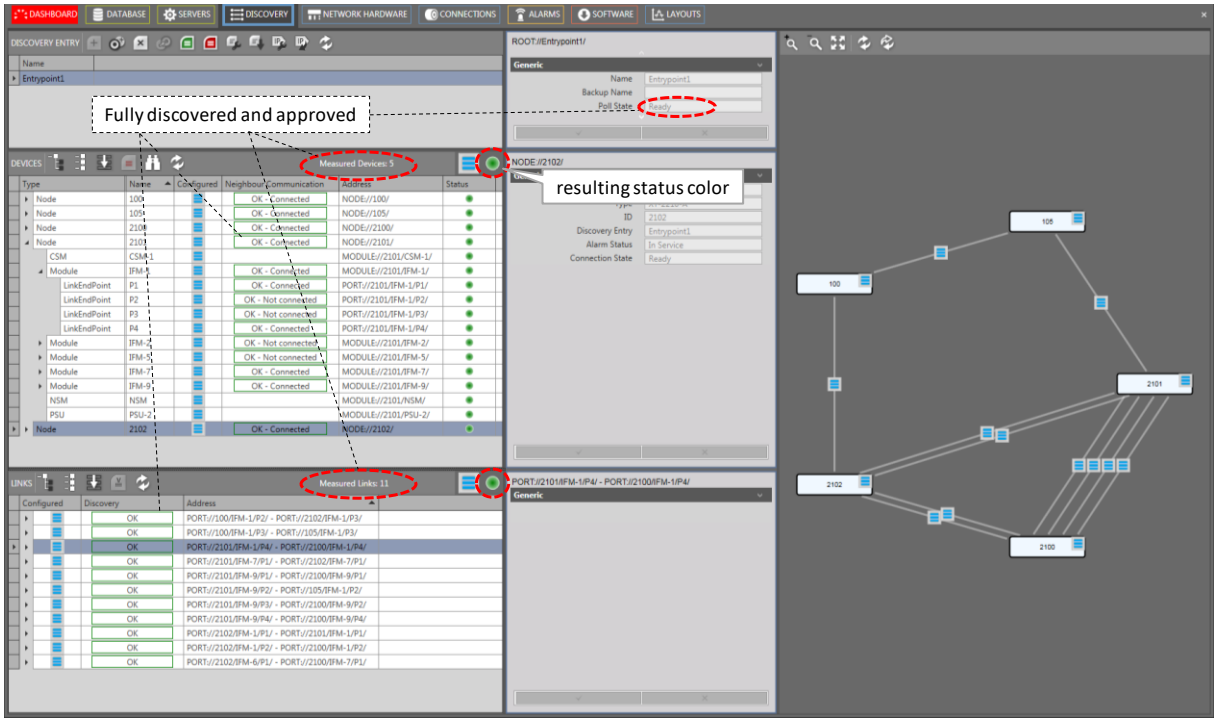


Figure 22 Network Fully Discovered and Approved: Ready/Measured Devices and Links

b. Approve Single Network Elements after Network Modifications

If small adaptations are done in an already approved network, e.g. an extra inserted device, an extra link etc... The impacted and neighbor network elements run into an error state with a red border, the other network elements remain OK. To solve these issues, follow the actions for the detected errors in Table 5.

2.5.5 Redundant Discovery Entry Point or Cable Connection

a. General

A redundant discovery entry point must only be created when one HiProvision PC needs two access points via two management cables into the Dragon PTN network, as a precaution to a management cable break.

NOTE: Redundant discovery entry points always share the same Device IP Range (or go to the same Dragon PTN network), whereas two individual created entry points always have a unique Device IP Range (or each go to a different Dragon PTN network);

It is strongly advised to do this! This feature is called ‘Dual Access Discovery Entry Points’.

Number of NICs required in the Dragon PTN PC when configuring a redundant entry point:

- two NICs: each NIC is directly connected to the Dragon PTN network via a management cable;
- one NIC: the NIC is connected to a switch which is connected via two management cables to the Dragon PTN network. Two IP addresses, one for each access point, must be configured on the HiProvision NIC, see §2.1.3b.

When a cable break occurs with only one management cable between the HiProvision PC and the Dragon PTN network, the HiProvision PC loses connection with the Dragon PTN network. As a result, the Dragon PTN network stays alive but cannot be monitored/configured anymore.

NOTE: When two redundant HiProvision PCs each have one management cable connected to the network (see §11.7), it means only one discovery entry point per PC, no redundant discovery entry points are involved in this case.

b. Create Redundant Discovery Entry Point

Follow the steps below:

- Install a second NIC (if not already available) in the HiProvision PC and connect this NIC to another CSM in the same node (=redundant CSMs) or a CSM in another node as described in §2.2;
- Click the active or first entry point in the entry point list to highlight the icon;
- Create the redundant entry point by clicking. It is similar as described in §2.5.2;
- After the redundant discovery, two entry points (in our example Entry Point1 and Entry Point2) will be visible in the list, see figure below:
- Which entry point is the active one, which one is redundant or standby?
  - PollState = Ready → active entry point;
  - PollState = StandBy → standby entry point.

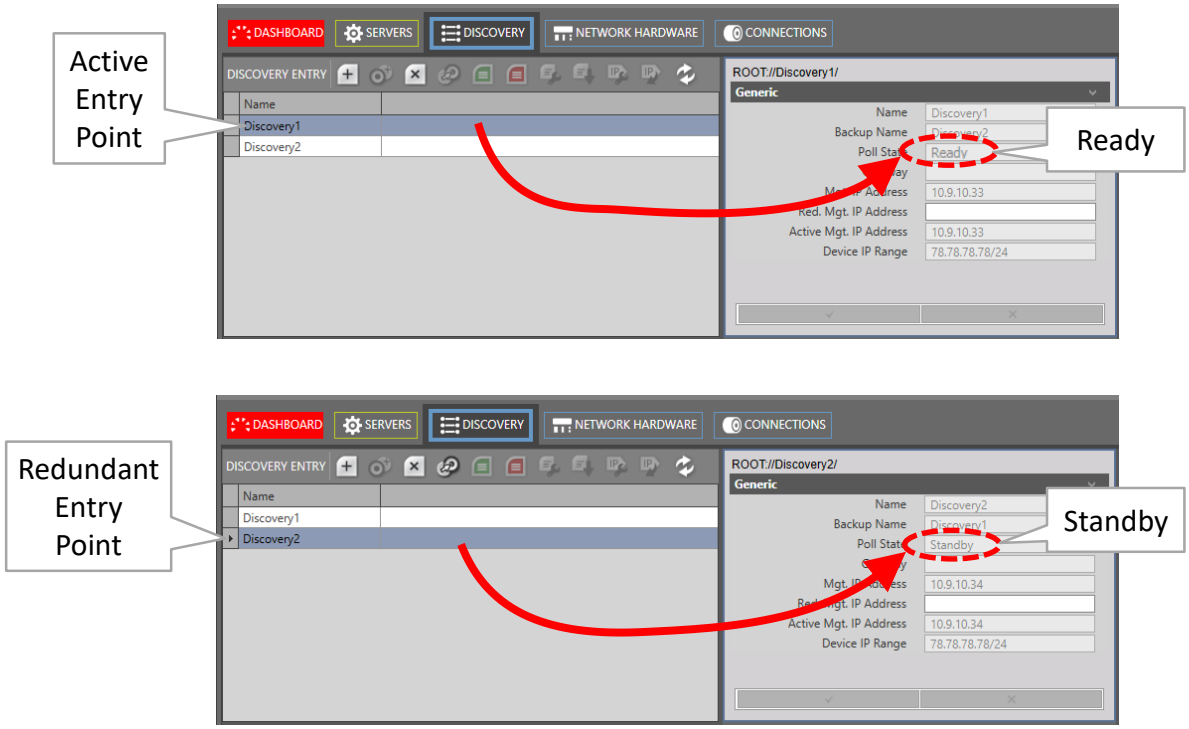


Figure 23 Active/Redundant Discovery Entry Point

c. Switchover Active and Standby Entry Point

There are three ways to switch over from the active to the standby entry point.

- Automatically via a NIC-CSM cable break of the active entry point;
- Manually via clicking the button
- Connected CSM not reachable (e.g. reboot due load action sync...)

A switchover:

- makes the standby entry point the new active one, its PollState turns into 'Discovering' and finally results in 'Ready';
- makes the active entry point the new standby one, whatever the reason for the switchover was (manual, broken link, ...), its PollState turns into 'Standby'.

Revertive/Non-revertive behavior:

- The redundant entry points are always non-revertive: once a switchover of the entry point has occurred, the new active point stays active until a manual switchover or switchover caused by a cable break occurs again. No automatic switchback to the original entry point will occur, not even when a possible cable break has been recovered.

2.5.6 Routed DCN

a. General

The Dragon PTN discovery can be done via a routed management network where at least one router is between the HiProvision PC and Dragon PTN, see figure below. The routed DCN is only possible when the Routed checkbox has been checked in the Entry Point creation.

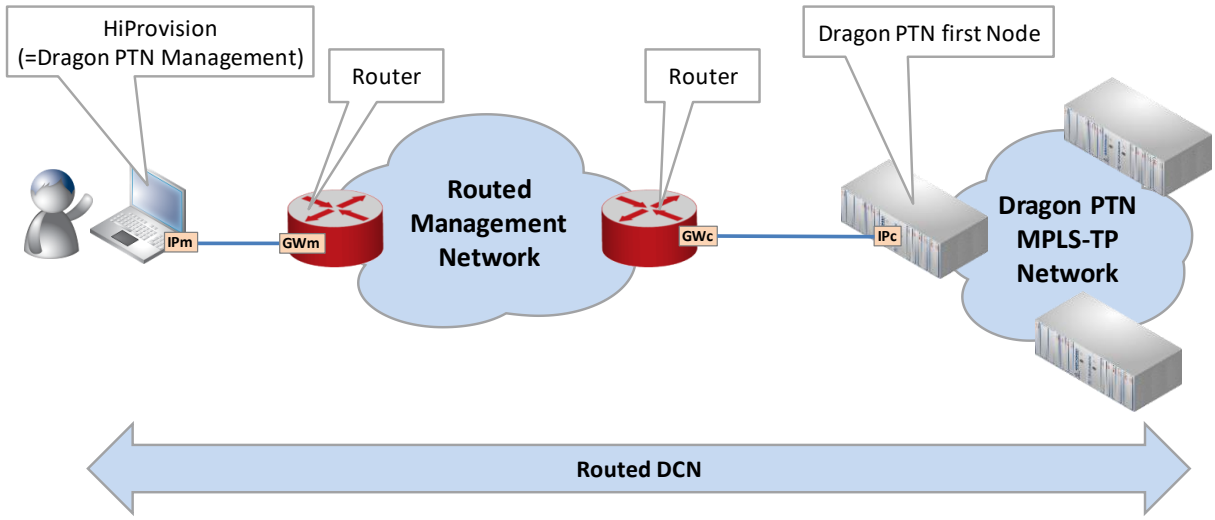


Figure 24 Routed DCN: Routed Management Network

b. Configuration: NIC in HiProvision PC

- In the IP Protocol settings of the NIC on the HiProvision PC, configure:

- IP address 'IPm' (see picture above, 'm' refers to management PC);
- Gateway IP Address 'GWm';
- IP Subnet mask.

c. Configuration: CSM Gateway Address

Fill out a CSM Gateway Address 'GWc' in the CSM Front IP Address configuration to make sure that the first node can reach HiProvision again, see §2.5.7;

d. Configuration: Entry Point: Routed + Gateway Address

Create an Entry Point as described in previous paragraphs and check the 'Routed' checkbox. Fill out the Mgt. IP Address 'IPc' (=CSM IP address) and the Gateway address 'GWm' in the Gateway field. The Gateway field is only active when Routed has been checked.

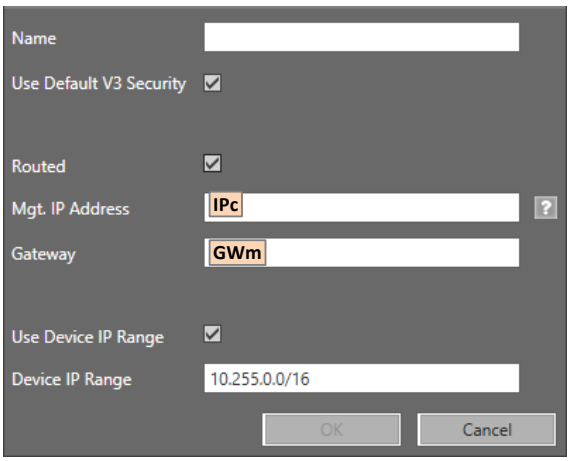


Figure 25 Entry Point with Routed Checked, Gateway Field

e. Configuration: Routers

In the routers that are directly connected to the Dragon PTN network(s), every possible path from those routers to the Dragon PTN network(s) must be configured as a static route. Via a routing protocol in the Routers (e.g. OSPF), those static routes can be advertised to indirectly connected routers.

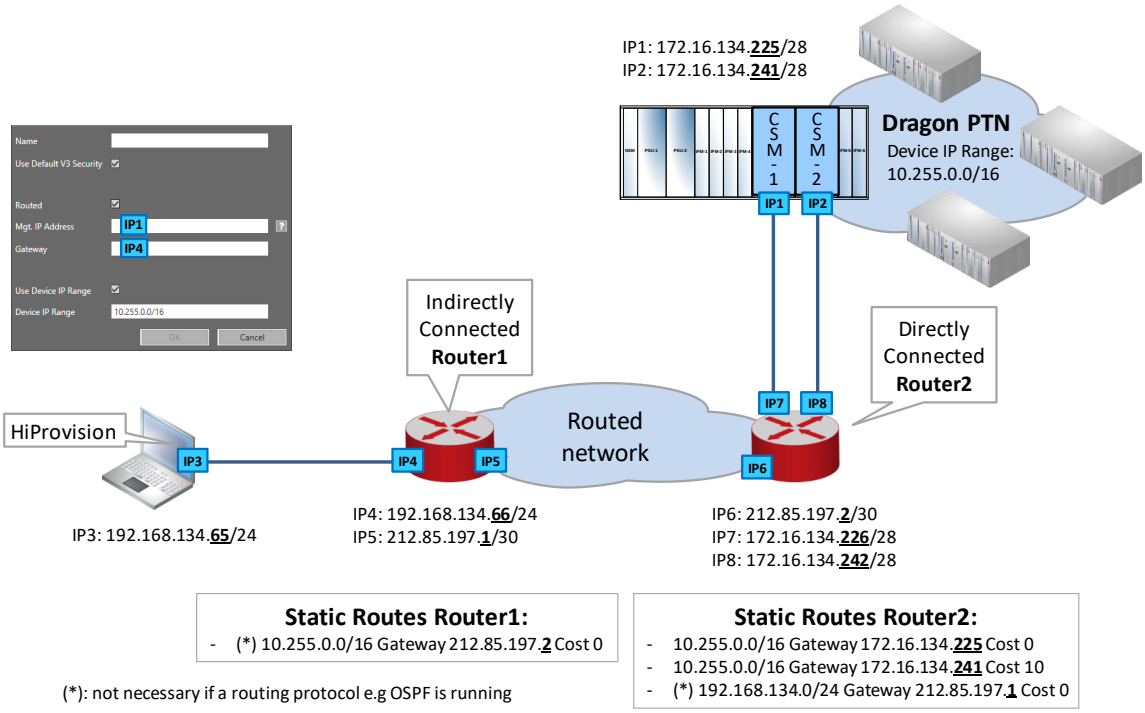


Figure 26 Routed DCN: Static Routes in Routed Network

Static Route example for directly connected routers (=Router2):

- The Dragon PTN network must be reachable via the CSM front IP address 'IP1' and 'IP2';
- Static Route: <Device IP Range> Gateway <CSM Front IP Address> Cost <cost value>;
- See example routes in figure above;

2.5.7 CSM Front IP Address

a. General

- Is the IP address on the management connector (see Figure 5) on the CSM front panel (=Mgt. IP Address in the Entry Point);
- Is the IP address via which HiProvision connects to the Dragon PTN network, local connection;
- Is default/factory in the CSM IP Range 172.x.y.z/28 and based on the node number (=device ID);
- Is used by remote client to access HiProvision via DCN;
- Must be changed when there is at least one router between the HiProvision PC and the Dragon PTN network or to avoid IP conflicts with a possible modified Device IP Range in the Dragon PTN network.

CAUTION: When changing IP addresses or IP ranges:
- Make sure that the Device IP Range of your network does not conflict with the CSM Front IP Addresses of your entry points for this network. All these IP addresses and ranges can be verified in the Entry Point(s) in the Discovery Tile.
- Make sure that the CSM Front IP address of each node only belongs to its own unique subnet. Therefor each node must be configured in a different subnet.
- Redundant CSMs can be configured in the same subnet. If they are configured in a different subnet, make sure each subnet is unique network wide.

NOTE: This management port can be disabled for security reasons via the Dashboard → Network Hardware → Devices → Node → CSM → Properties (Specific) → Management Port: Down. This management port is by default up.

- Set CSM Front IP Address via Local Connection: see §b;
- Set CSM Front IP Address via Network Connection: see §c;
- Set CSM Front IP Address on New Second CSM in Live Existing Device: see §d;
- Reset CSM Front IP Address to Factory Defaults: see §e;

b. Set CSM Front IP Address via Local Connection

By default, the node has a management IP address in the range 172.x.y.z/28 (based on the node number).

1. Power up the node that includes the CSM(s);
2. Visit the node locally and connect the HiProvision PC directly via an RJ-45 cable to the HiProvision management connector on a CSM in the node;
3. Verify the current CSM front IP address and write it down on a paper. This IP address is shown on the CSM display.
   NOTE: It can be configured in HiProvision (*) how many times ('n') the IP address must scroll on the CSM display after plugging in the management cable or rebooting the CSM. After these 'n' times, the IP address will not be displayed anymore e.g. for security reasons. If you want to show the IP address again for 'n' cycles, pull out the cable and plug it in again. By default, the IP address is always displayed in every CSM display-cycle.

   NOTE: (*) The amount of times can be configured via HiProvision → Network Hardware Tile → Devices → Select CSM → Fill out 'Display' properties. By default the field shows '-1' indicating that the value is displayed forever, '0' means never, 'n' with n > 0 means n times.

4. Configure the IP address of the HiProvision PC (**) in the same IP address range as the one of the device. This can be done in the IP Protocol settings of the NIC (=Network Interface Card) on the HiProvision PC: configure IP address, IP Address subnet mask (Gateway will be filled out automatically later on by HiProvision, when configuring a routed entry point, see further);
   NOTE: (**) This is just a temporary IP address for HiProvision to interconnect with the node.

5. Go to Dashboard → Advanced (TOOLS) → CSM Front IP Addresses;

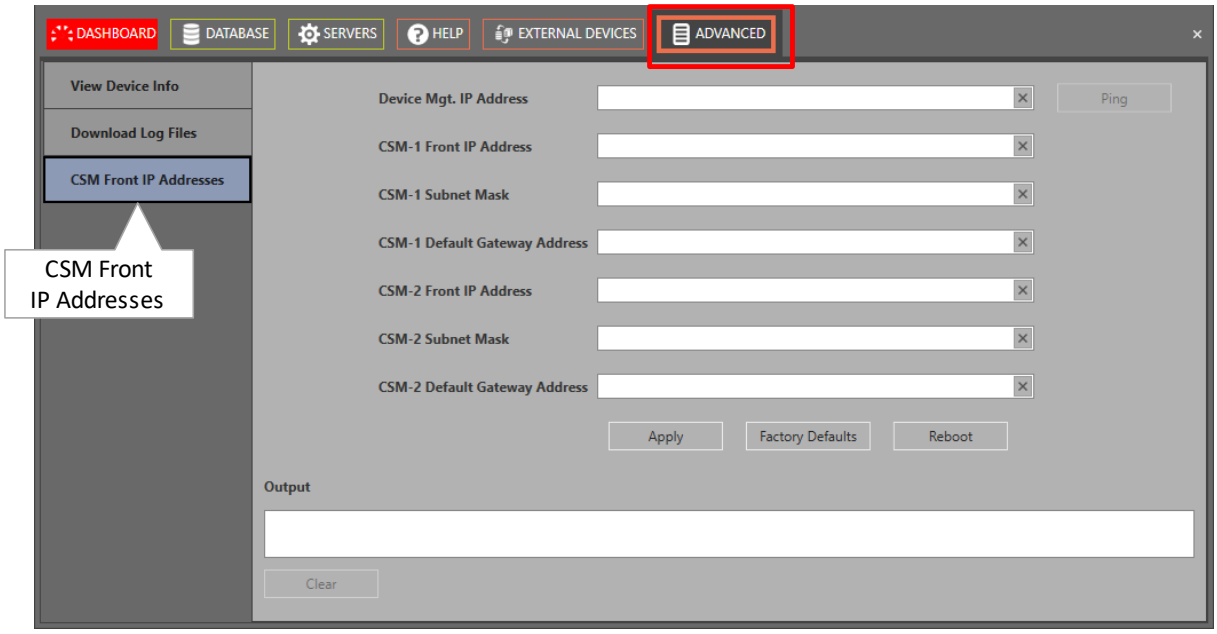


Figure 27 Advanced Tab: CSM Front IP Addresses

6. Fill out the current IP address of the CSM in the 'Device Mgt. IP Address' field and click 'Ping' to check whether the HiProvision PC can reach the node;
7. If the node is reachable, change the CSM IP address by filling out the new unique IP information per CSM. If you have redundant CSMs, fill out both the CSM-1 and CSM-2 fields. If only one CSM resides in the node, fill out the CSM-1 (CSM is plugged in on the left-hand CSM slot) or the CSM-2 (CSM is plugged in on the right-hand CSM slot) fields.
   - '<CSM-1/CSM-2> Front IP address of the node;
   - '<CSM-1/CSM-2> Subnet Mask' of the node;
   - '<CSM-1/CSM-2> Default Gateway Address of the node (only necessary if a router is between this node and the HiProvision PC).
8. Click Apply. Click Reboot and confirm the pop-up;
9. After the reboot of the node, the new IP address(es) will be set on the node or CSM(s).
   NOTE: As of now, the node will be unreachable for the HiProvision PC when the HiProvision PC IP address range mismatches the new CSM IP address range(s);
10. Configure the IP address of the HiProvision PC again in the new and same IP address range as the connected CSM to verify it is reachable again.

c. Set CSM Front IP Address via Network Connection

It is possible to change the CSM front IP address of any other node in the network, while HiProvision not being locally connected to that node. This can be useful if you want to prepare the IP configuration for a redundant set up and connection in your network.

1. In Figure 27 in the 'Device Mgt. IP Address field', just fill out the Mgt. IP address (*) of the node with the CSM that must be have another IP configuration. Click 'Ping' to check whether the HiProvision PC can reach the node;
   NOTE: (*): The Mgt. IP address can be found in Network Hardware → select device row → Generic Properties → Mgt. IP Address. This is the IP address which HiProvision uses to manage the device. This is either the Device IP Address for

remote nodes or the CSM front IP address for the node connected to HiProvision.

2. Fill out the correct new IP address information in the other fields;
3. Click Apply. Click Reboot and confirm the pop-up;
4. The node will reboot with the new IP configuration on its CSM;

d. Set CSM Front IP Address on New Second CSM in Live Existing Device

Prerequisites: HiProvision can reach the node via the network. It is not a requirement that the second CSM is plugged in into the node to configure this IP information. The new configuration of the second CSM will be stored on the first CSM. The second CSM will get this information later on (when plugged in) from the first CSM.

1. Go to Dashboard → Advanced (TOOLS) → CSM Front IP Addresses;
2. In Figure 27, Fill out the current IP address of the device (or CSM that was already configured) in the 'Device Mgt. IP Address' field and Click 'Ping' to check whether the HiProvision PC can reach the device;
3. If the device is reachable, the IP information of the CSM already configured will be filled out. The IP information of the new CSM is filled out with zeros. Fill out or modify the fields of the new CSM, either CSM-1<IP fields> or CSM-2 <IP fields> with the new IP information.
   - '<CSM-1/CSM-2> Front IP address' of the device;
   - '<CSM-1/CSM-2> Subnet Mask' of the device;
   - '<CSM-1/CSM-2> Default Gateway Address' of the device.
4. Click Apply. Click Reboot and confirm the pop-up;
5. After the reboot of the node, the new IP address information will be configured.

e. Reset CSM Front IP Address to Factory Defaults

1. Go to Dashboard → Advanced (TOOLS) → CSM Front IP Addresses;
2. In Figure 27, Fill out the current IP address of the device that must be reset to factory defaults and click 'Ping' to check whether the HiProvision PC can reach the node;
3. If the node is reachable, the IP information of the configured CSM(s) will be filled out.
4. Click Factory Defaults and confirm the pop-up to reset the IP addresses in the CSM;
5. Click Reboot and confirm the pop-up;
6. After the reboot of the node, the new IP address information will be configured.

2.5.8 Device IP Address

a. General

- is the IP address of the device, stored in the CSM and used by HiProvision to address the devices in the Dragon PTN network via DCN;
- is default/factory in the Device IP Range 10.255.x.y/16 and based on the node number (=device ID);
- is an IP address in the Device IP Range in the Entry Point;
- can be changed, see paragraphs below.

CAUTION: When changing IP addresses or IP ranges, make sure that the Device IP Range of your network does not conflict with the CSM Front IP Addresses of your entry points for this network. All these IP addresses and ranges can be verified in the Entry Point(s) in the Discovery Tile.

b. Set All Devices in Entire Network in the Custom Device IP Range

1. Click the  button;

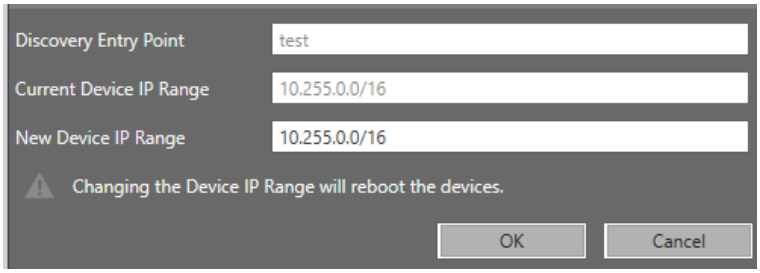


Figure 28 Change Device IP Range

2. The Current Device IP Range is shown. The New Device IP Range is by default filled out with the Current Device IP Range in the network. Fill out the new desired Device IP Range;
3. Click OK (no load action required!). CAUTION: All the devices in the network will reboot!
4. All the devices in the network will get a new device IP address in the configured Device IP Range. HiProvision will be able to communicate with these devices provided that HiProvision and the devices all reside in the same IP subnet.

c. Set New Devices in the Network in the Custom Device IP Range

If one or more devices, with an IP address in a wrong Device IP Range, are added to an existing operational network, these devices will be discovered by HiProvision but will remain grey in the network drawing. These news devices must get a new IP address in the same Device IP Range as the operational network.

1. Click the  button;
2. Both the Current Device IP Range and New Device IP Range field show the current Device IP range configured in the network.
3. Click OK (no load action required!);
4. The new devices will reboot and start up with an IP address in the New Device IP Range. The existing devices keep their IP addresses and will not reboot.
5. HiProvision will be able to communicate with these devices provided that HiProvision and the devices all reside in the same IP subnet.
6. Only new devices that are directly connected (= 1 hop) to the Dragon PTN network can be applied with the new Device IP Range. If you have added more than 1 hop, repeat previous steps for every hop until all hops have been discovered and assigned the correct IP address.

d. Factory Reset Device IP Range in the Entire Network

1. Click the  button and click OK to factory reset the Device IP Range to 10.255.x.y/16 for the entire network! CAUTION: All the devices in the network will reboot!

2.5.9 Connect HiProvision PC to another Node, Different Entry Point

By changing the HiProvision PC connection from one node to another node, the discovery entry point (see §2.5.2) changes. Follow the steps below the make a successful connection change:

- Before changing the HiProvision connection, go in HiProvision to Discovery → Discovery Entry;
- Delete the Discovery Entry by selecting it in the list and clicking  ;
- Remove the HiProvision cable from one node;
- Configure a new HiProvision IP address according to §2.1.3;
- Plug in the HiProvision cable into the other node;
- Discover the network topology again as described in, see §2.5.2;

2.6 HiProvision: Network Database Configuration

The network database configuration can be done automatically via Dashboard → Discovery or manually via Dashboard → Network Hardware.

2.6.1 Automatic Configuration via Dashboard → Discovery

In the Discovery tab, select one or multiple network element(s) (or one or more of its children) and click the auto-creation icon  to create the selected devices/links automatically in the HiProvision database. The parameters of the auto-created network elements will have default values. Whether an element has already been created in the HiProvision database is indicated by following creation-status icon in the Configured column and the network visualization.

-  = empty: network element not yet created in HiProvision database;
-  = empty + blue: network element partially created in HiProvision database;
-  = blue: network element fully created in HiProvision database.

Make sure that all the devices and links are fully created in the database. This can be easily verified by viewing the network drawing in the figure below: all creation-status icons must be blue.

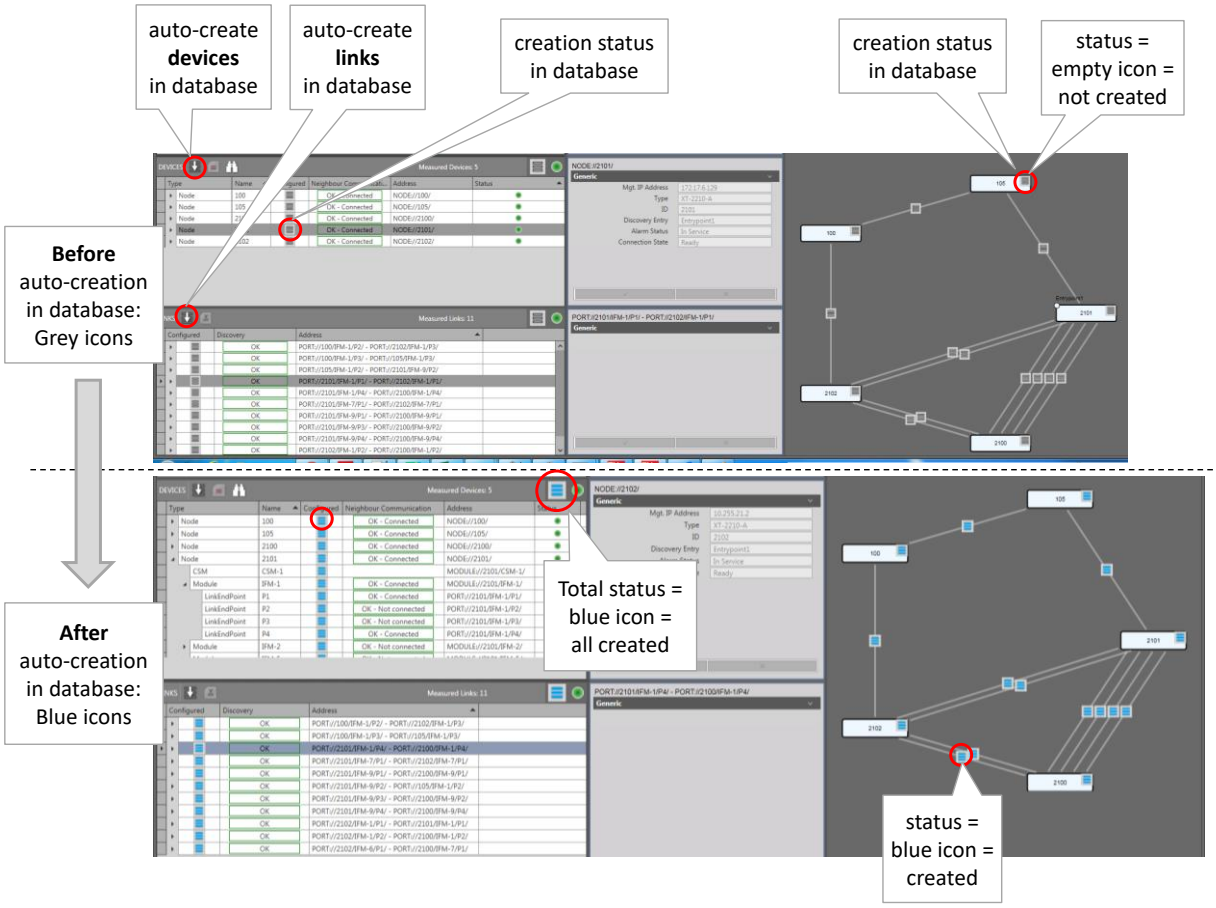


Figure 29 Discovery Tab: Auto-Creation of Network Elements in Database

2.6.2 Manual Configuration via Dashboard → Network Hardware

In this tab, device and links can be configured manually, see figure below:

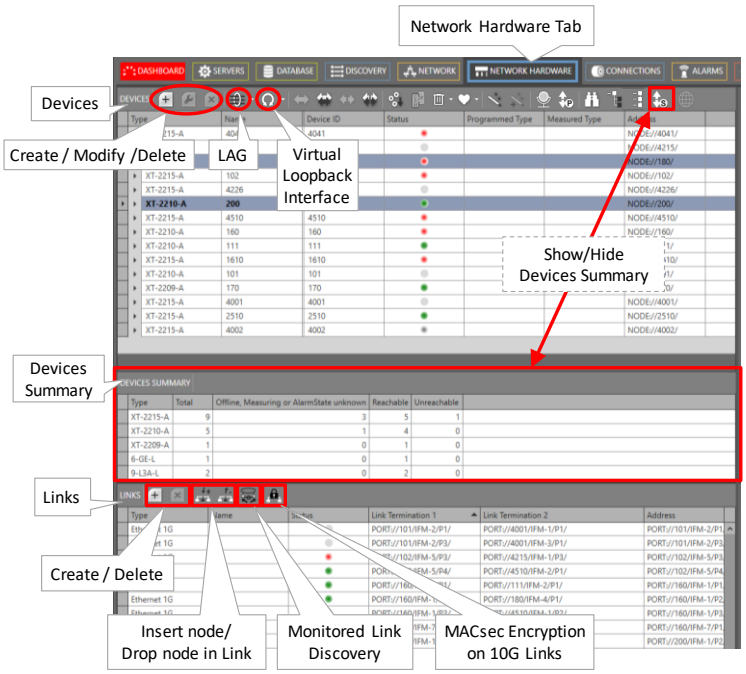


Figure 30 Manual Configuration Devices/Links

a. Devices:

- Create:
  - Page1: Fill out the name (max. 128 characters), type and ID of the device or node. The ID must be the same as the node number configured on the NSM, see Ref. [1] in Table 1. It is possible to have External Devices types (=third party devices) in the list, see §18.
  - Page2: Select a module (IFM, CSM, PSU, NSM, ….) via the module selector (scroll the list for more pictures) and drag and drop it into a highlighted slot in the node. Only the allowed slots will highlight. It is not possible to drop a module in the wrong slot. Furthermore, it is possible to delete the dropped module if necessary.

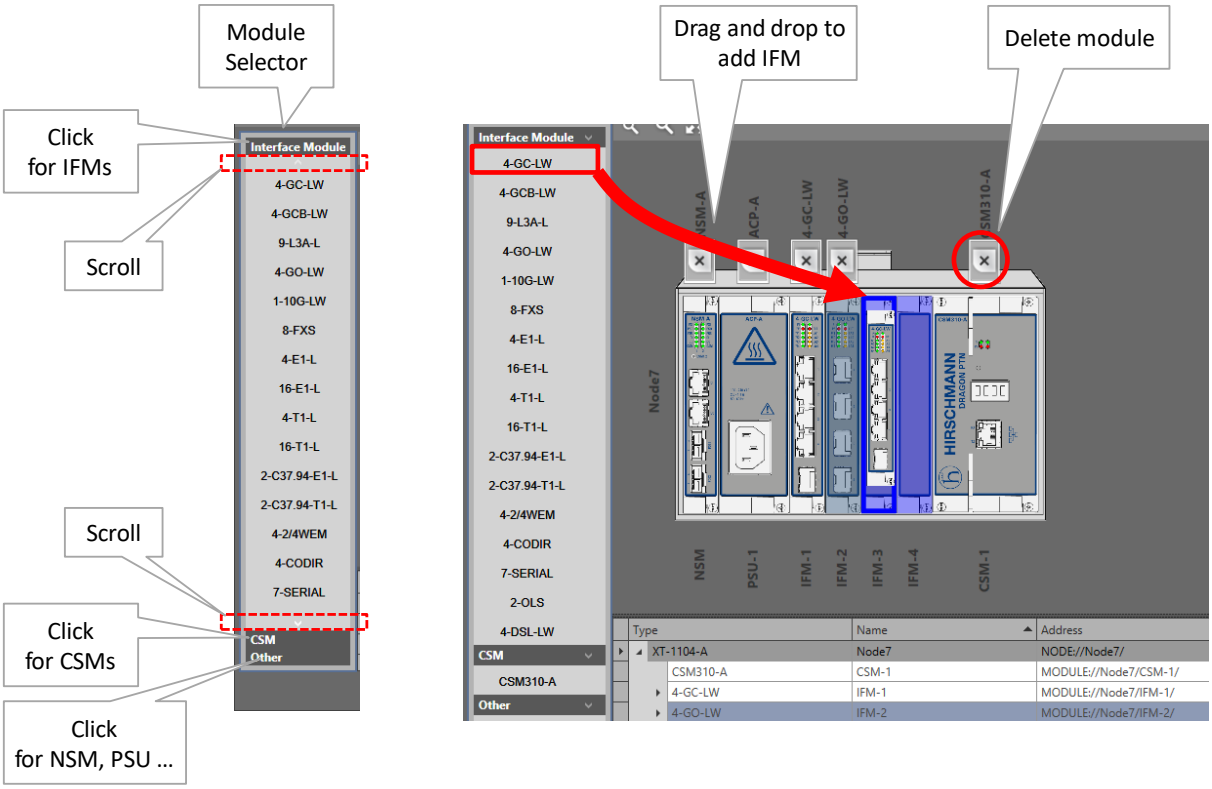


Figure 31 Drag and Drop Modules into Device Picture

- Modify: New modules can be dropped into the selected node or existing modules can be deleted from the selected node. Also the node name can be changed;
- Delete: the selected device or node can be deleted if its modules have been removed or deleted first. Its modules can be removed if they have been removed from links/tunnels/services first;
- LAGs: Create/Modify/Delete Link Aggregation Groups, see Ref. [2Eth] in Table 1;
- Virtual Loopback Interface, see Ref. [2Eth] in Table 1;

b. Devices Summary

See Ref. [2Net] in Table 1.

c. Links

- Create:
  - Select the link type of the WAN connections e.g. Ethernet 1G, Ethernet 10G, Ethernet 40G …. This type defines the bandwidth of the link, e.g. 1G, 10G, 40G, … 'External E1 Links' must only be used when the Local Mode service is used on 2-OLS or 2-C37.94 IFMs (see Ref. [2Leg] in Table 1). The 'External E1 Link' will be created beyond the Dragon PTN network and usually goes through an external network (e.g. SDH). An 'External E1 Link' will be indicated by a cloud icon . A 'Monitored Link' must be created between a Dragon PTN node and a third party or generic device (=non-Dragon PTN node) or between generic devices. This link type allows that the generic device is shown in all the network drawings and that the link towards these devices is monitored. When something goes wrong with the link, alarms will be raised. More info on Generic Devices in §18;

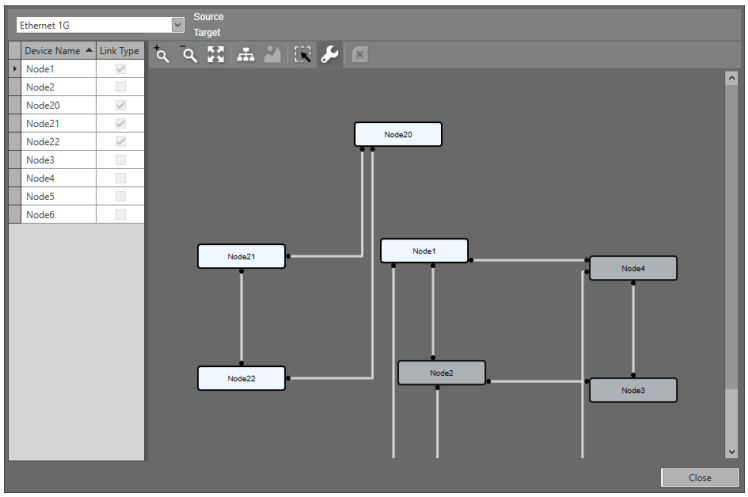


Figure 32 Create Links

  - Find below the IFMs that could be selected according to the selected link speed. The Link Type checkbox is selected (or its node icon is white-highlighted) when that node has still a WAN port available in the selected link speed. If the node does not highlight (=grey color), set some extra ports to WAN first via Dashboard → Network Hardware → Network Settings Wizard button = → Port Mode;
    - Ethernet 1G → 4-GC-LW/4-GCB-LW/4-GO-LW;
    - Ethernet 10G → 1-10G-LW/4-10G-LW;
    - Ethernet 40G → 1-40G-LW;
  - Create a link between two white nodes by clicking the first node, clicking an available (=brown) WAN port and do the same for the second node, a port selection example can also be found in the figure below.

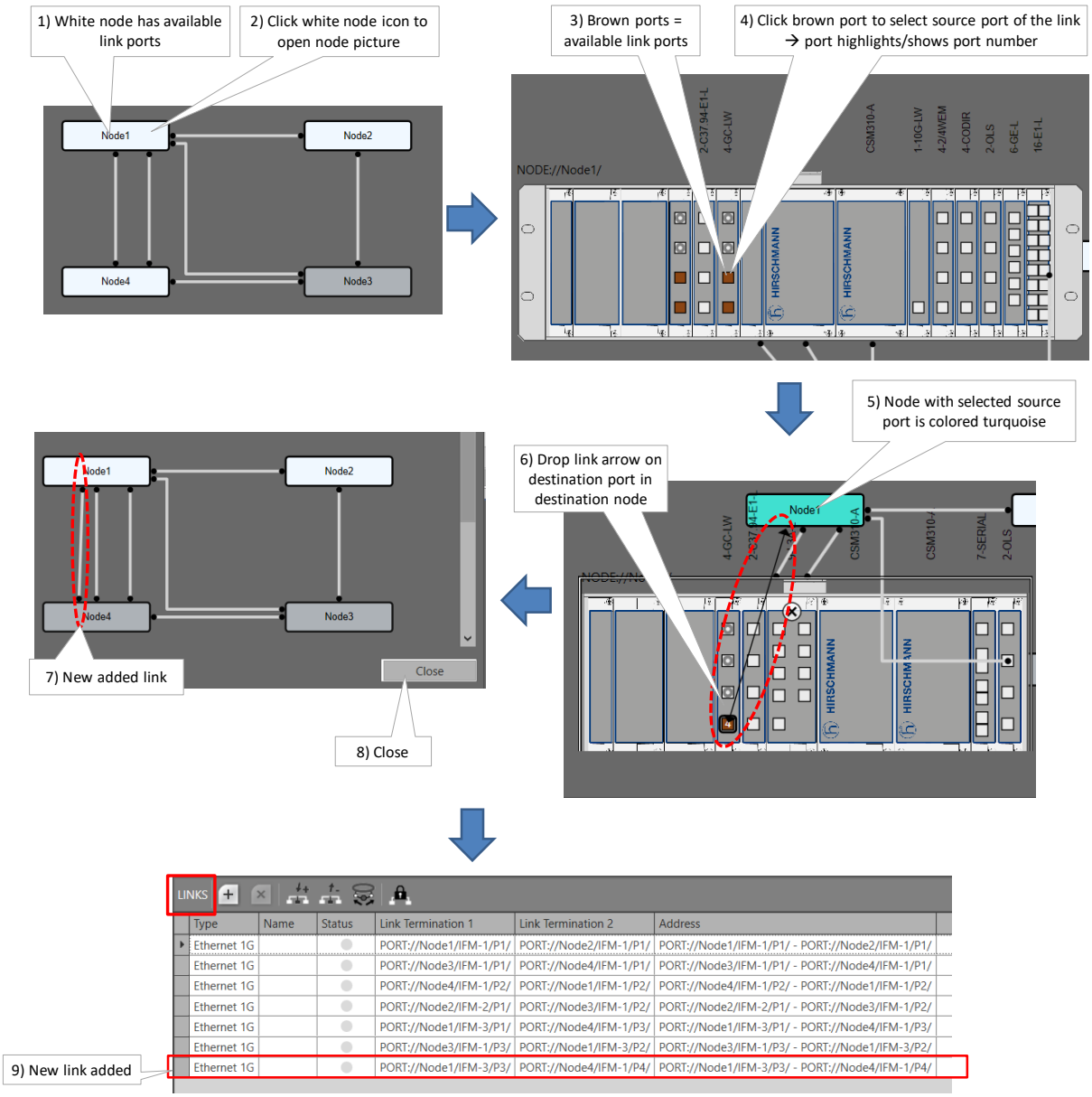


Figure 33 Add New Link

NOTE: The Link Capacity can be tuned later on, see Ref. [2Net] in Table 1.

NOTE: An additional Name and Info field can be filled out for each created link via Network Hardware → Links → Selected Link → Generic. The Info data, if filled out, will be displayed when hovering the link in the network drawings, e.g. in the network tile.

- Delete: the selected link can be deleted if it is not in use anymore. A link can be selected by clicking the link;
- Insert Node: insert a node between two linked nodes, see §2.6.3;
- Drop Node: drop or remove a node between two linked nodes, see §2.6.4;
- Monitored Link Discovery: (currently not supported);

- MACsec: Configure MACsec encryption on 10 Gbps links, see §2.6.6;

2.6.3 Links: Insert Node

Insert Node ( ) inserts a new LSR node on a link in between two existing nodes without removing the configured tunnels and services on the existing link. While loading the changes of this wizard to the network, one of the two existing nodes and the new node will be reprogrammed by HiProvision. Follow the steps below to insert a node between two links in the live network.

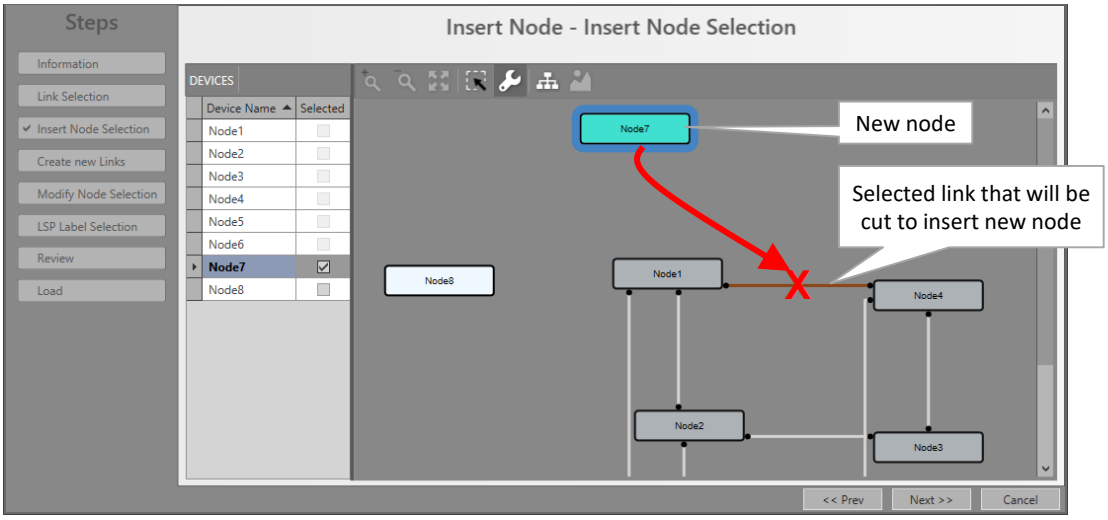


Figure 34 Insert Node

- Prerequisites: If nothing can be inserted (everything is greyed out) in the wizard, one of the prerequisites below is NOT met:
  - At least one node must be 'insert-ready';
  - A node is 'insert-ready' when:
    - it has been created in HiProvision having the necessary IFMs with WAN ports configured;
    - it has at least 2 free WAN ports of the same type as the link-to-cut, e.g. 2 free 10G ports are required for a 10G link;
    - it fulfils one of the following:
      - it is a new node: unlinked or isolated node;
    - it is an existing node: an already linked node in the network not part of any tunnel on the link-to-cut.
    - Hardware: Power up and install the new node physically (do not insert it yet into the network), assign a node number, clear the CSM(s) and provide the necessary WAN ports (number & type);
    - Dashboard → Network Hardware: Create the new node & configure its modules;
- Insert Node Wizard:
  - Link Selection: Select the link (by clicking it) on which the node must be inserted;
  - Insert Node Selection: Select the new node that must be inserted in the red-crossed link. This red-crossed link will disappear afterwards;

- Create New Links: Create new links between the new (cyan) and the two existing nodes (white) by clicking the nodes and selecting the link ports;
- Modify Node Selection: One of the two existing nodes (white) must be reprogrammed by HiProvision (=will get new LSP labels). Select one of the two nodes that can be reprogrammed. If it does not matter which one, select just one of them;
- LSP Label Selection: Shows the new LSP labels used to insert the new node. If desired, the labels can be modified by clicking the cell and changing the value;
- Review: if ok, click Finish. The configuration load manager will be invoked. Do NOT load yet, it won't be possible as the new node is not reachable yet.

- Hardware: Re-wire your WAN cables (= insert the new node physically);
- Dashboard → Discovery (see §2.5):
  - Wait until the Discovery is ready again, verify the new situation;
  - Clear both Neighbor Approvements for the involved link;
  - Wait until the Discovery is ready again, verify the new situation;
  - Approve Link for both involved links;
- Dashboard → Network Hardware:
  - Connect to the new node;
  - Load to the network (see also §7).

2.6.4 Links: Drop Node

Drop Node ( ) drops (or removes) an LSR node between two existing nodes without removing the configured tunnels and services on the existing link. Follow the steps below to remove a node between two links in the live network.

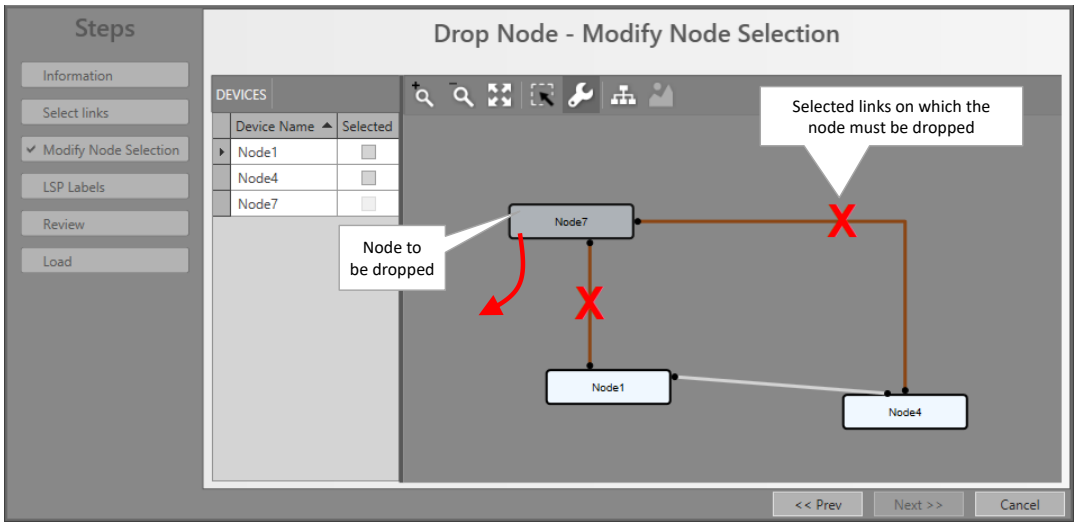


Figure 35 Drop Node

- Prerequisites: If nothing can be dropped (everything is greyed out) in the wizard, one of the prerequisites below is NOT met:
  - A least one node must be 'drop-ready';
  - A node is 'drop-ready' when:
    - it has at least 2 links;

        - its 2 adjacent links (link1 and link2), from which the node will be dropped, must have the same link type, e.g. both Ethernet 10G;
        - it is an LSR node for all tunnels it belongs to;
    - link1 and link2 have the same set of tunnels.

- Drop Node Wizard:
    - Select Links: Select two links adjacent to the node that must be dropped;
    - Modify Node Selection: One of the two existing nodes (white) must be reprogrammed by HiProvision (=will get new LSP labels). Select one of the two nodes that can be reprogrammed. If it does not matter which one, select just one of them;
    - LSP Label Selection (read only): shows the resulting LSP labels after dropping the node;
    - Review: if ok, click Finish. The configuration load manager will be invoked. Do NOT load yet;
- Dashboard → Network Hardware: Optional: Only delete the node including its modules when the node is not used anymore afterwards or completely isolated;
- Hardware: Re-wire your WAN cables (= remove the node between the two links);
- Dashboard → Discovery (see §2.5):
    - Wait until the Discovery is ready again, verify the new situation;
    - Clear both Neighbor Approvements for the involved link;
    - Wait until the Discovery is ready again, verify the new situation;
    - Approve Link for the involved link;
    - Dashboard → Network Hardware: Load to the network (see also §7);

2.6.5 Links: Monitored Link Discovery (currently not supported)

NOTE: Also verify chapter §18 which describes the confiuration of External Devices and linking them to the Dragon PTN network.

The Monitored Link Discovery () wizard allows to easily configure ‘monitored link’ modifications. A monitored link is an external link between the Dragon PTN network and all its connected external devices.

2.6.6 Links: MACsec

MACsec () is used to encrypt 10 Gbps 1-10G-LW WAN links.

- MACsec: Media Access Control Security using 802.1AE IEEE;
- A Dragon PTN network can be equipped with encrypted 1-10G-LW WAN links. These links have all data exchanged encrypted between two neighbor nodes (one side encrypts and the other side decrypts). This is useful when links between nodes share a common infrastructure or in general because there is a risk of data interception. The encryption is done via MACsec 802.1AE IEEE industry-standard security technology that provides secure communication for all traffic on the WAN links.

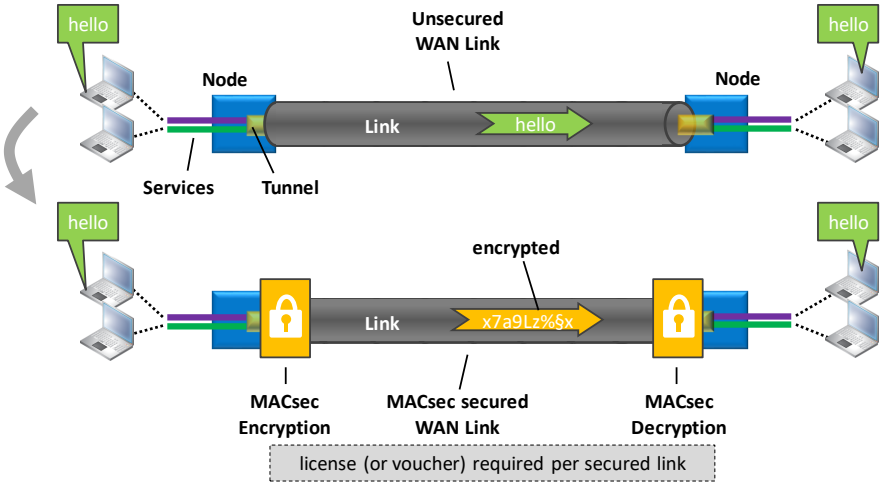


Figure 36 MACsec

- This wizard allows to:
  - Use the same or different encryption keys per selected WAN link;
  - Export all the WAN links with their encryption key, if any, in a CSV file;
  - Clear WAN link encryptions.
- This feature requires a license (or voucher) per secured link!
- MACsec Wizard:
  - Page: Link Selection: the 10 Gbps links on on 1-10G-LW IFMs are shown. Select the links on which you want to activate MACsec encryption. If the selected checkbox is already checked for some links, it means that this link has already MACsec encryption enabled.

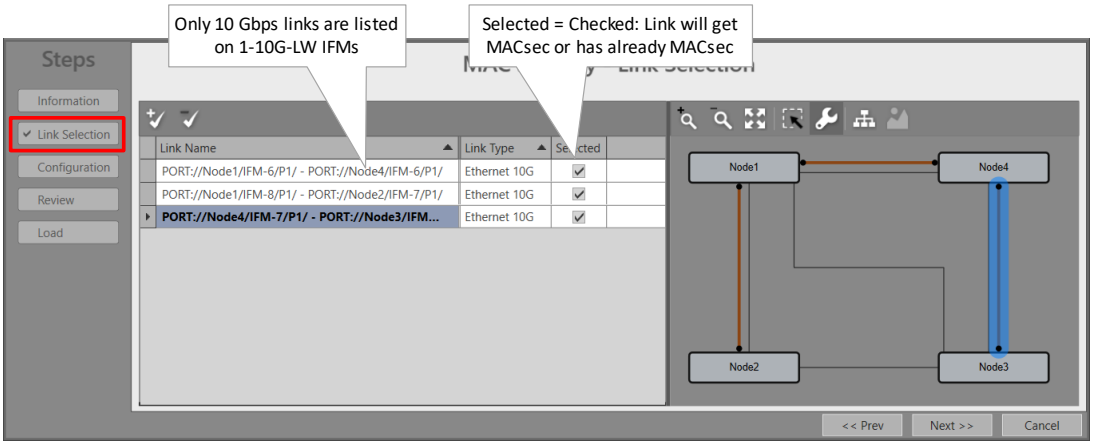


Figure 37 MACsec Link Selection

  - Page: Configuration: The selected links will automatically get a unique MACsec key (encryption/decription) key assigned. Via the buttons below, some key manipulations can be done:
    -  : Click this button to generate a different unique key for one or more selected links (=selected rows) in this page;

- : Click this button to generate the same key for one or more selected links (=selected rows) in this page;
- : Click this button to clear or delete the key for one or more selected links (=selected rows) in this page;
- : Export all the keys into a CSV file;

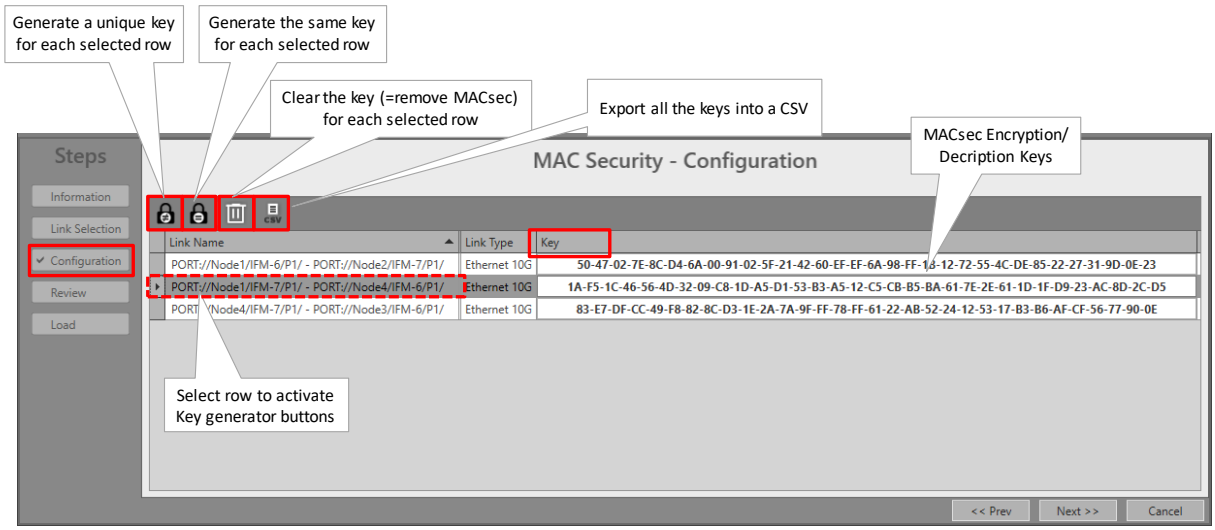


Figure 38 MACsec Link Selection

NOTE: It is possible to manually edit the Key field. This key field is completely random and free to fill out what you want.

NOTE: Removing MACsec from a link can be done in two ways in the MACsec wizard. 1)Just unselect the links in the Link Selection page and finish the wizard. Or 2)Delete/Clear the key from the desired links in the Configuration page and finish the wizard.

NOTE: The best way to find out which links have MACsec configured is to go via the MACsec wizard. Links with MACsec will have key selected checkbox selected in the the Link Selection page. In the Links section in the figure below, the selected 10 Gbps links show an extra MAC Security section with a MAC Security Status. If it is Active, it means that MACsec is activated on the link in the live network. In any other case, no MACsec is configured or activated on the link.

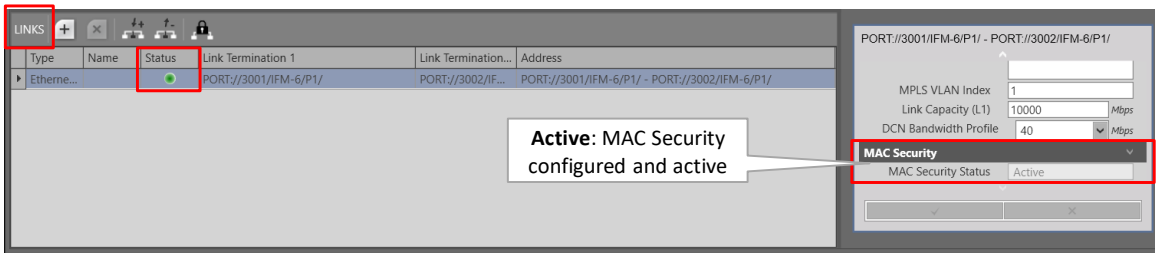


Figure 39 Active: MAC Security

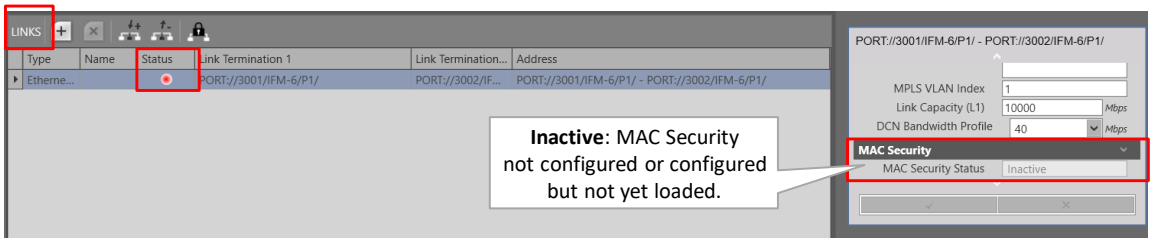


Figure 40 Inactive: MAC Security

NOTE: If a 10 Gbps link cable with MACsec has been accidently plugged into a port without MACsec, a MACsec mismatch alarm will be raised, see below.

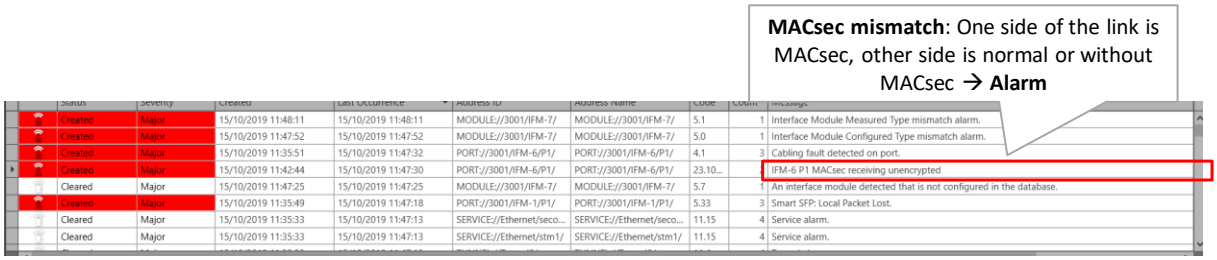


Figure 41 MACsec Mismatch: Receiving Unencrypted Alarm

2.7 HiProvision: Check Network Hardware

Prerequisite: HiProvision is offline: grey status bullets in Network Hardware tab;

The created network elements can be verified in the database via the Dashboard → Configuration → Network Hardware. See figure below:

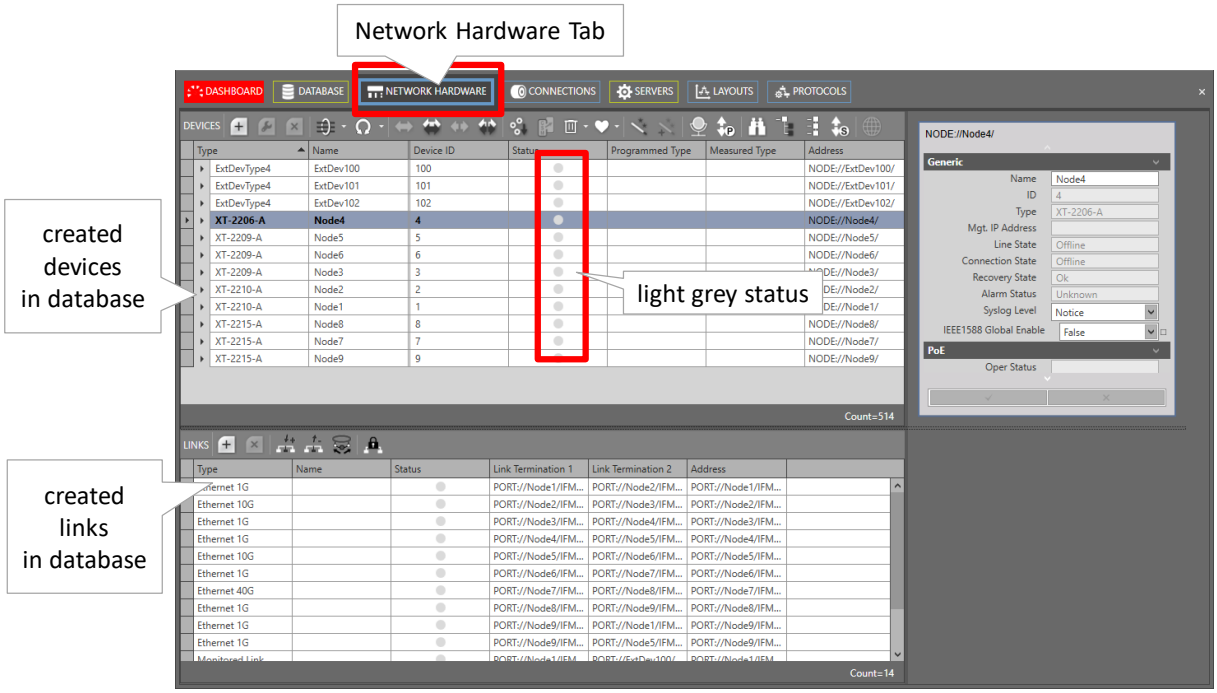


Figure 42 Network Hardware Tab: Created Network Elements

The purpose is to go online with HiProvision into the network in a controlled way, to make the network elements reachable for configuration. It is possible to go online with only one, some or all network elements together. When going online, the status bullets will be colored. The tables below show the meaning of the status bullets.

Table 9 Status Bullets: Devices

Bullet Color	Description
Light Grey	Not connected yet, network element is offline.
Dark Grey	Connected, device is unreachable (e.g. broken cable, missing device...)
Green	Connected, device is online/reachable and OK, device has no alarms.
Other color	Connected, device is online/reachable but has an alarm. The bullet color indicates the alarm color or severity. See §9.2 for the meaning of the alarm color.

Table 10 Status Bullets: Links

Bullet Color	Description
Light Grey	At least one of the two nodes to which the link is connected, is offline or not connected yet.
Green	Link is up and running, everything OK.
Red	Link is broken - Connected, device is unreachable (e.g. broken cable, missing device...) or - Connected, device is online/reachable but has an alarm on that link port. The bullet color indicates the alarm color or severity. See §9.2 for the meaning of the alarm color.
+ <colored bullet>	The link is an 'External E1 Link', the meaning of the color bullet is the same as described above.

CAUTION:
Make sure to have purchased a voucher for each node in your network before going online. A license pack is required to go online via the connect buttons below! See also §4.

HiProvision can go online (offline) via the connect (disconnect) buttons. See figure below:

- : Go online, connect to all devices at once;
- : Go online, Connect to all the selected devices (multiple via the CTRL and SHIFT keys);
- : Go offline, Disconnect all devices at once;
- : Go offline, Disconnect the selected devices;

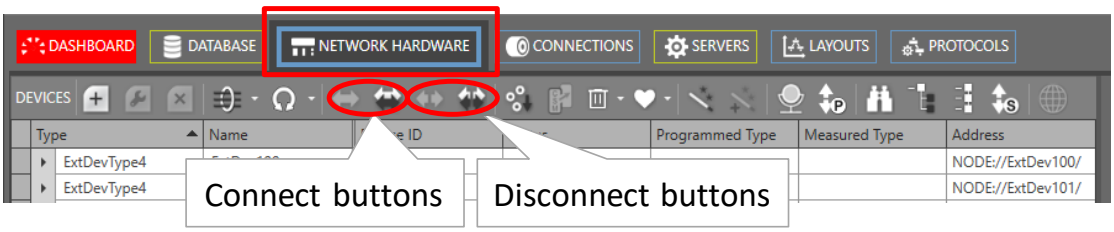


Figure 43 Connect/Disconnect Buttons

Click one of the connect buttons to go online. As a result, if this is the first connect ever and no database configuration was loaded into the network before, configuration alarms will be generated. These alarms are raised because there is a mismatch between what is measured and what is configured in the nodes. Loading the configuration into the network will clean up the mismatches and as a result solve the alarms.

The Alarms tile in the dashboard will turn dark red (=critical alarms). The tile color is the same as the alarm color of the alarm with the highest severity. All these alarms can be viewed more in detail via clicking the Alarms tile. See figures below.

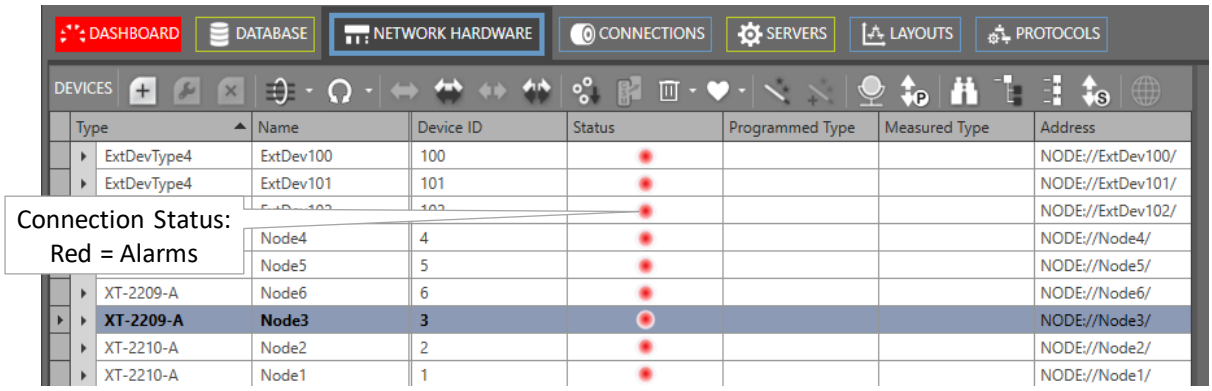


Figure 44 Connection Status After Connect

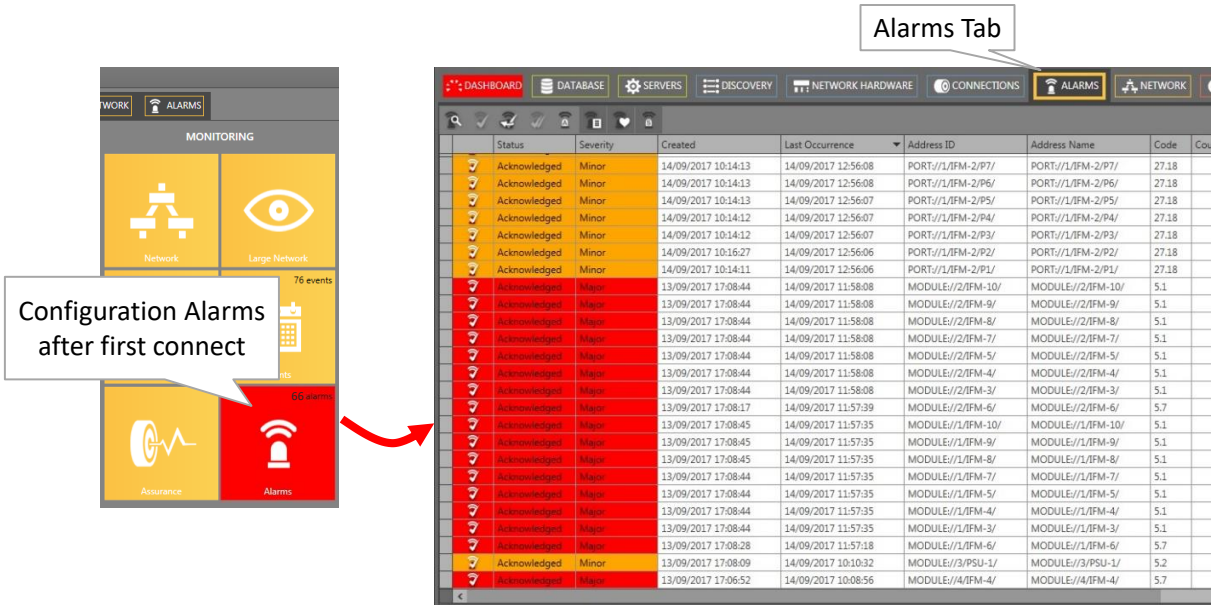


Figure 45 Configuration Alarms

An appearance of alarms means that HiProvision is online. The alarms itself indicate for example mismatch alarms (= mismatches between database and network) and status alarms (e.g. temperature too high, …). There is no configuration yet in the network because it has not been loaded yet into the network so far (except for the discovery expected values).

NOTE: More information on alarm handling, severity and colors can be found in §9.2.

2.8 HiProvision: Load Configuration into the Network

Loading the database configuration into the network will configure the live network and clean up all the mismatch alarms between database and network. As a result, the red status bullets will turn into green bullets.

In the Network Hardware Tab, click the load icon to start the configuration load manager. See §7 for an overview of this tool.

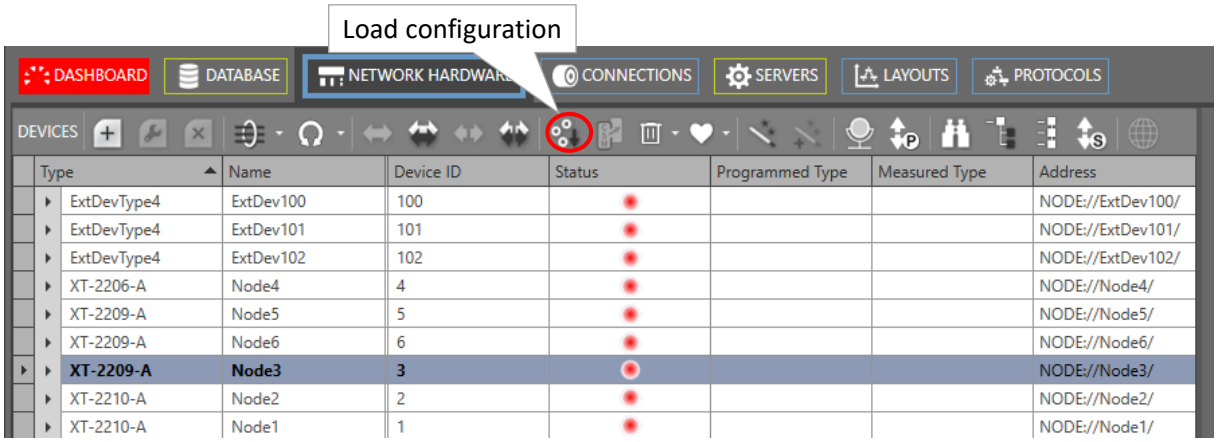


Figure 46 Load Configuration Into the Network

After everything has been loaded successfully, the status bullets in the Network Hardware tab should be green. If not, solve the mismatches. Next, load again. Repeat these steps until all bullets are green.

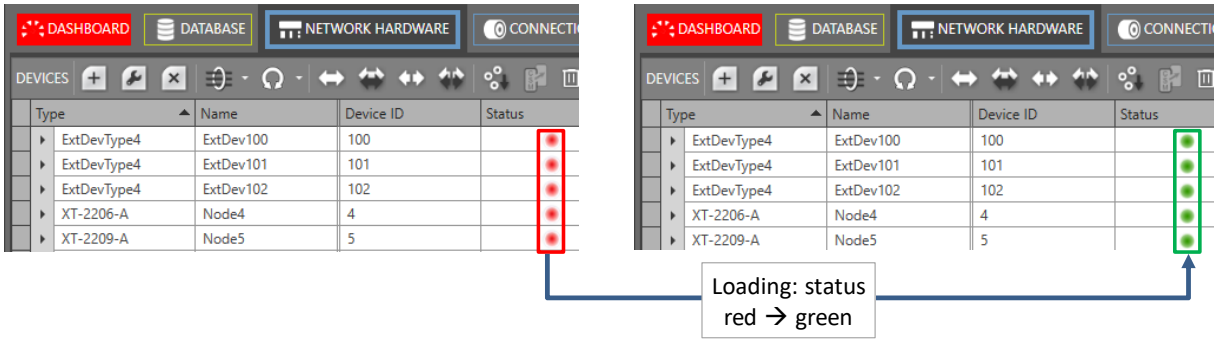


Figure 47 Status Color Change After Successful Loading

2.9 HiProvision: Set the Node Timing via an NTP Server

2.9.1 General

(NTP = Network Timing Protocol)

To make sure all the nodes in the Dragon PTN network use the same node timing (e.g. use of timestamps for logging, alarms etc...), an NTP server must be used. Either an external NTP server can be configured, or the HiProvision PC itself can act as an NTP server. By default, no central network timing or NTP server is configured.

CAUTION:
An External NTP server must always be connected to Dragon PTN via the CSM front port. The NTP is distributed via the DCN Channel!

Find some examples below:

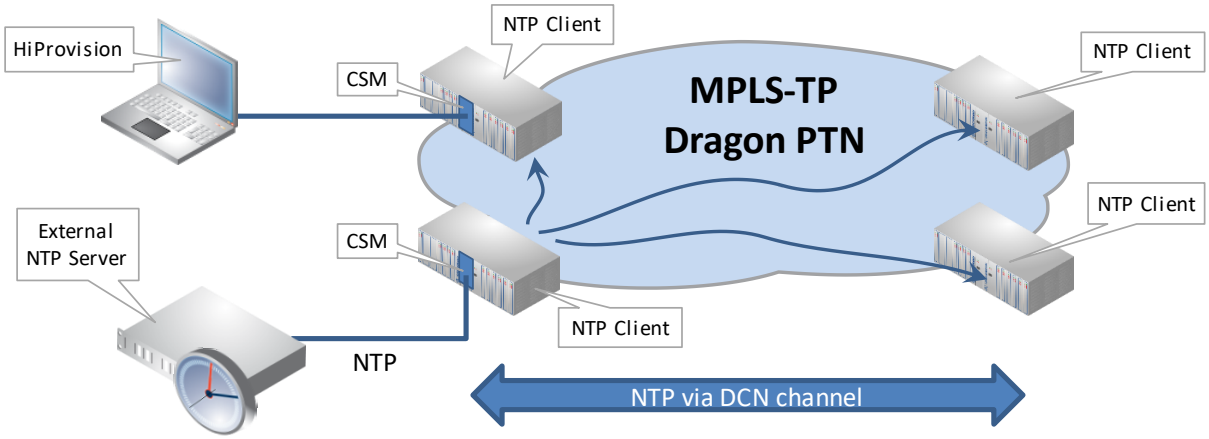


Figure 48 Example1: External NTP Server Directly Connected to CSM

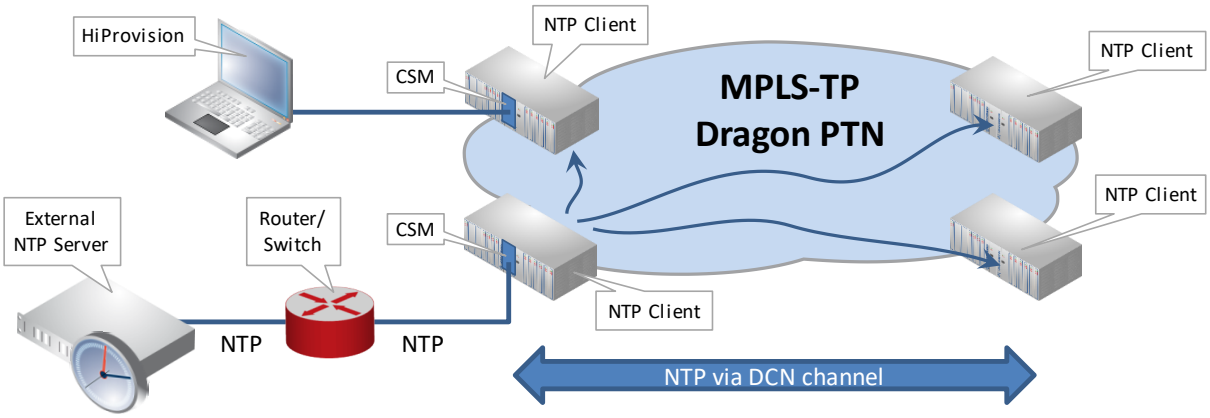


Figure 49 Example2: External NTP Server Connected via Router/Switch

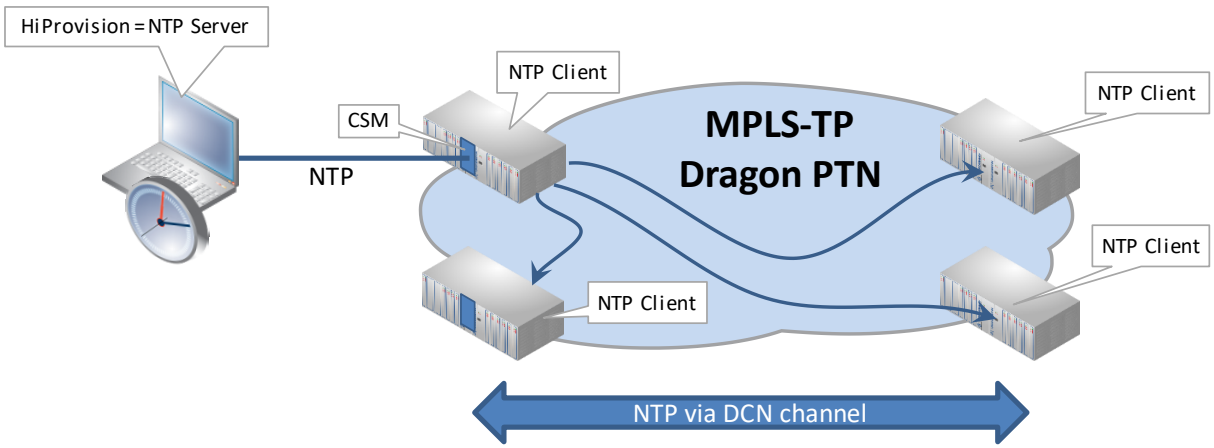


Figure 50 Example3: HiProvision Acts as NTP Server

- Example 1: Direct Connection
  - Make sure that the NTP server is in the same IP subnet as the node. Routes must be set correctly on the NTP server.
  - Configure an NTP server in HiProvision: see §2.9.2;
- Example 2: Connection via Router or Switch
  - Via Router: NTP server can have any IP address as long as it is reachable via the router;
  - Via Switch: NTP server and HiProvision should be in the same IP subnet. Routes on the NTP server for the device IP addresses (§2.5.8) should be set correctly;
  - Configure an NTP server in HiProvision: see §2.9.2;
  - Extra step to configure HiProvision as NTP Server: see §2.9.3;
- Example 3: HiProvision acts as NTP Server
  - Configure an NTP server in HiProvision: see §2.9.2;
  - Extra step to configure HiProvision as NTP Server: see §2.9.3;
- I do not want to use NTP: see §2.9.4;

2.9.2 Configure NTP Server/Backup NTP Server in HiProvision

The network settings wizard allows to easily set the IP address of an NTP server. Click the Network Settings Wizard button , see figure below:

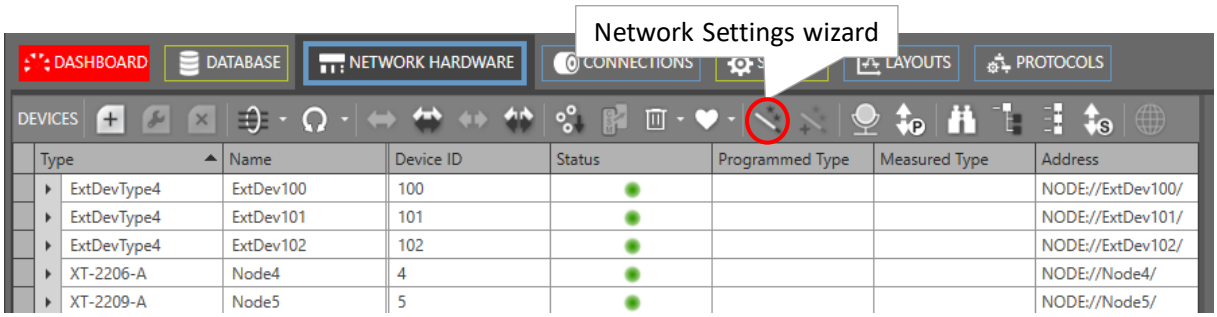


Figure 51 Network Settings Wizard Button

The Network Settings wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Selection: select Time/Date Mode;
- Time/Date Mode: Shows the CSMs in the network and their NTP settings.
  - Set Time/Date Mode
    - NTP (=default): Use this value. The NTP server will regularly update the Dragon PTN network timings with new timestamps;
    - Manual: see §2.9.4 below.
  - NTP Server IP address is filled out by default with the HiProvision Server IP address. If HiProvision must act as an NTP server, keep these IP addresses. If an external NTP server must be used, overwrite this IP address (for all CSMs) with the IP address of an NTP server in your network. You can select each CSM individually or select them all at once via the Multiple Settings Mode. Click Apply after selecting the CSMs and filling out the IP address. See figure below;

- Backup NTP Server IP address:
  - 0.0.0.0 (=default): No backup NTP Server is used;
  - Custom IP address: Overwrite this IP address (for all CSMs) with the IP address of a backup NTP server in your network. You can select each CSM individually or select them all at once via the Multiple Settings Mode. Click Apply after selecting the CSMs and filling out the IP address. See figure below;
- Review: if ok, click Finish. The configuration load manager will be invoked, see §7;

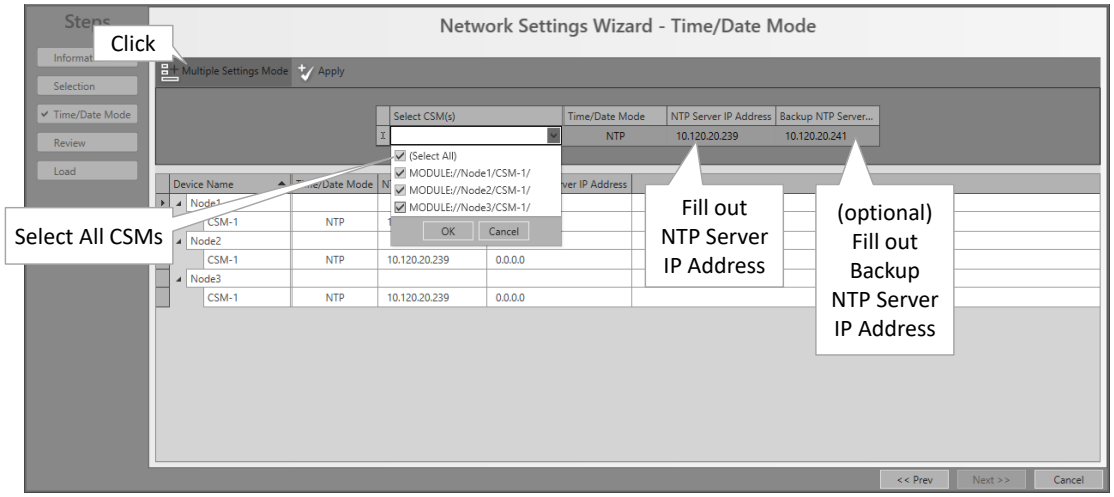


Figure 52 NTP Server IP Address

After loading the NTP configuration into the Network, the configured NTP settings are also visible in the Dashboard → Network Hardware tile → CSM → Specific:

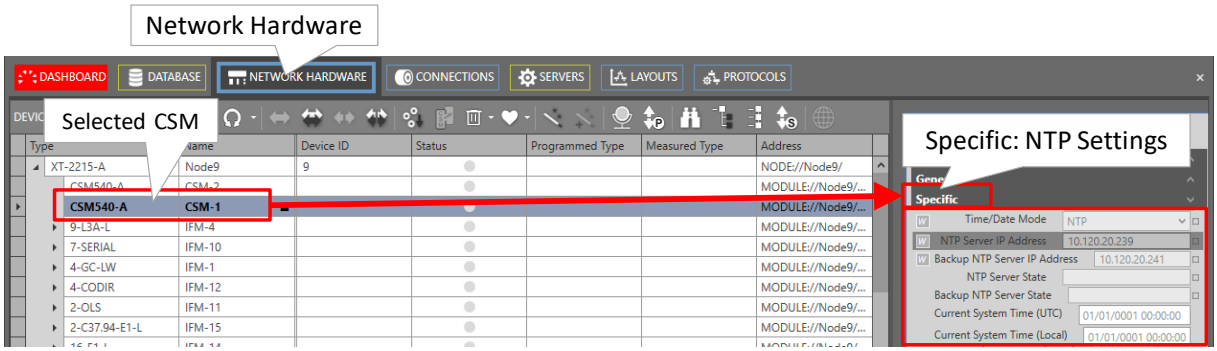


Figure 53 CSM NTP Settings

2.9.3 Configure HiProvision Server PC as NTP Server

If you don't have an external NTP Server and you still want to use NTP, it is possible to configure the HiProvision server as NTP Server as listed below:

- Open the Windows Registry Editor;
- Set following registry values:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config:
    - AnnounceFlags = 0x5

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer:
  - Enabled = 1

- Close the Windows Registry Editor;
- Open (as Administrator) a command prompt on the HiProvision Server PC;
- Restart your time service via entering the command:
  - net stop w32time && net start w32time

2.9.4 Manual Setting (=No NTP Server)

If you do not have an NTP server or don't want to use one, it is also possible to set Time/Date Mode to 'Manual' (Figure 52). As a result the HiProvision Server time and date will be pushed into the network only once and only when the load action occurs in this Time/Date wizard, just after clicking the Finish button.

2.10 Set Up Your Dragon PTN Network

For any required action to configure the network itself (without the services), see Ref. [2Net] in Table 1.a

2.11 Set Up Your Services

- For an application that uses pure Ethernet, see the Ethernet services manual in Ref. [2Eth] in Table 1;
- For any other application, see the Legacy services manual in Ref. [2Leg] in Table 1.

3. HIPROVISION AGENT

3.1 General

The HiProvision agent is the master engine process that must run before the HiProvision server and Client can run. The HiProvision Agent is installed as a MS Windows service or as a program, see §2.1.2.

3.2 How is the HiProvision Agent Installed on my HiProvision PC?

If you find a HiProvision Agent service via MS Windows start button → Services, it has been installed as an MS Windows service. If not, it has been installed as a program.

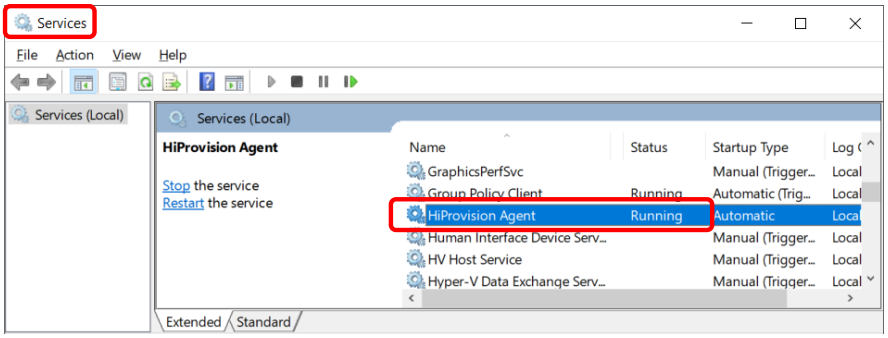


Figure 54 HiProvision Agent Service

3.3 Is My HiProvision Agent Running?

If the HiProvision Agent has been installed as a service, it is not always visible via the desktop whether it is running or not. Therefor, it can be verified as follows:

- HiProvision Agent installed as a program: It is running when you see a black HiProvision Agent DOS box or when a HiProvision Agent Icon is visible in the taskbar;
- HiProvision Agent is installed as a service: It is running when the status of the HiProvision Agent service is 'Running' in Windows start button → Services.

3.4 Start HiProvision Agent

If your HiProvision Agent is not running and you want to start it, it can be done as follows:

- HiProvision Agent installed as a program: Double-click the HiProvision Agent icon on the desktop. As a result, a HiProvision Agent DOS box is shown with a HiProvision Agent icon in the Windows taskbar.

Figure 55 Program:HiProvision Agent Icon on the Desktop

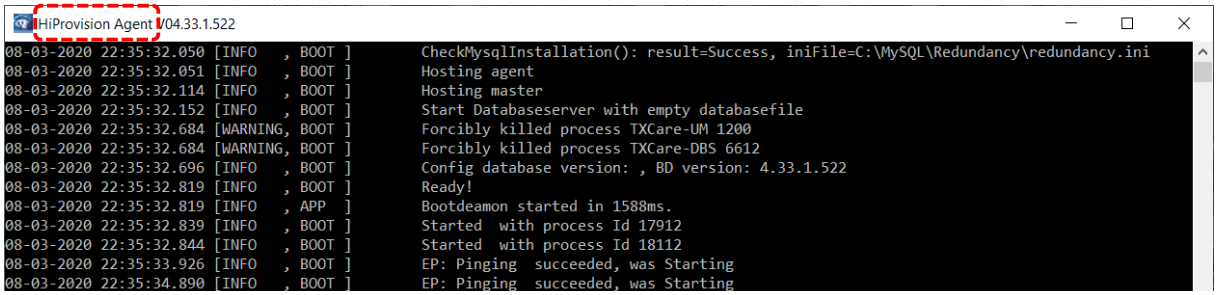


Figure 56 Program: HiProvision Agent DOS Box

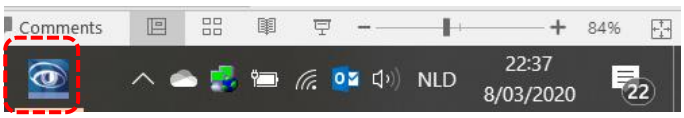


Figure 57 Program: HiProvision Agent in Taskbar

- HiProvision Agent installed as a service: By default, the HiProvision Agent is already running. Just in case somebody stopped the service, just go to Windows Start button → Services → right-click HiProvision Agent → Start;

3.5 Stop HiProvision Agent

If your HiProvision Agent is running and you want to stop it, it can be done as follows:

- HiProvision Agent installed as a program: Close the HiProvision Agent DOS box.

- HiProvision Agent installed as a service: Windows Start button → Services → right-click HiProvision Agent → Stop;

4. SERIAL KEY / VOUCHERS / LICENSE PACK

The licenses concept consists out of three parts:

- Serial Key (see §4.1);
- Voucher(s) (see §4.2);
- License Pack (see §4.3);

How to deal with licenses can be found in:

- Generate License Pack and Install in HiProvision (see §4.4);
- Monitor Licenses in HiProvision (see §4.5);
- Licenses Operation (see §4.6);

4.1 Serial Key

- is required for the HiProvision installation and looks like 'DRN2-aaaa-aaaa-aaaa-aaaa-aaaa-aaaa';
- is available for free via https://hiprovision.hirschmann.com → Shortcuts → Licenses HiProvision → Serial Key;
- must only be used for one unique single HiProvision installation;
- is valid for future HiProvision upgrades on the same HiProvision PC;
- serial key used at installation can be found in the HiProvision Info box, see §2.4.5a.

4.2 Voucher(s)

- is a unique number that grants the permission to use a specific node or run a specific feature within the Dragon PTN network for a specific major Dragon PTN Release (=Release Dependent, see §2.4.5a);
- must be purchased via Hirschmann Automation and Control GmbH;
- following vouchers types are available and must be purchased if needed:

Table 11 Available Vouchers

Voucher	Voucher Prefix	Release Dependent (*)	Amount
Dragon PTN R4.x: Node PTN2210	DRX40	Yes	1 Per Node
Dragon PTN R4.x: Node PTN1104	DRX41	Yes	1 Per Node
Dragon PTN R4.x: Node PTN2206	DRX42	Yes	1 Per Node
Dragon PTN R4.x: Node PTN2209	DRX43	Yes	1 Per Node
Dragon PTN R4.x: Node PTN2215	DRX44	Yes	1 Per Node
Dragon PTN Upgrade: Node PTN2210	DRX90	No	1 Per Node
Dragon PTN Upgrade: Node PTN1104	DRX91	No	1 Per Node
Dragon PTN Upgrade: Node PTN2206	DRX92	No	1 Per Node

Voucher	Voucher Prefix	Release Dependent (*)	Amount
Dragon PTN Upgrade: Node PTN2209	DRX93	No	1 Per Node
Dragon PTN Upgrade: Node PTN2215	DRX94	No	1 Per Node
CSM Redundancy	DRX0	No	1 Per CSM Redundant Node
HiProvision Redundancy	DRX1	No	1 Per Serial Key
HiProvision Add-on: SNMP NorthBound	DRX2	No	1 Per Serial Key
HiProvision Add-on: CAR IP	DRX3	No	1 Per Serial Key
Large Network Monitor	DRS2	No	1 Per Serial Key
PTN Device	DRO0	No	1 Per PTN Device
Hirschmann Device	DRH0	No	1 Per Hirschmann Device
Generic Device	DRS1	No	1 Per Generic Device
Dragon PTN R4.x Chinese Language	DRL40	Yes	1 Per Serial Key
Dragon PTN Upgrade: Chinese Language	DRL90	No	1 Per Serial Key
Dragon PTN R4.x German Language	DRL41	Yes	1 Per Serial Key
Dragon PTN Upgrade: German Language	DRL91	No	1 Per Serial Key
Dragon PTN R4.x Polish Language	DRL42	Yes	1 Per Serial Key
Dragon PTN Upgrade: Polish Language	DRL92	No	1 Per Serial Key
Dragon PTN R4.x Spanish Language	DRL43	Yes	1 Per Serial Key
Dragon PTN Upgrade: Spanish Language	DRL93	No	1 Per Serial Key
MACsec Security	DRX4	No	1 Per 10Gbps WAN Link
(*) Release Dependent (Yes/No): **Yes**: These vouchers will work in all the major Release not higher than the mentioned Major Release (e.g. R4.x), upgrading to a higher future major release later on (e.g. R5.x) requires to purchase the vouchers again for the new major release or to purchase Upgrade vouchers; **No**: These vouchers will work in any Dragon PTN Release;			

- will be sent to you in an email after having it purchased;
- always looks like '<Voucher Prefix>-aaaa-aaaa-aaaa-aaaa-aaaa-aaaa';
- E.g. **DRX40**-1234-5678-9012-3456-7890-1234 represents a voucher for the **PTN2210** node for Dragon PTN Release 4.x.

4.3 License Pack

- is a unique '*.dat' file including your Serial Key and vouchers;
- is generated via https://hiprovision.hirschmann.com → Licenses HiProvision → Get License Pack based on your Serial Key and Vouchers;
- grants HiProvision the permission to manage/monitor nodes and features in the live network;
- must be placed in the License folder on the HiProvision PC;

4.4 Generate License Pack and Install in HiProvision

NOTE: Offline configuration in HiProvision can be done without a License Pack. When going online (connect to nodes in the live network), a License Pack is required.

1. If there is no license pack installed yet, the Licenses tile shows 'No License Pack';
2. Generate the license pack via https://hiprovision.hirschmann.com → Licenses HiProvision → Get License Pack;
3. You will receive a license pack (*.dat file) via mail (or directly via download);
4. Save the license pack in the license folder (see Licenses Tile) on the HiProvision PC. In case of HiProvision Redundancy, save the license pack on both PCs;

CAUTION:
Only one License Pack or '*.dat' file is allowed in the license folder. Make sure to remove the old License Pack when replacing it by a new one.

5. Stop and restart the Servers;
6. HiProvision reads out the license pack in the license folder and updates its license information on the tile and behind the tile.

4.5 Monitor Licenses in HiProvision

Example: We have a network with 4 'PTN2210' nodes and configured it in HiProvision. We purchased 1 voucher for an PTN2210 node, 1 voucher for an PTN2206 node and 2 vouchers for an PTN1104 node. Furthermore, we tried to 'connect' (see §4.6) all the nodes in the live network.

Result: there are 4 'PTN2210' nodes, which means that 4 'PTN2210' vouchers are required (=Vouchers Required). Only 1 voucher is purchased (=Vouchers Available) for this type of node. It means that only 1 of 4 nodes can be connected (=Vouchers Used) and 3 extra vouchers must be purchased to connect all the nodes. No 'PTN2206' and 'PTN1104' nodes are configured, so none of these vouchers are required or used.

NOTE: The hardware configuration can be verified via the Network Hardware tile;

NOTE: Only as many nodes can be connected as there are Vouchers Available;

NOTE: Also the Serial Key used during installation, License folder and License Pack (=license file) are shown;

Click on the License tile to see all the voucher and license info of your system:

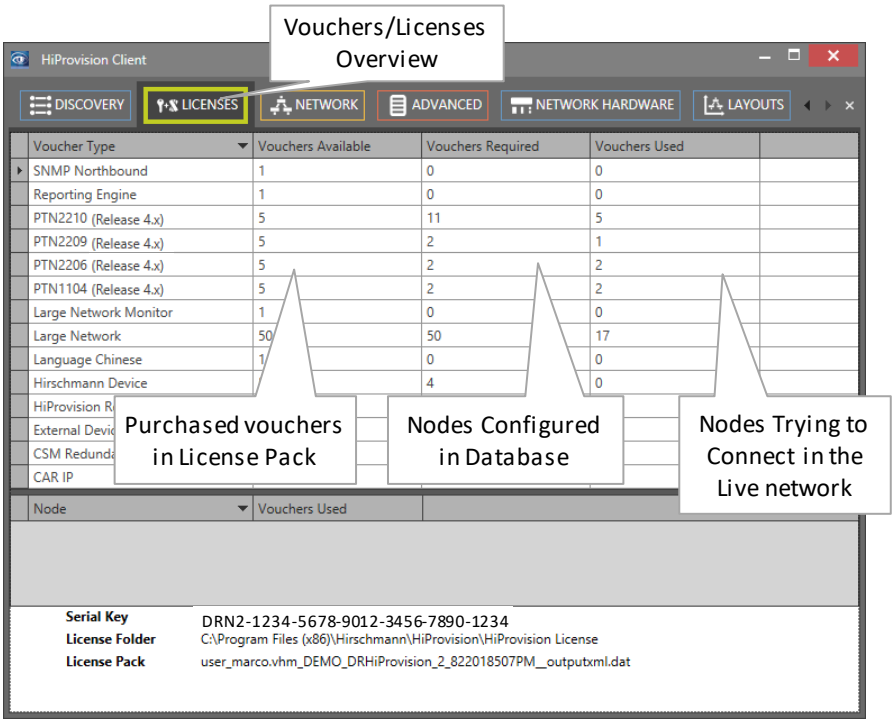


Figure 58 Vouchers/Licenses Overview1

Clicking on a voucher type in the list, shows the nodes that need such a voucher type to get online or connected. HiProvision cannot monitor or manage a live node if it cannot connect to it.

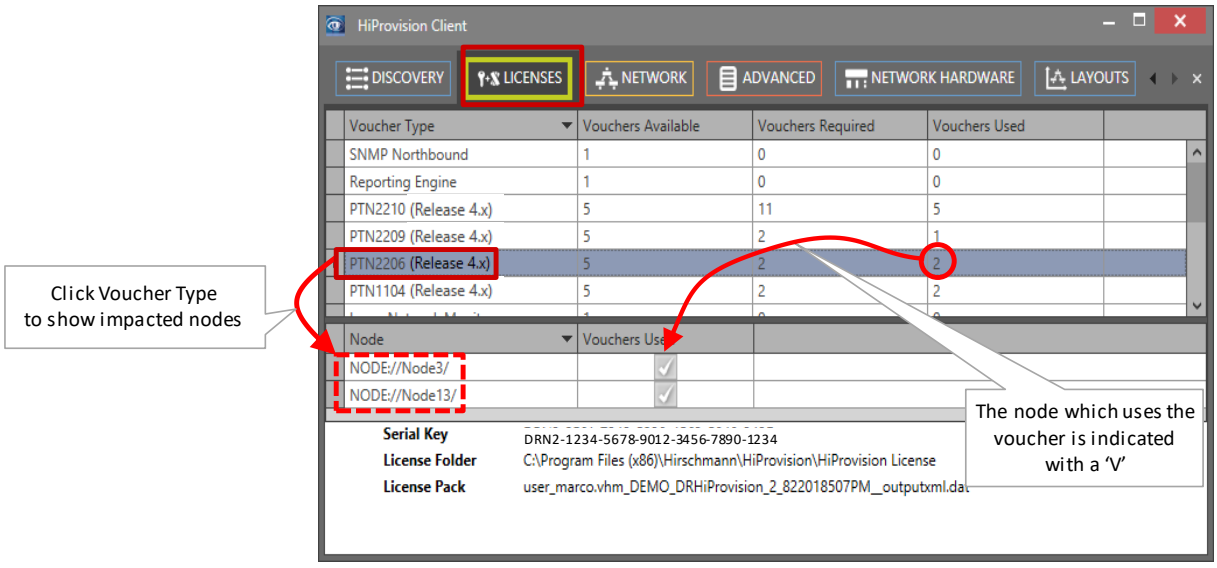


Figure 59 Vouchers/Licenses Overview2

4.6 Licenses Operation

When the operator goes online via a 'connect', HiProvision verifies the all the voucher/license info.

- Enough node vouchers available for all nodes:

- if a voucher is available for each configured node, HiProvision can connect to each node and the entire live network can be managed/monitored. Both 'connect' ( ) or 'connect all' ( ) buttons in the 'Network Hardware' tab can be used to go online.

- Not enough node vouchers available for all nodes:
  - Make sure that tunnel and service configuration is limited to only those nodes that will use the voucher. Use 'connect' ( ) to connect each of these nodes with a voucher individually. Do not use a 'connect all' ( ) which will connect nodes randomly;
  - The live nodes that have a voucher can be managed/configured by HiProvision;
  - A major **'License Alarm'** will be raised when you configure offline/online more nodes (=required vouchers) in HiProvision than you have vouchers purchased (=available vouchers);
  - A '**Node Connect Failed**' pop-up will show up when you try to connect online more nodes (=used vouchers) than you have vouchers purchased (=available vouchers). HiProvision only connects as many nodes as there are vouchers available. Only the connected nodes can be managed/monitored. A 'connect all' will try to connect all the nodes;

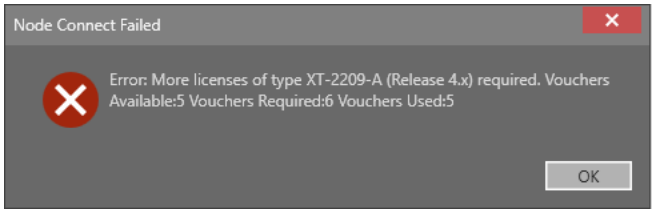


Figure 60 Connect: Not Enough Vouchers

5. SAVE USER HIPROVISION SETTINGS

When a user logs off/closes HiProvision/stops the servers, he will have the option to save its personal HiProvision settings as shown in the box below:

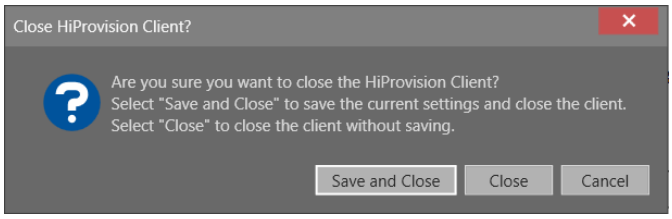


Figure 61 Save HiProvision Settings

Which HiProvision settings?

- Table layouts (shown fields, order of fields etc...), see §15.1;
- Opened tabs;
- Large Network Monitor tab state information, see §15.2.4;

When the user logs on again and ...

- ... settings were saved: HiProvision starts up and automatically opens the last saved tabs, uses the last saved table layouts and Large Network settings;
- ... settings were never saved: HiProvision starts up with the default setup.

To clear all the saved settings:

- See Ref.[15] in Table 1;

6. CLEAR/RESET ACTIONS ON NODE OR NETWORK

6.1 Clear Node or Network

Prerequisite: HiProvision must be online or connected to the network;

6.1.1 General

The clear command should be used when:

- an erroneous CSM in that same node, with a correct configuration, is reused, see Ref.[10] in Table 1;
- HiProvision cannot load the node configuration into the network, e.g. due to timestamp mismatches, ...;
- you are not sure of the loaded configuration within a node;

Clearing a node:

- erases all data (services and configured IFMs) in the CSM of that node;
- only affects data in the real network, the data in the HiProvision database is not touched;
- does NOT erase the discovery or DCN configuration, the communication with the node or management path stays alive;

Result: All the IFMs in that node stay in the configured state, alarms will be raised in HiProvision with 'type mismatch' because the hardware is different from the database configuration.

6.1.2 Clear one Node

CAUTION: The entire node goes out of service after clearing it!

1. Go to Dashboard → Network Hardware;
2. Select the node in the devices list;
3. Click → Clear. This node will go out of service after confirmation!

6.1.3 Clear the Entire Network

CAUTION: THE ENTIRE NETWORK GOES OUT OF SERVICE AFTER CLEARING IT!

1. Go to Dashboard → Network Hardware;
2. Select all the nodes in the devices list (via CTRL and/or SHIFT keys);

3. Click → Clear. THE ENTIRE NETWORK GOES OUT OF SERVICE after confirmation!

6.2 Reset Node or Network

Prerequisite: HiProvision must be online or connected to the network;

6.2.1 General

The Reset command should be used when:

- you want to set the node back to its factory default settings;
- a new CSM module is implemented, unless the Micro SD memory card from an erroneous CSM in that same node, with a correct configuration is reused, see Ref.[10] in Table 1.
- A new node is added to the network;

Resetting a node:

- sets the node back to its default settings;
- erases the discovery or DCN configuration, the communication with the node or management path to the node will be lost;
- only affects data in the real network, the data in the HiProvision database is not touched;

6.2.2 Reset one Node

CAUTION: The entire node goes out of service after resetting it!

1. Go to Dashboard → Network Hardware;
2. Select the node in the devices list;
3. Click → Reset. This node will go out of service!

NOTE: Also possible via pushing the hidden reset button on the CSM for at least 7 seconds, see Ref. [9] in Table 1;

6.2.3 Reset the Entire Network

CAUTION: THE ENTIRE NETWORK GOES OUT OF SERVICE AFTER RESETTING IT!

1. Go to Dashboard → Network Hardware;
2. Select all the nodes in the devices list (via CTRL and/or SHIFT keys);
3. Click → Reset. THE ENTIRE NETWORK GOES OUT OF SERVICE!

7. CONFIGURATION LOAD MANAGER

7.1 General

The configuration load manager is a tool that starts and monitors the load process of loading a HiProvision configuration or database into the live network.

CAUTION:
- if you want to load a restored database (see §8.5) into the network, make sure to clear the entire network first. THE ENTIRE NETWORK WILL GO OUT OF SERVICE AFTER CLEARING IT. The clear function is explained in §6.1.
- loading will FAIL when there are more nodes configured in the network database than nodes measured in the live network.
- while the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

This tool is invoked as follows:

- By clicking the load icon  in the Network Hardware tab. This button only becomes active when HiProvision is online;
- Advancing into the last page of a wizard after clicking Next in the review page: Network Settings wizard, Tunnel wizard, services wizard, …..

Some definitions (more details in further paragraphs):

- Load: transmit or load the feature configurations from the HiProvision database into the live network. After a successful Load, the feature creations/configurations/modifications will be up and running in the live network;
- Load Scenario: a list of actions that HiProvision must perform to load the latest creations/configurations/modifications of the specific feature into the live network.
- Persist checkbox: Possibility to persist the loaded configuration on the node.

7.2 Persist Configuration?

- Checked, Yes (default): The configuration change will still be active in the node after a reboot of the node.
- Unchecked, No: The configuration change will be lost after a reboot of the node. The node falls back to the latest saved or persisted configuration.

7.3 Get Load Scenarios

Before loading the configuration into the network, sometimes the button ‘Get Load Scenarios’ appears on top of the page, especially in wizards. If this button appears, click on it to retrieve and show all the scenarios in the configuration load manager. Not clicking this button will forbid you to load into the network.

7.4 Configuration Loading and Status

By default, all the nodes are selected. Nodes can be unchecked individually if they do not have to be loaded. Click the Load button to start the configuration loading into the network. If the entire configuration has been loaded successfully, the configuration load status

indicates ‘Load success’ with Warnings = 0, Errors = 0. If not, the load to one or more network elements has failed. See figure below. All load status values are listed in Table 13.

Table 12 Load Manager Menu Buttons

Button	Short Description
/	Expand/Collapse the network element treeview.
/	Only active if the load has failed on at least one network element. Click these buttons to jump to the next/previous warning or error in the network element treeview. Hovering the error icon in the network element shows some error information, which is also available in the HiProvision log files.

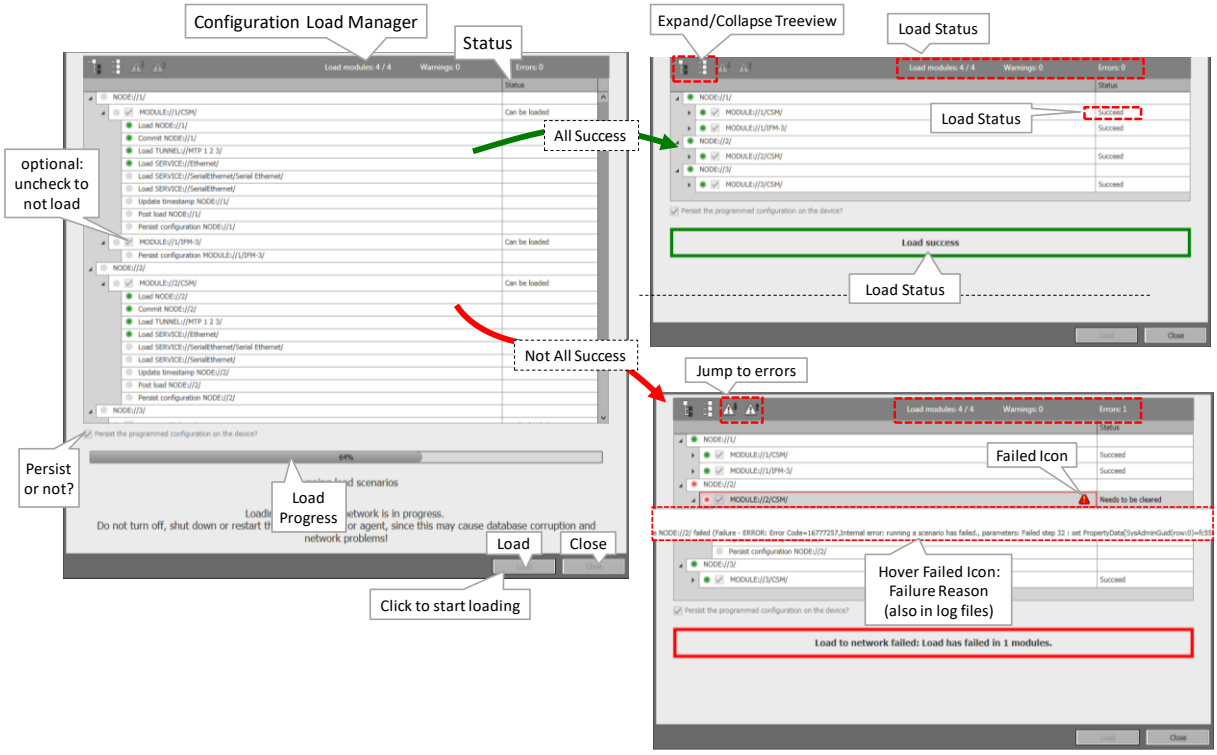


Figure 62 Configuration Load Manager

Table 13 Load Manager Status Values

Status	Retrieve Scenarios	Load	Short Description
Note: - x: status can occur; - (x): status can occur when something changes between a retrieve and a load action; - ---: status can not occur;			
Success Cases			
Can be loaded	x	---	Load scenario has been retrieved succesfully. Configuration is ready to be loaded into the network.
Succeed	---	x	Configuration successfully loaded into the network.
Error Cases			
Offline	x	(x)	The node is offline, make sure to connect this node first and try again.

Status	Retrieve Scenarios	Load	Short Description
Timestamp Mismatch	x	---	The timestamp in the node reflects the latestmoment in time that something was loaded by HiProvision into the node. The timestamp in the node does not match its timestamp in the HiProvision database. This could mean that a corrupt or invalid database is used in HiProvision or that the node has an invalid configuration. Use the correct database or clear the node and try again.
Needs to be cleared	x	x	Something went wrong during loading.
Unreachable	x	(x)	HiProvision is trying to connect the node but fails because the node (or CSM) can not be discovered e.g. IP address problem. Make sure that the node is reachable and try again.
Not present	x	---	The selected L2/L3 module is missing in the node. Insert this missing module into the node and try again.
Firmware not valid	x	---	The present firmware in the network element is not allowed in this HiProvision version. Verify the Software Tile and the allowed firmware versions, load the correct firmware into the network element and try again.
Passive CSM	x	---	HiProvision is connected via one management cable to a node with redundant CSMs. The cable is connected to a CSM that is not active. Perform a CSM switchover to make the other CSM, connected to HiProvision, the active one.
Timeout	x	x	A loading Timeout occurred.
Other	x	x	An unkown error has occured.

8. DATABASES HANDLING AND BACKUPS

8.1 General

Prerequisites: If you have chosen a custom installation path for MySQL Server at installation, change the path first as described in §8.2.1.

All database activities can be performed in the Dashboard → Database tile. The application behind the tile has three main sections, see figure below:

- Databases: All the network configuration databases available on the HiProvision server;
- Active Database: database from the list that is really used by HiProvision. Only one database can be active at a time. The active one is marked with a green border;
- Local Backups: backups of one or more databases from the 'Databases' list. The local backups are stored on the HiProvision Server. The default path is `<HiProvision installation Path>\HiProvision Backups\Databases` which was filled out in the Backup Folder field at installation time. The Backup Folder can be opened directly in HiProvision via clicking the  icon. Creating automatic backups is possible.
- Network Backups: a network backup is a copy of a local backup and is stored in one or more CSMs in the network at the same time. Each node shows a list of its network backups. Network backups in a node are possible when the Micro SD card is plugged into the CSM (=Central Switching Module) of that node, see also Ref. [10] in Table 1. This is by default the case;

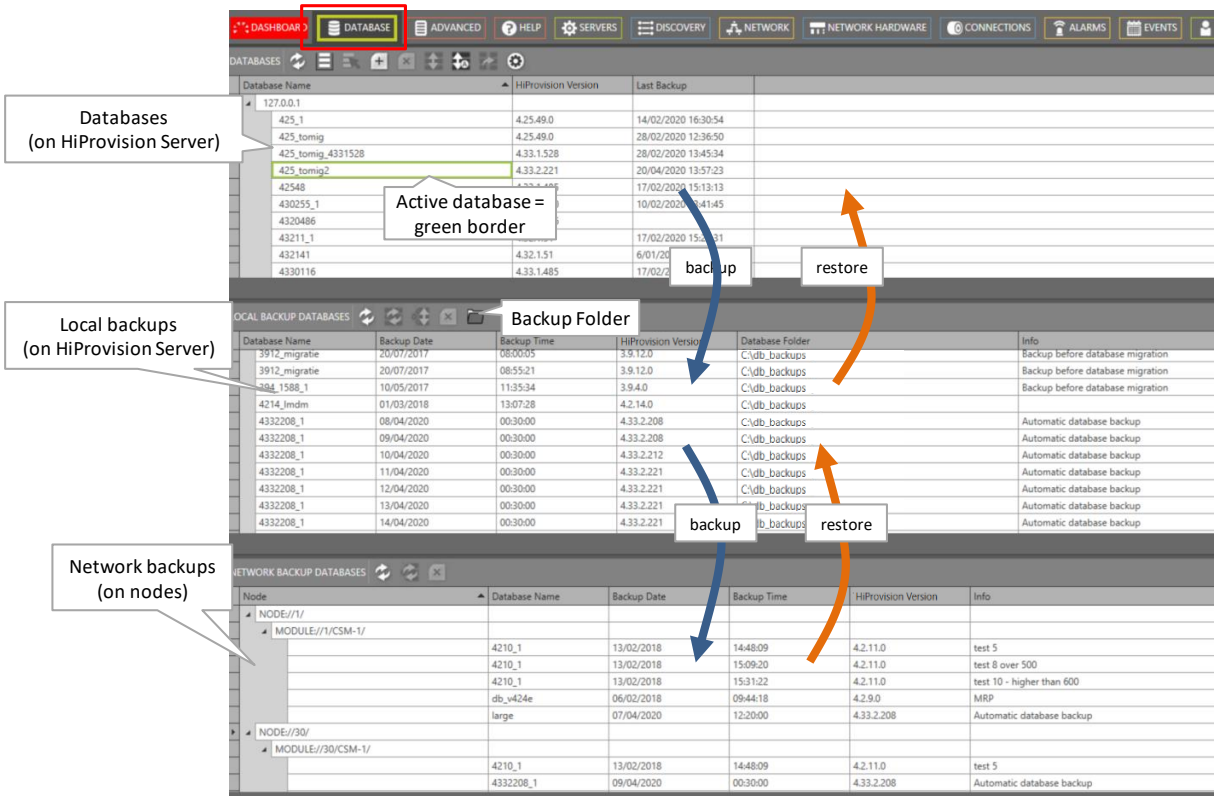


Figure 63 Database Tile

A database can be backed up locally on the HiProvision Server first (step1). This can be done manually or automatically. If desired, it can be backed up further on in the network on one or more nodes (step2). During this backup to the network, the targeted node(s) will not be affected or interrupted. The backup mechanism provides a lot of database redundancy. See figure below:

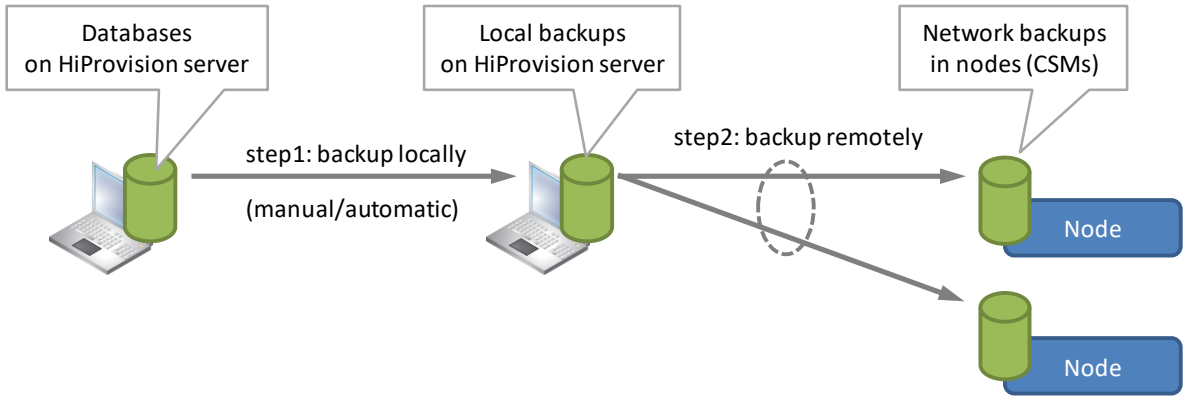


Figure 64 Backup Databases

A database can be restored from a network backup by restoring it first to a local backup (step1), followed by a restore from the local backups to the databases (step2). If a database must be restored only from a local backup, only step2 must be performed. See figure below:

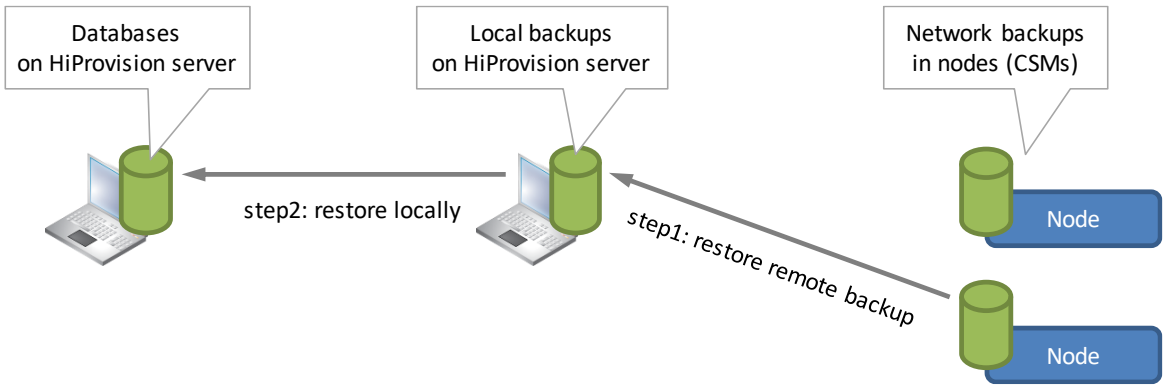


Figure 65 Restore Databases

8.2 MySQL Server Database Settings

8.2.1 Installation Path

The MySQL database server is by default installed in 'C:\Program Files\MySQL\MySQL Server x.y\bin'. If you have chosen another location at installation time, adapt the default path to the custom installation path via the options button.

8.2.2 Change Password

CAUTION: In case of HiProvision Redundancy, always make sure that both MySQL servers have the same root password!

The default password of the MySQL Server used during installation can be changed afterwards via the MySQL Workbench tool:

1. Start the 'MySQL Workbench Tool' on the HiProvision PC. By default it is installed in C:\Program Files\MySQL\MySQL Workbench <version> CE\MySQLWorkbench.exe';
2. Connect to the HiProvision database via Database → Connect to Database, select your connection in 'Stored Connection' and click OK;
3. Log in: username = **root**, password = **private**

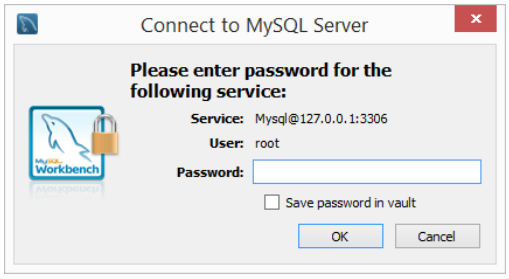


Figure 66 Connect to MySQL Server

4. On the left-hand side, click on Management → Users and Privileges;
5. For all 'root' accounts that have a 'From Host' filled out:
   1. Fill out the new password and confirm it;
   2. Click Apply;

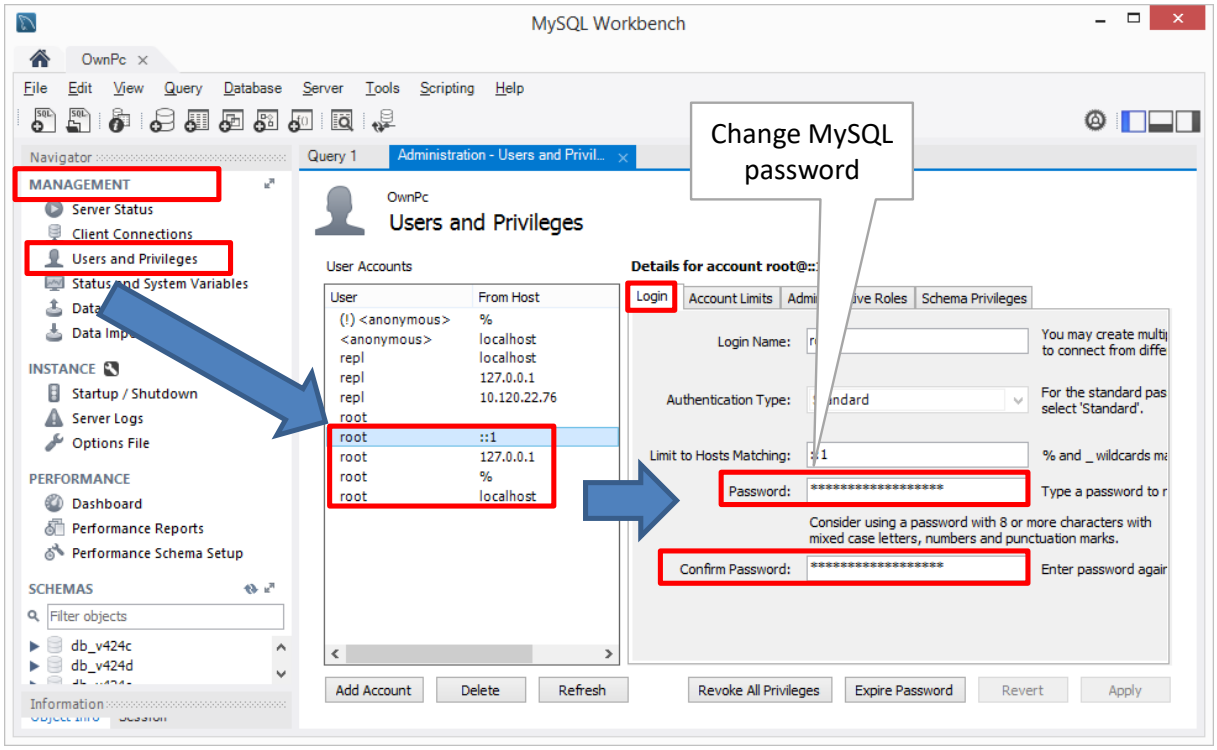


Figure 67 MySQL Workbench: Root Password Change

6. Close the MySQL Workbench;

7. Close and restart HiProvision (servers and client), log in with a HiProvision user authentication;
8. Click the Dashboard → Database tile (authentication failed) and click the database server button ;
9. Fill out the new password in the screen below and click Connect and OK:

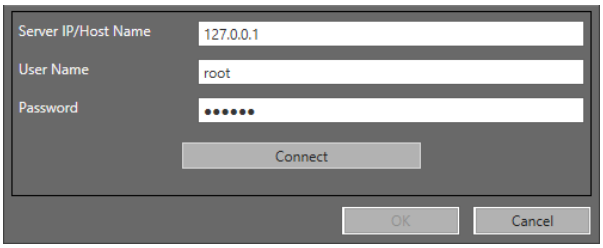


Figure 68 Connect to MySQL Server with New Password

If the connect succeeds, the password update was successful.

8.3 Activate a Database in HiProvision

CAUTION: Activating a database in HiProvision does not include loading the database into the network, see §7 to do so.

Only one database can be active at a time. Perform the steps below to activate a database:

1. Stop the servers via the Dashboard → Servers tile → ;
2. In the Dashboard → Database tile: Select the database that must become the active one by clicking it in the 'Databases' list;
3. Click the button to activate the database, it will be marked with a green border;
4. Start the servers again via Dashboard → Servers Tile → ;

8.4 Make a Backup

The backup functionality can be found in Dashboard → Database tile.

8.4.1 Make a Local Backup (Manual/Automatic)

From 'Databases' to 'Local Backups' list.

CAUTION: only the configuration database is backed up. The user database and the permanent monitoring database (Permanent Monitoring Add-on) are not backed up.

a. Manual

1. Click the database in the 'Databases' list that must be backed up;
2. Click the button to create a local backup, a backup comment can be added, the new backup will appear in the 'Local Backups' list.

b. Automatic

Prerequisites: The HiProvision Servers must run;

Some facts:

- Automatic backups are only taken from the active database, the one marked with a green border;
- Automatic backup settings are by default enabled for a new database, so when the new database becomes active, it will be backed up automatically;
- The configuration database will be backed up automatically. The user database and the Permanent Monitoring (see Ref.[26] in Table 1) database, if any, will not be backed up;
- Each database will have its own set of Automatic Backup Settings;
- Each time a backup is successfully created, an event will be logged in the Events tile: 'Automatic backup of database <active database> successful';

1. Click the Automatic Backup Settings button to open the window below:

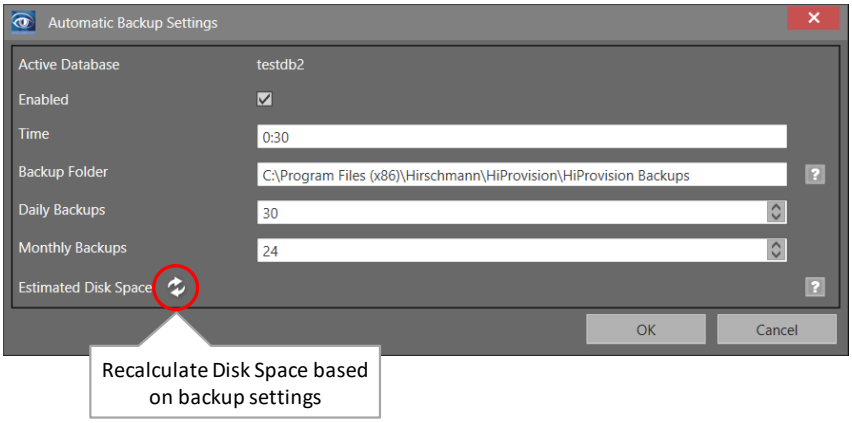


Figure 69 Automatic Backup Settings

2. Fields explained:
   - Active Database: indicates the database that will be backed up automatically;
   - Enabled:
     - Checked (=default): Enable automatic database backup. By default, each new database has the automatic backup enabled. Whether it's automatically backed up, depends on whether it's active or not;
     - Uncheck: Disable automatic database backup;
   - Time (default = 0:30 = 0:30 AM): indicates the day-time that backups are made according the Daily Backups/Monthly Backups schedule. Time formatting = <0..23>:<0..59>;
   - Backup Folder (default = `<HiProvision installation Path>\HiProvision Backups\Databases` which was filled out in the Backup Folder field during installation): indicates the backup folder path on the HiProvision server in which automatic backups will be stored. The folder can be changed provided that the new folder is an existing folder. It is possible to enter a network shared drive as well (e.g. \\<server>\<share>) provided that the HiProvision server has connection to it.

     NOTE: If HiProvision is installed as a service (see §3.2) and a shared drive or network drive is configured as backup folder, it is possible that HiProvision does not know this folder, although it exists. Some permissions must be verified/configured first to grant HiProvision access to this folder, see §***.

   - Daily Backups (default = 30, range [0…1200]): indicates the number of daily backups that are stored in the backup folder. By default, after 30 days, the oldest daily backup will be removed and replaced by the newest daily backup etc… The daily backups will be taken every day at the configured Time;
   - Monthly Backups (default = 24, range [0…1200]): indicates the number of monthly backups that are stored in the backup folder. By default, after 24 months (or 2 years), the oldest monthly backup will be removed and replaced by the newest monthly backup etc… A monthly backup will always be taken at the first day of the month at the configured Time;

     NOTE: At least one daily or monthly backup must be configured.

- Estimated Disk Space: Click the Refresh button to recalculate the required estimated disk space (in Megabytes MB) for the filled-out backup settings. This recalculation takes longer for larger databases.

CAUTION: An alarm will be raised at backup time if the disk is full and as a result the new backup can not be created.

8.4.2 Make a Network Backup

Prerequisite: the servers in the Dashboard → Servers tile must be running.

From 'Local Backups' to 'Network Backups' list:

1. Click the local backup in the 'Local Backups' list that must be backed up;
2. Click the  button;
3. Select one or more CSMs in the network on which a backup must be stored. Only CSMs with a working SD memory card can be selected. The CSM must be in the ACT (active) or STB (standby) state to succeed;
4. The new backups show up in the 'Network Backups' list under the selected nodes.

8.5 Restore a Backup

The restore functionality can be found in Dashboard → Database tile.

CAUTION:
A restored backup does not automatically become the active database!
A restored backup is not automatically loaded into the network, see §7 to do so!

8.5.1 Restore a Local Backup

From 'Local Backups' to 'Databases':

1. Click the backup that must be restored in the 'Local Backups' list;
2. Click the  button to restore the backup into a new database file. An existing database cannot be overwritten, the new filename must be non-existing;
3. The new database file appears in the 'Databases' list;
4. If you want this file to become the active database, see §8.1.

8.5.2 Restore (or Retrieve) a Network Backup

Prerequisite: the servers in the Dashboard → Servers tile must be running;

From 'Network Backups' to 'Local Backups':

NOTE: If you want it to restore it further to your 'Databases' list, follow §8.5.1.

1. Select the backup from the 'Network Backups' by expanding the necessary node and CSM and selecting the desired backup by clicking the database row;
2. Click the  button to restore (or retrieve) the backup into the 'Local Backups' list. An existing database, meaning same filename and timestamp, in that list will be overwritten.

8.6 Migrate a Database

It is possible to migrate an older database version to the version required in the running HiProvision. Migration can be done in two ways:

Must the older database become the active one after migration?

- Yes:
  1. Select the older database in the 'Databases' list and click the select button;
  2. A pop-up requests for migration. Click the OK button in the pop-up. If the database already has the latest version, no migration will be requested;
  3. A new migration window will appear. Click the Migrate button. A local backup of the older database will be created automatically and appear in the list after migration;
  4. Migration starts, click the Close button after the migration, the database version has changed
  5. Select the database in the list again and click the select button to activate it.

- **No**:
  1. Select the older database in the 'Databases' list and click the migrate button;
  2. A new migration window will appear. Click the Migrate button. A local backup of the older database will be created automatically and appear in the list after the migration;
  3. Migration starts, click the Close button after the migration, the database version has changed.

8.7 Export Database (*.bak, *.xml) to a Mail, USB, ...

1. Make a local backup first as described in §8.4.1;
2. Two files (*.bak and *.xml) are created in the back up folder `<HiProvision installation Path>\HiProvision Backups\Databases`. The filename includes the database name and a timestamp, for example:
   - db_v424_13012018_091142.bak
   - db_v424_13012018_091142.xml
3. These two files always belong together and must be exported together. These two files must be used later on when importing the database.
4. Just copy these two files on a USB or zip these two files first before sending them as a mail-attachment.

CAUTION: Database filenames must never be changed!

8.8 Import Database (*.bak, *.xml) from a Mail, USB, ...

1. A backed up database exists of two files: *.bak and *.xml. The filename includes the database name and a timestamp, for example:
   - db_v424_13012018_091142.bak
   - db_v424_13012018_091142.xml

2. Copy the two database files (unzip them first if zipped), from your USB or mail-attachment into the folder `<HiProvision installation Path>\HiProvision Backups\Databases` on the HiProvision PC;
3. In HiProvision, click the refresh button in the LOCAL BACKUP DATABASES section. The database from your USB/mail will show up in the Local Backups list;
4. Restore this database as described in §8.5.1.

CAUTION: Database filenames must never be changed!

9. ALARM HANDLING

9.1 General

When an alarm situation occurs in a Dragon PTN network, a corresponding alarm will be raised in HiProvision. These alarms can be detected and viewed in several ways in HiProvision:

- Dashboard → (Monitoring) Alarms Tile;
- Dashboard → (Monitoring) Network Tile;
- Dashboard → (Configuration) Network Hardware Tile;
- A flashing dashboard tab indicates active alarms;

9.2 Hardware: Measured/Programmed/Configured Values

This paragraph describes the concept of configuration consistency and synchronization between HiProvision and the live network.

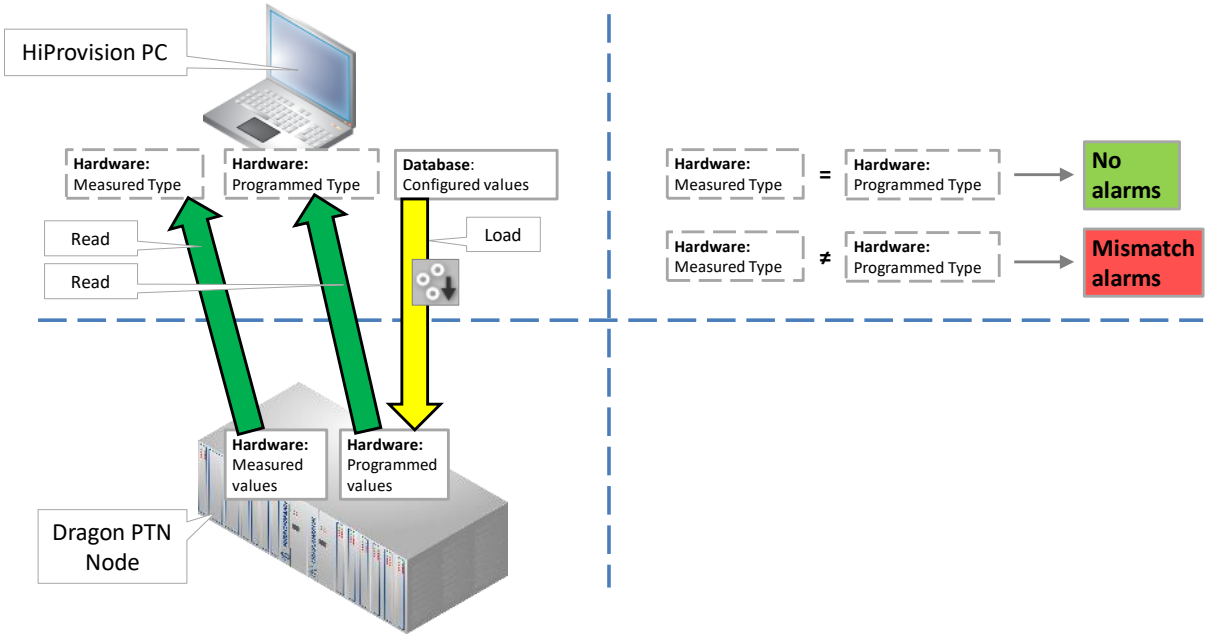


Figure 70 Measured / Programmed / Configured Values

- Measured values: network elements (e.g. PSUs, CSM, IFMs, ….) that are really physically present in the live network or nodes and which are measured or read by HiProvision. These values are read and filled out by HiProvision in the Measured Type field (Network Hardware tab) of the node modules;
- Programmed values (=expected values): programmed configuration (e.g. PSUs, CSM, IFMs, ….) available in the live network or nodes. This online configuration is a result of a load action via HiProvision. This programmed configuration is read and filled out by HiProvision in the Programmed Type field (Network Hardware tab) of the node modules;
- Configured values: database configuration (e.g. PSUs, CSM, IFMs, ...) that a HiProvision administrator configures in HiProvision. Via a load action, the database configuration is loaded from HiProvision into the programmed values in the live network.
- If not all values (measured, programmed and configured) are the same, a mismatch alarm will be raised. E.g. if you configured and programmed a 4-GC-LW module in slot1 of node 100 but slot1 of node 100 is empty in the live network, a mismatch alarm will be raised.

9.3 Alarm Sensitive Properties in HiProvision

An alarm sensitive property in the Network Hardware tile is a property:

- marked by a little square box behind the field, see figure below;
- that has two fields:
  - upper field1: Measured value from the live Dragon PTN network;
  - lower field2: Configured expected value in HiProvision. This field is only visible after clicking the little square box;

HiProvision polls and measures the Dragon PTN network. If a mismatch occurs between the measured and the configured expected value for this property, an alarm is raised and the little square box gets the alarm color.

Little box color:

- Grey: everything is ok, no alarm;
- other color: alarm active, see §9.4;

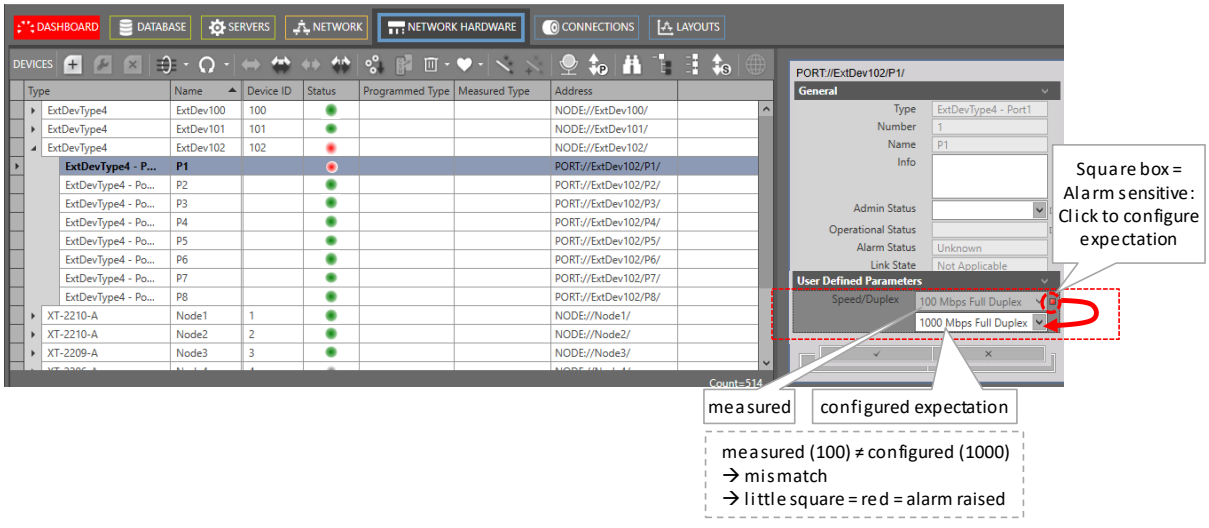


Figure 71 Alarm Sensitive Properties: Little Square Box

9.4 Alarm Colors and Severity

The severity of an alarm is indicated by a color:

- Dark red: Critical alarm (highest severity);
- Red: Major alarm;
- Orange: Minor alarm;
- Yellow: Warning (lowest severity);

9.5 Alarms Tile and Window

9.5.1 The Tile Itself

The Dashboard → Alarms tile itself indicates the active alarms. The tile color indicates the color of the severest alarm that is still active, see §9.2 for alarm colors and severity.

9.5.2 Alarms Window

Clicking the Alarms tile shows the window below. It lists all the alarms with some basic information whereas the bottom section shows detailed information of the selected alarm.

NOTE: An overview of all the possible alarms can be found in Ref.[19] in Table 1.

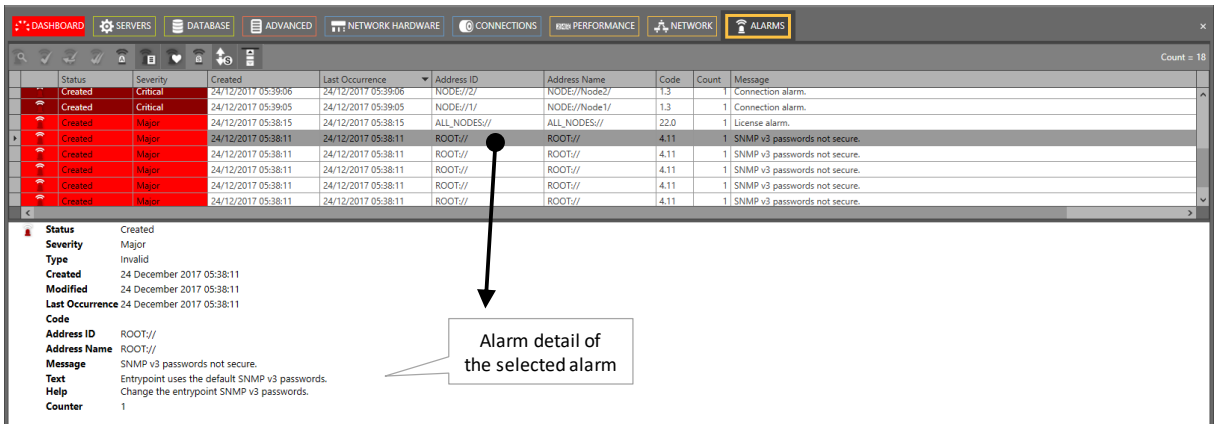


Figure 72 Alarms Window

NOTE: You could use additional table filters for filtering out alarms, see also §15.1.2e.

NOTE: Raised Timestamp (field only visible in Alarms detail when alarm raised by hardware): In the Alarm Detail, 'Created' indicates the timestamp when the alarm was created in HiProvision whereas 'Raised Timestamp' indicates the timestamp when the alarm occurred somewhere in the hardware. Most of the time, the alarm is raised in HiProvision itself resulting in only the 'Created' field filled out. Some alarms are raised in hardware (not in HiProvision), resulting in both the 'Raised Timestamp' and 'Created' field filled out. Good to know: 'Raised Timestamp' = value set by node = UTC, 'Created' = MS Windows PC time UTC + offset!

9.5.3 Alarm Colors and Severity

The alarm severity is indicated in the Severity column and reflected by the row color in the list. The meaning of the colors can be found in §9.2.

9.5.4 Alarm Status

The alarm status is indicated by a status icon and column in the list, see below. An alarm disappears automatically out of the list after it has been cleared and acknowledged.

- Created: alarm is active but not yet acknowledged;
- Acknowledged: alarm has been acknowledged, it means that the operator has indicated that he/she is aware of the alarm existence;
- Cleared: alarm has disappeared or the error situation has gone before it has been acknowledged.

9.5.5 Action Buttons

The buttons below can be used to handle alarms in the alarm window:

- : Navigate to the source of the selected alarm or warning in HiProvision for further investigation;
- : Acknowledge the selected alarm or warning, the status icon changes into ;
- : Acknowledge all the alarms and warnings, all the status icons changes into ;
- (enabled): Auto-Acknowledge of alarms is enabled, all new alarms are acknowledged automatically without any user action. Clicking this icon disables it;
- (disabled): Auto-Acknowledge of alarms is disabled. Clicking this icon enables it;
- (enabled): Alarm logging to a log file is enabled. Clicking this icon disables it;
- (disabled): Alarm logging to a log file is disabled. Clicking this icon enables it;

NOTE: Log file in <HiProvision Install Path>\HiProvision\HiProvision_VX.Y.Z\Logging\System Logging\Alarms

- (enabled): 'Keep alarm logging alive' is enabled. If no alarm has been raised the last hour, an event is written to the Event log file. Clicking this icon disables it;
- (disabled): 'Keep alarm logging alive' is disabled. If no alarm has been raised the last hour, nothing is written to the Event log file. Clicking this icon enables it;

NOTE: Event log file in <HiProvision Install Path>\HiProvision\HiProvision_VX.Y.Z\Logging\System Logging\LogEvents

- (enabled): All the alarms, including the SysLog alarms are shown together in one list in the alarm window. Clicking this icon disables it;

- (disabled): SysLog alarms are filtered out from the other alarms and shown in a separate list at the bottom section of the alarm window. Clicking this icon enables it;

- (greyed out): is enabled. Syslog events are integrated in the alarms list itself and as a result cannot be shown/hidden separately.
- (enabled): is disabled. Shows the separate SysLog alarms at the bottom of the page.
- (disabled): is disabled. Hides the separate SysLog alarms at the bottom of the page.

- (enabled = default): Each time when a new alarm is raised, the alarm view automatically scrolls to the top of the alarms list, so that the latest alarms are automatically viewed.
- (disabled): The alarm view remains its view when a new alarm is raised. No automatic jump to the top of the alarms list when a new alarm is raised.

- SysLog alarms:
  - are alarms and events generated by the system itself e.g. authentication failure etc. which are quite different from Dragon PTN network configuration alarms;
  - are only visible in the Created state;
  - are removed from the alarm list immediately after it has been acknowledged;
  - never clear automatically, they will be cleared when they are acknowledged;

9.6 Alarms in (Monitoring) Network Tile

9.6.1 Network Example

Depending on the network element (device/link/tunnel/service), alarms are visualized in various ways (colors, colored bullets, cloud icons) on various locations (tables, network drawing, navigation section) in the Network Tile. See some example figures below. More information about the alarms and the meaning of them can be found further on.

NOTE: Cloud icons refer to alarms related to 'External E1 Links' interconnecting the Dragon PTN network over an external network, see also §2.6.2b.

NOTE: Displayed Column: ‘X’ indicates the selected network element , ‘(x)’ indicates a linked network element of the selected ‘X’ network element, see also §9.6.4.

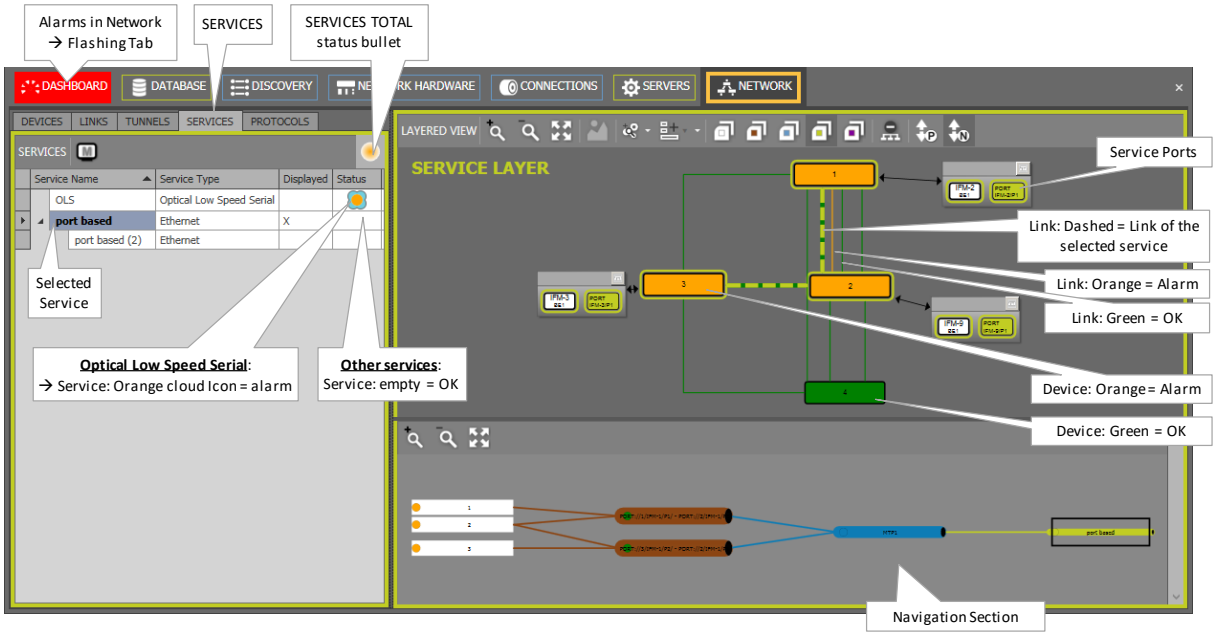


Figure 73 Alarms in Example Network: Services Tab

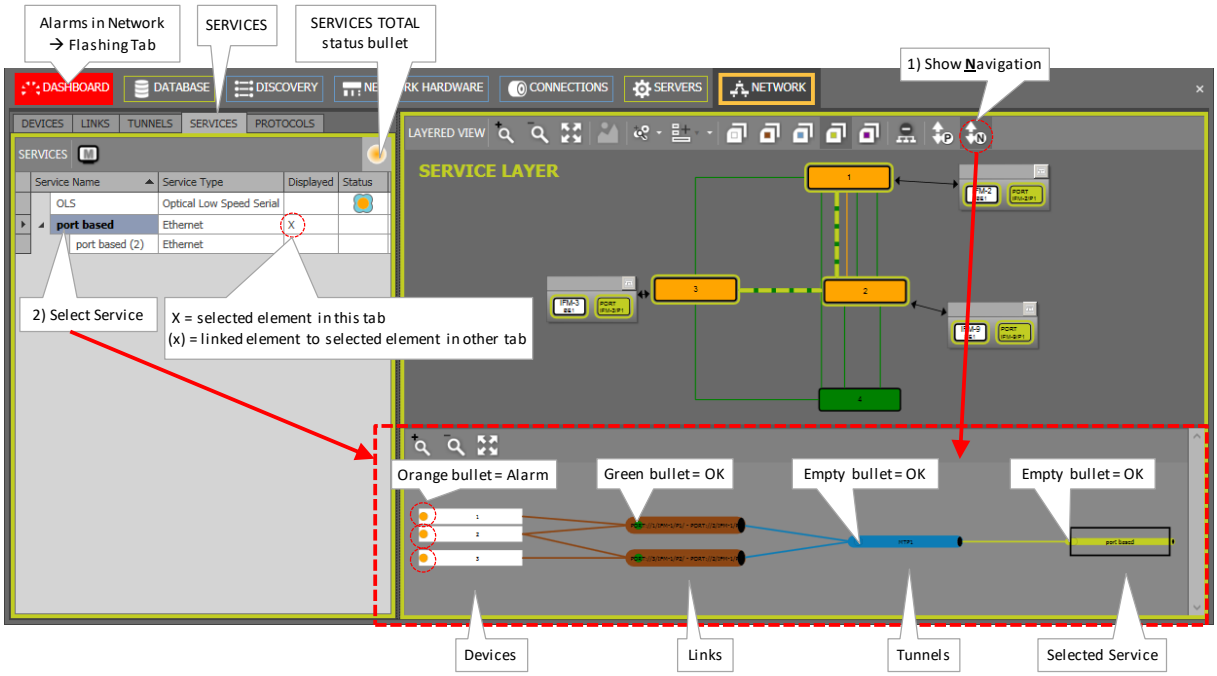


Figure 74 Show Navigation (N) of Selected Device/Link/Tunnel/Service

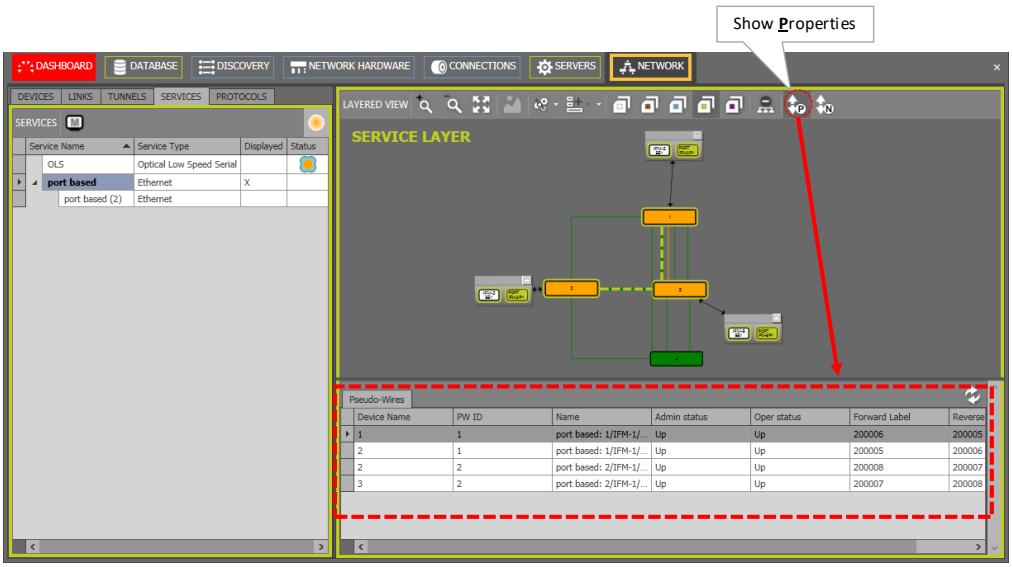
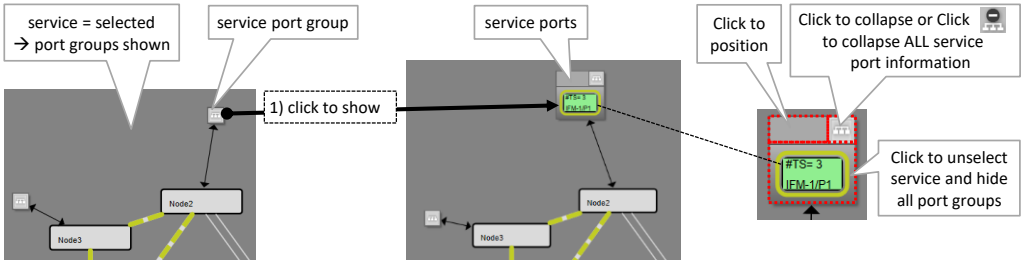


Figure 75 Show Detailed Properties (P) of Selected Tunnel or Service

9.6.2 Menu Buttons

Table 14 Menu Buttons

Button	Short Description
	Zoom in / Zoom out in the network drawing
	Fit content, the layout is maximally fitted within the HiProvision screen. If your nodes and links look lost, click this button to bring them back in focus.
	Shows/hides the background picture of this network drawing. If there is no background picture, the button will be greyed out.
	**Commit**: Commits the pending upgrades, modules or nodes will swap to another image and will reboot
	**Checked/Unchecked**: shows/hides the link labels (on both sides of the link) in the network drawings. A link label shows the IFM slot and the used link port in that IFM e.g. 'IFM-4/P2'.
	Displays the clicked or selected device Layer (white)/ Link Layer (brown) /Tunnel Layer (blue)/ Service Layer (green) / Protocols Layer (purple). Clicking or selecting a row in the associated table (or tab) has the same effect as clicking these buttons. Note: the Protocols Layer is used for RGERP and MRP (see Ref. [2Eth] in Table 1) monitoring.
	When having selected a service in the services table, this icon can be clicked to collapse all service port information in the network drawing. As a result, the network drawing is less detailed and shows a better overview. See the figure below for some extra options. 
	Shows/hides the monitoring **P**roperties of the selected tunnel or services, see example Figure 75.
	Shows/hides the **N**avigation of the selected element. It shows how the selected network element is interconnected with other elements, see example Figure 74.

9.6.3 Status / Colors / Bullets / Clouds

The meaning of the alarm colors can be found in §9.2.

The table below lists the possible alarm indications and how they are visualized on the different network elements and locations.

When an alarm color turns green (devices/links) or disappears (tunnels/services), it means that the alarm has been cleared on this network element. It cannot be viewed in this screen whether an alarm has been acknowledged, see also §9.5.

Table 15 Alarm Indications

Network Element	Alarms in Network Element Table (or Tab)	Alarms in Network Drawing	Alarms in (N) Navigation Section
Device	- per network element via colored status bullets; - per network element table (or tab): one colored status bullet for the entire table in the top right-hand corner indicating the severest alarm color of all its network elements in the table. E.g. if you have two devices e.g. with status bullet of device1 = 'orange' and status bullet of device3 = 'green', the total status bullet of the devices will be 'orange' (orange is more severe than green). - No alarm, everything OK: - Devices/Links: green status bullet; - Tunnels/Services: no status bullet; - Network Element offline: grey status bullet;	- Via colored device icons; - No alarm, everything ok = green device icon; - Offline: grey device icon;	- Via colored status bullets; - No alarm, everything ok = green status bullet; Offline = grey bullet;
Link		- Via colored links - No alarm, everything ok = green link; - Offline: grey link;	- Via colored status bullets; - No alarm, everything ok = green status bullet; - Offline = grey bullet;
Tunnel		None	- Via colored status bullets; - No alarm, everything ok, offline = Empty status bullet;
Service		None	- Via colored status bullets - No alarm, everything ok, offline = Empty status bullet;
Protocols	None	None	None

Note: If the network element is involved in an 'External E1 Link', its colored status bullet will be embedded in the cloud icon in the Tables and Navigation Section. 'External E1 Links' must only be used when the Local Mode service is used on 2-OLS or 2-C37.94 IFMs (see Ref. [2Leg] in Table 1).

- = External E1 Link: (empty): No Local Mode service on this link → link ports and link are down;
- = External E1 Link: (grey) link status unknown, HiProvision offline;
- = External E1 Link: (green), Local Mode service on this link, link is up and running, all OK;
- = External E1 Link: (yellow), Local Mode service on this link, warning on link;
- = External E1 Link: (orange), Local Mode service on this link, minor alarm on link;
- = External E1 Link: (red), Local Mode service on this link, major alarm on link;
- = External E1 Link: (dark red), Local Mode service on this link, critical alarm on link;

If an 'External E1 Link' is selected, its cloud icon will be shown on the link in the network drawing as well.

9.6.4 Selected Network Elements

In the table section on the left-hand side, the selected element shows an 'X' in the Displayed column. All the other related network elements in the other Tabs (e.g. Devices, Links,

Tunnels) show a '(x)' in the Displayed column. In the network drawing, the selected network element will be highlighted.

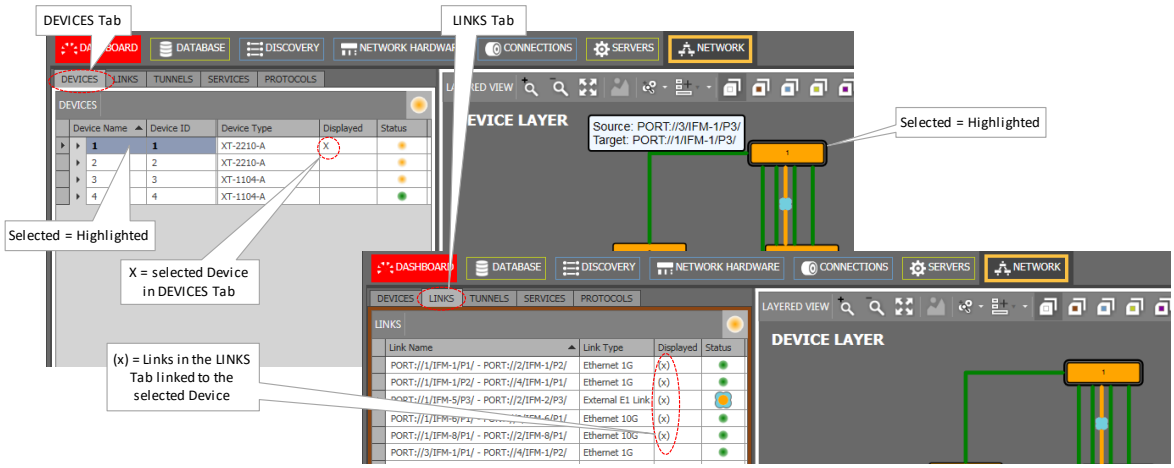


Figure 76 Selected Network Elements: X / (x) in Displayed Column

9.6.5 Protected Tunnel: Broken Working Path

The example below differs from the example in previous paragraph. It indicates via '//' how to see whether a working path in a protected tunnel is broken or the protection path is active. This view is visible when selecting a tunnel or tunnel layer in the (Monitoring) Network Tab. Also have a look in Ref. [2Net] in Table 1.

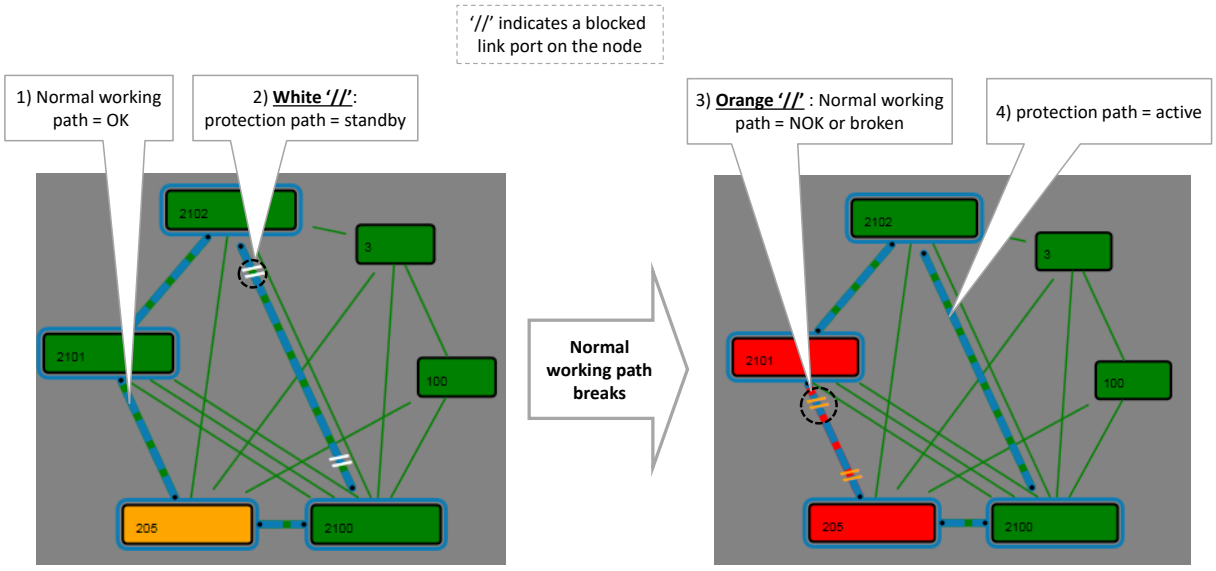


Figure 77 Protected Tunnels: Protection Path, Blocked Port Indication: '//'

9.7 Alarms in (Configuration) Network Hardware Tile

After clicking the Network Hardware tile, a window like Figure 44 pops up. The status bullets in the devices and links list indicate whether the network element has alarms or not. See §2.6.3 for more info.

9.8 Configure Alarms for NSM Digital Input Contacts

An alarm can be assigned to the NSM digital inputs DI1/DI2. It means that a change in these contacts can raise an alarm in the Alarms Window (see §9.5.2). The alarm can be configured via the Network Hardware tile by clicking the NSM in the desired node and filling out the I/O section on the right-hand side. An alarm will be raised for DI1 when following two conditions are met (similar for DI2):

- 'DI1 Current Detected' mismatches the configured expectation for this field. The expectation can be configured via clicking the little square box behind the field and selecting Yes/No. Example mismatch: the expectation is 'Yes' and no current is detected (=DI1 Current Detected = 'No') (or vice versa);
- A severity different from 'none' has been configured;

Following fields can be configured for DI1 (similar for DI2):

- DI1 Input:
  - DI1 Current Detected (Yes/No): Indicates whether input current has been detected; Configure the expectation via the little square box;
  - DI1 Alarm Severity: None (=default), Indeterminate, Warning, Minor, Major, Critical; 'None' means that no alarm will be raised for this input;
  - DI1 Alarm message: Fill out a short alarm message that will appear in the (Alarms Window);
  - DI1 Alarm Text: extra info to describe the alarm (Alarms Window - detail);
  - DI1 Alarm Help: what to do when this alarm occurs (Alarms Window - detail).

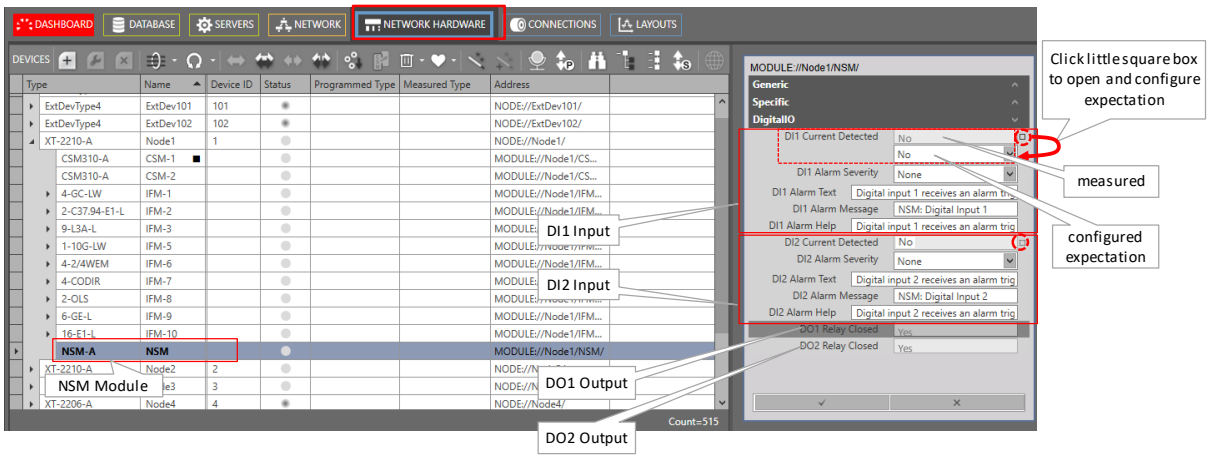


Figure 78 NSM Digital I/O Contacts

9.9 Device Alarms via Digital Output Contacts on the NSM

9.9.1 General

The CSM supervises all the hardware in the node and generates the necessary device alarms when something is wrong in the node. These alarms are collected by HiProvision. HiProvision can be configured to output one or more of these device alarms to the digital output contacts (DO1=minor, DO2=major) on the NSM (=Node Support Module).

NOTE: The measured state of the output contacts DO1/DO2 can be viewed in Figure 78.

These contacts can be used for example to activate an alarm siren. The NSM can be found in the nodes manual, see Ref. [8], [9] in Table 1.

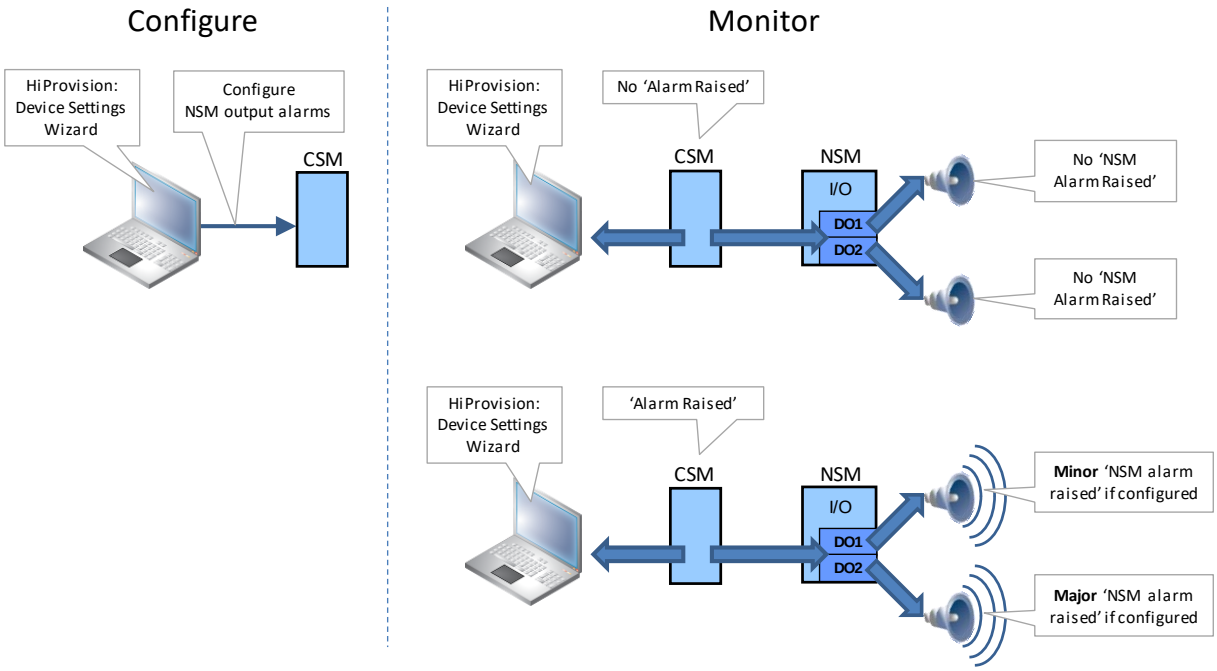


Figure 79 Operation Of Device Alarms/Digital Outputs

9.9.2 Device Settings Wizard

These alarms can be configured via the Device Settings. Select the CSM of the intended node, click the button, select 'Digital Output' and fill out the Alarm Severity and Alarm Trigger by clicking the cell and selecting a value. Apply the changes. See figures below.

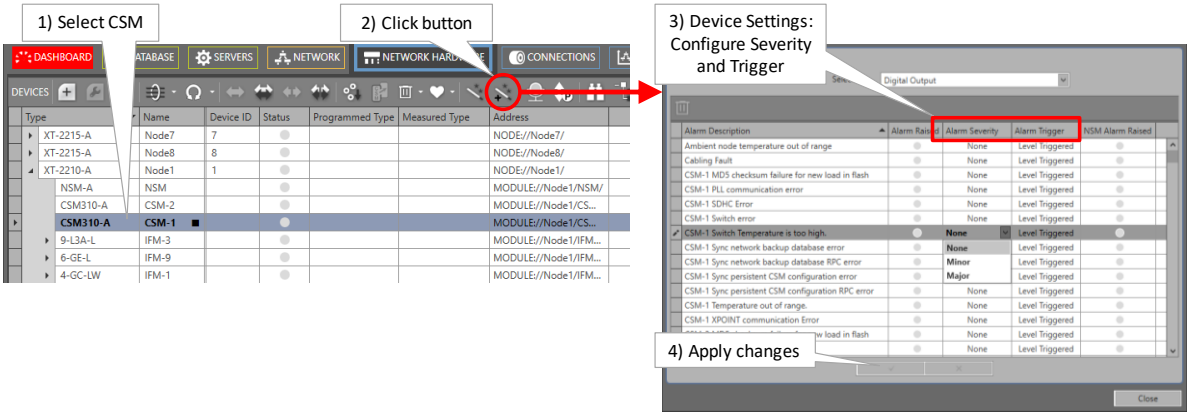


Figure 80 From CSM to Device Settings

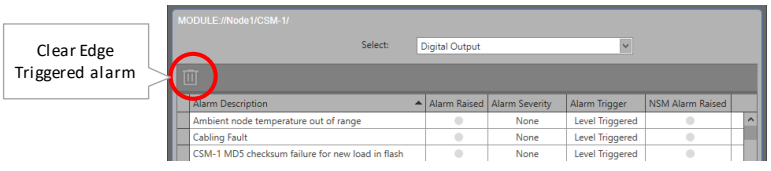


Figure 81 Device Settings: Clear Edge Triggered Alarm

Device Settings:

- Lists all the possible device alarms. These alarms can be configured towards the digital outputs (DO1/DO2) on the NSM, but can also be used to monitor these alarms via the 'Alarm Raised' and 'NSM Alarm Raised' LED. If one of these alarms occur, they will also appear in the general Alarms window in §9.5.2.
- Alarm Description: short description of the device alarm;
- Alarm Raised: this LED turns red if the associated alarm occurs. This LED turns green again when the alarm disappears. It just follows the alarm existence, regardless the configured Alarm Severity and Alarm Trigger;
  - green LED: alarm is not active on the CSM or in the node;
  - red LED: alarm is active on the CSM or in the node;
- Alarm Severity: Click the cell to open a drop-down list. Select None, Minor or Major.
  - None: this alarm will not be outputted on the NSM DO contacts, although the alarm may be active (Alarm Raised LED is red);
  - Minor: if this alarm occurs on the CSM or in the node, it will deactivate the NSM **DO1** contact (if not already deactivated by another minor alarm). It will also darken the **DO1** LED on the NSM (if not already darkened by another minor alarm);
  - Major: if this alarm occurs on the CSM or in the node, it will deactivate the NSM **DO2** contact (if not already deactivated by another major alarm). It will also darken the **DO2** LED on the NSM (if not already darkened by another major alarm);
- Alarm Trigger / NSM Alarm Raised:
  - Level Triggered: The 'NSM Alarm Raised' LED turns red if the associated alarm occurs. This LED turns green again when the alarm disappears. The clear button will never be active for a Level Triggered alarm;
  - Edge Triggered: The 'NSM Alarm Raised' LED turns red if the associated alarm occurs. This LED remains red (although the error may have disappeared) until the alarm has been selected and the clear button has been clicked.

NOTE: If an alarm situation changes, the LEDs in HiProvision and the DO LEDs/DO contact on the NSM change a few seconds later;

9.10 Alarms in Large Network Monitor (LNM)

Alarm indications in the LNM tile occur in exactly the same way as alarm indications in the Network drawing of the Network tile.

- For alarm indications in the Network tile, see §9.6.
- For an overview of the LNM description, see §16.

10. HIPROVISION REDUNDANCY

10.1 General

Prerequisite: The HiProvision Redundancy feature needs one voucher or license for the entire Dragon PTN network. The generated license pack or file must be placed on both the HiProvision Servers. See §4 for more voucher and license info.

HiProvision Redundancy means that two HiProvision PCs are connected to the Dragon PTN network via a CSM with each CSM located in a different node. If one HiProvision PC fails the other PC will take over in order to maintain network connectivity.

One PC is the Master while the other is the Redundant PC. The Master PC is the PC on which all the redundancy configurations will be done (see further).

At startup, the Master is 'Started' and the Redundant PC is 'Standby'. The 'Started' PC will be able to do all the network configurations and monitoring. The 'Standby' PC is just waiting and will not be able to configure/monitor the network, all tiles (except database and servers tile) will be locked on the 'Standby' PC.

The 'Started' PC will push all its network modifications to the 'Standby' PC (=database replication, synchronization). In case of problems or a switchover request, the 'Standby' PC becomes 'Started' and the previous 'Started' one becomes 'Standby'. In some problem scenarios, both PCs can be 'Started' at the same time.

HiProvision Redundancy is non-revertive.

Both PCs communicate via heartbeat signals over DCN through the Dragon PTN network. Database replication and synchronization occurs via an Ethernet service through Dragon PTN or via an external LAN. Using an external LAN is better for redundancy reasons. An external LAN requires an extra NIC (=Network Interface Card) per PC. A basic HiProvision Redundancy set up can be found in the picture below:

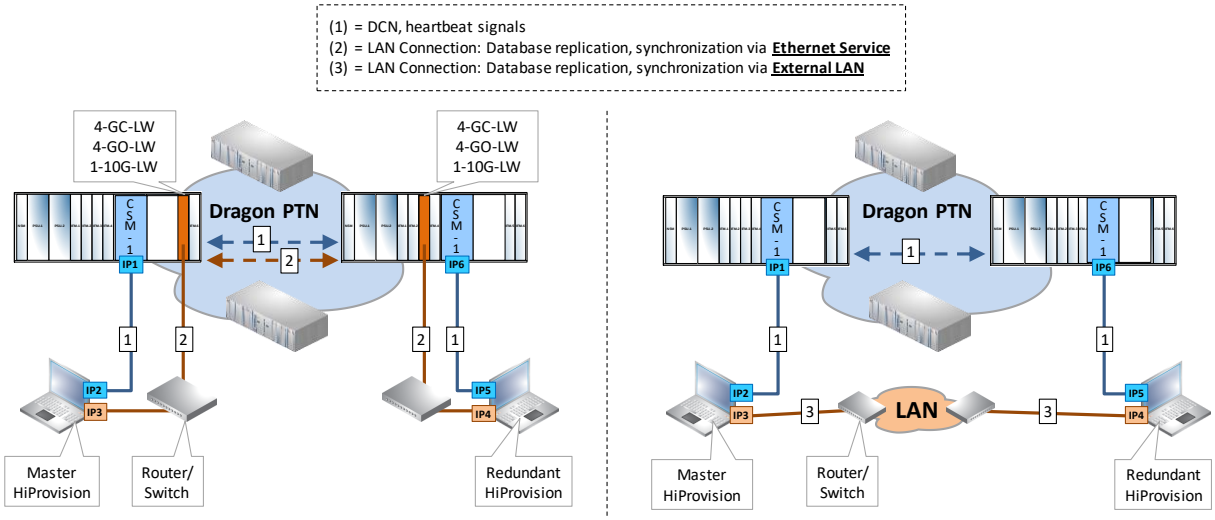


Figure 82 Basic HiProvision Redundancy: Via Ethernet Service/External LAN

10.2 Set up HiProvision Redundancy

Prerequisites:

- Make sure that both PCs are correctly connected to the Dragon PTN network via the CSMs with respect to the correct IP ranges;
- Both HiProvision PCs must have a full HiProvision Installation;
- Make sure that HiProvision Redundancy voucher or license is installed on both the servers, the entire license pack (or *.dat file) must be copied from the master server to the redundant server;

10.2.1 Actions on the Redundant HiProvision PC

On the Redundant HiProvision PC, only the HiProvision Agent must be started (see §3). All other configuration actions must be done on the Master HiProvision PC.

NOTE: Starting the HiProvision Agent is enough to make HiProvision Redundancy operational. In addition, if you want to look/manage the network via the HiProvision client of the Redundant HiProvision PC, the client has to be started manually.

10.2.2 Actions on the Master HiProvision PC

Follow the steps below to set up and start HiProvision Redundancy:

1. Click on the Dashboard → Servers Tile. Without a Redundant setup, only a Master Server PC will be visible:

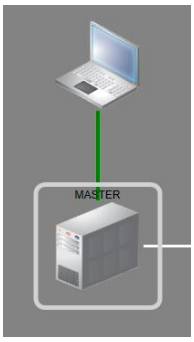


Figure 83 Master PC Only, No Redundancy

2. Start the servers via clicking the play button ;
3. Only one Discovery Entry Point must be created for a solution where both redundant PCs have only one cable connection to the Dragon PTN network. Make sure that both 'Mgt. IP Address' and 'Red. Mgt. IP Address are filled' out in the Discovery Entry Points, see figure below.

   NOTE: Other HiProvision Redundancy use cases between the HiProvision PCs and the Dragon PTN network, and their corresponding Entry Points can be found in §11.

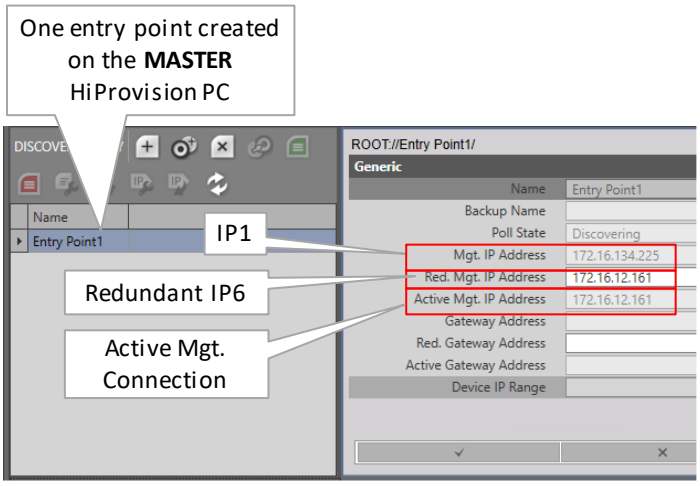


Figure 84 Discovery Entry Point: Redundant Management IP Address

NOTE: More info on Discovery Entry Points, see §2.5.2. More redundancy use cases with IP address examples can be found in §11;

4. Click the add button to create a HiProvision Redundancy setup. As a result, both a Master and Redundant Server will be visible. Just after creation or when Redundancy has been stopped later on via, the Master will be 'started' (=green) and the Redundant server will be 'unknown' (=red). See the global status on the left-hand side.

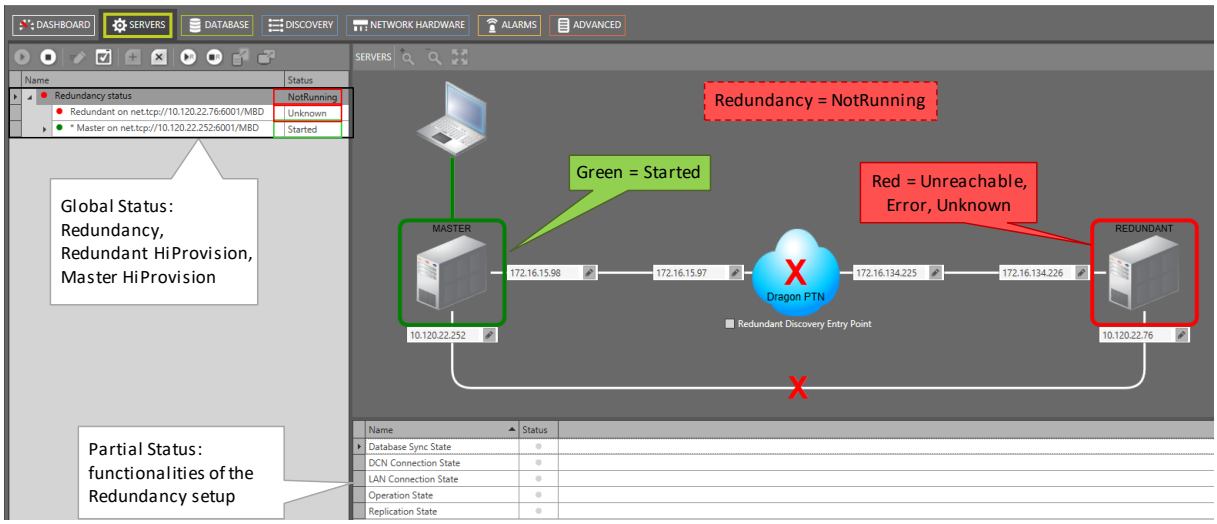


Figure 85 HiProvision Redundancy Setup: NotRunning

5. In case of redundant Entry Points, click the 'Redundant Discovery Entry Point' checkbox first. Fill out the IP addresses by clicking the IP address field and pressing ENTER or clicking in the IP address field.

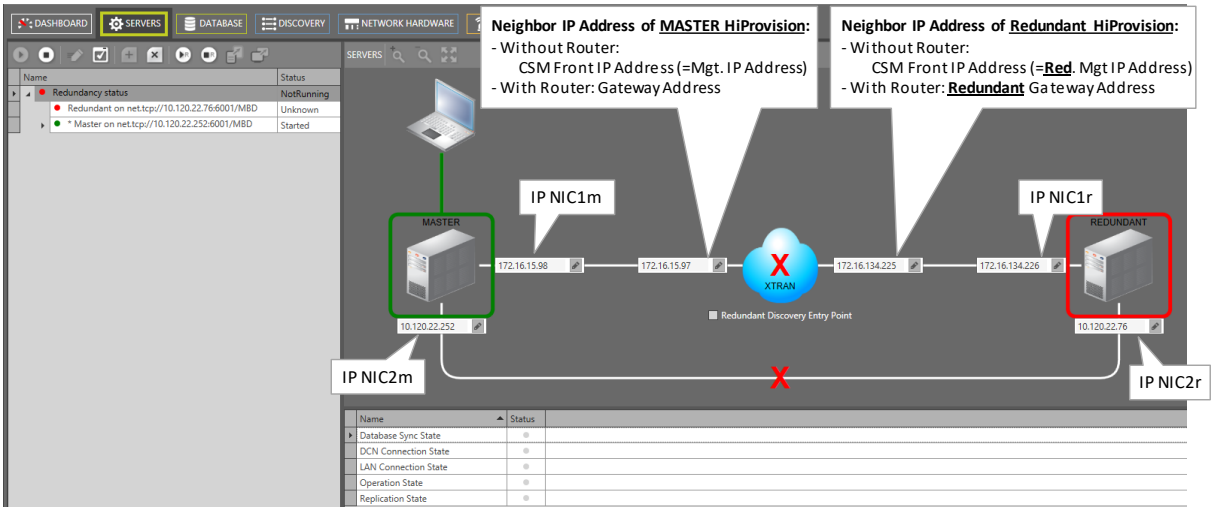


Figure 86 Fill Out IP Addresses

6. At this moment the Redundancy status is 'NotRunning'. Make sure that the HiProvision agent is running (see §3) on the Redundant PC. Start HiProvision Redundancy via clicking the redundancy play button  . The Redundancy starts:

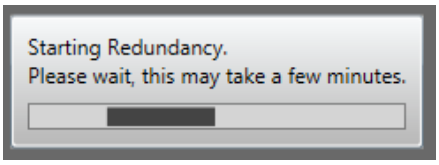


Figure 87 HiProvision Redundancy Starting

7. After the Redundancy has been started and is up and running, it could look like in the figure below. If the Redundancy would not work, verify that some external LAN ports are not blocked by a possible firewall, see §21.6;

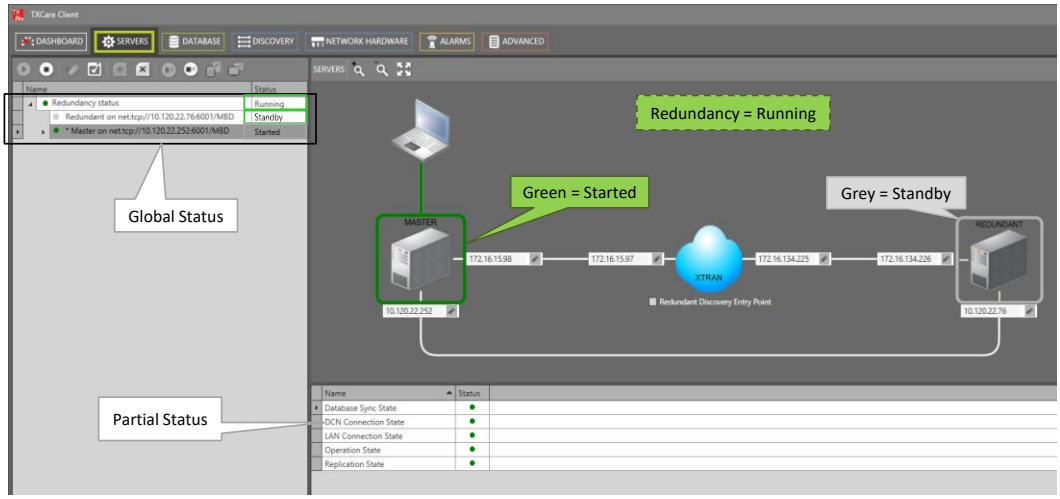


Figure 88 HiProvision Redundancy Setup: Running

Table 16 HiProvision Redundancy Status Info

Status	Description
Global Status	
Redundancy Status	**Running**: The redundancy setup has been started via the play button and is active now. **NotRunning**: The redundancy setup has been stopped via the play button and is not active anymore. **RedundancyError**: Something is wrong with the Redundancy, check the Partial States (see further) to solve the problem;
Master on net.tcp…	**Unknown**: Only possible on the Redundant Server. It means that Redundant Server cannot communicate with the Master Server. **Started**: The Master server is the 'Started' one. HiProvision processes have been started on this server. It means that all the network configurations/monitoring must be done via this PC. **Standby**: The Master server is 'Standby'. It is ready to take over in case something goes wrong on the other side or a switchover is initiated via clicking ;
Redundant on net.tcp..	**Unknown**: Only possible on the Master Server. It means that the Master Server cannot communicate with the Redundant Server. **Started**: The Redundant server is the 'Started' one. HiProvision processes have been started on this server. It means that all the network configurations/monitoring must be done via this PC. **Standby**: The Redundant server is 'Standby'. It is ready to take over in case something goes wrong on the other side or a switchover is initiated via clicking ;
Partial Status	
DCN Connection State	Heartbeat signals are exchanged between the two servers over the DCN channel through the Dragon PTN network. **Green/Red**: This server **can/cannot** communicate with the other server via heartbeat signals.
LAN Connection State	Database replication and synchronization occurs via an external LAN network or via a programmed Ethernet service over the Dragon PTN network. **Green/Red**: This server **can/cannot** communicate with the other server via the external LAN path or via a configured Ethernet service in the Dragon PTN Network.
Replication State	**Green**: database replication between the two servers is OK. **Red**: database replication between the two fails or is not OK. This can be due to a failure in the external LAN path, configured Ethernet service or a replication failure on the MySQL Server.
Database Sync State	**Green**: databases on both servers are (or can be) perfectly synchronized **Red**: databases on both servers cannot be synchronized. This can be due to a failure in the external LAN path, configured Ethernet service or database mismatches due to manual database modifications on both sides. Manual modifications on both sides can be done if both servers become 'Started' during a DCN connection state failure. The user must indicate which of both databases the correct one is when this failure occurs.
Operation State	**Green**: The redundancy setup is up and running without errors. **Red**: Both servers are in the 'Started' state which is a failure situation. This is only possible when both servers cannot communicate via DCN and as a result, the server that was in 'Standby' will start itself as a precaution.

8. The Dashboard Servers tile indicates whether the HiProvision Redundancy has been set up or not. A double gear on the Tile means that HiProvision Redundancy has been configured. A green color and 'started' means that the own server is running in case the Redundancy has been stopped or no redundancy or that the redundancy has been started and running without errors.

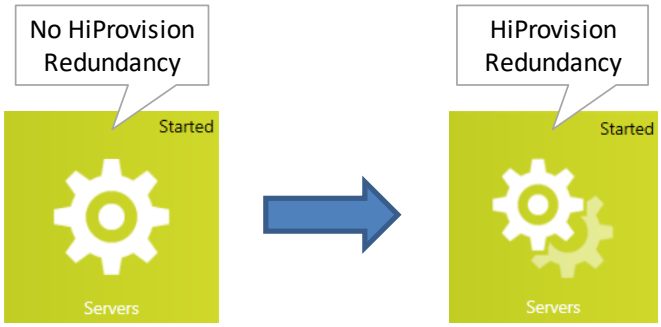


Figure 89 Servers Tile: HiProvision Redundancy

10.3 Stable State: Switchover from Started to Standby HiProvision PC

A manual switchover can be performed when HiProvision redundancy is up and running and everything is fine, no error situations active.

- can be initiated via clicking the server switchover button ;
- makes the 'Standby' PC the 'Started' one and vice versa;
  - Stops the server processes on the 'Started' PC. This PC turns into 'Standby' mode;
  - Starts the server processes on the 'Standby' PC. This PC turns into 'Started' mode;
- can only be performed if one PC is 'Started' and the other is 'Standby';
- can take a few minutes, the total switchover time depends on the database and network size;
- does not cause network interruptions;

10.4 Unstable State: Error Situations

Some common situations are explained below provided that HiProvision Redundancy is up and running.

10.4.1 One or More Server Process Errors on the 'Started' PC

Prerequisites: DCN channel and LAN connection are fine.

If one or more processes on the 'Started' PC fail or don't start for some reason, the 'Started' PC will turn into a 'Failure' state. As a result, an automatic switchover occurs in which the 'Standby' PC becomes 'Started'.

10.4.2 DCN Path Break

Prerequisites: All server processes and LAN connection are fine.

A DCN path break can be the result of a cable break between HiProvision PC and the CSM or a path break somewhere in the Dragon PTN Network. As a result, no more heartbeat signals are possible between the 'Started' and 'Standby' server. Both servers become 'Started'.

The partial states 'DCN Connection state' turns red. If the LAN connection is configured via an Ethernet service, the partial states 'Replication state' and 'Database Sync' turn red as well.

The Redundancy status turns into 'Redundancy Error'. The databases between the two servers cannot be synchronized anymore.

When the DCN connection will be restored later on, it must be decided which of both servers must be the 'Started' one and which one 'Standby'.

10.4.3 LAN Connection Cable Break

Prerequisites: All server processes and DCN channel are fine.

The 'Started' server just keeps running and remains 'Started'. The 'Standby' server remains 'Standby'. The partial states 'LAN Connection state', 'Replication state' and 'Database Sync' turn red. The Redundancy status turns into 'Redundancy Error'. The databases between the two servers cannot be synchronized anymore.

When the LAN connection will be restored later on, the 'Standby' PC will synchronize its database with the one on the 'Started' PC.

10.5 Revertive/Non-revertive Behavior

HiProvision Redundancy is non-revertive: once a switchover of the HiProvision PC has occurred, the new 'Started' HiProvision PC stays 'Started' until a manual switchover or switchover caused by a cable break occurs again. No automatic switchback to the original HiProvision PC will occur when it is up and running again after a breakdown or a failure.

10.6 HiProvision Redundancy with Remote Client

If a remote client is used in combination with HiProvision Redundancy, it is possible to switchover the GUI view of the remote client from one server to the other via the GUI switchover button  . See §13 for more information.

11. HIPROVISION CONNECTIVITY REDUNDANCY: USE CASES

11.1 General

In Dragon PTN, some redundancy solutions are available to provide an enhanced failure proof HiProvision connectivity to the Dragon PTN network. Without HiProvision connectivity, a Dragon PTN network cannot be monitored or configured/modified! Therefore some redundancy is strongly advised.

Depending on the needs, a combination of the solutions below can be implemented to tune or optimize your HiProvision connectivity:

- CSM redundancy (feature license required per node);
- HiProvision PC redundancy (feature license required);
- Management cable/entry point redundancy.

The paragraphs below show some use cases starting from no redundancy at all up to a higher level of redundancy combining one or more of these redundancy solutions.

NOTE: With CSM redundancy, a switchover is only possible when both CSMs have the same firmware version and one CSM is 'active' and the other CSM 'standby'.

11.2 Use Case 0: No Redundancy at All

The HiProvision PC is directly connected via one management cable to a node with only one CSM.

Configuration:

- One IP address on the HiProvision NIC, see §2.1.3;
- One entry point in HiProvision, see §2.5.2;

HiProvision connectivity is lost when:

- The HiProvision PC, management cable or the CSM breaks. When the CSM breaks, the node goes out of service as well.

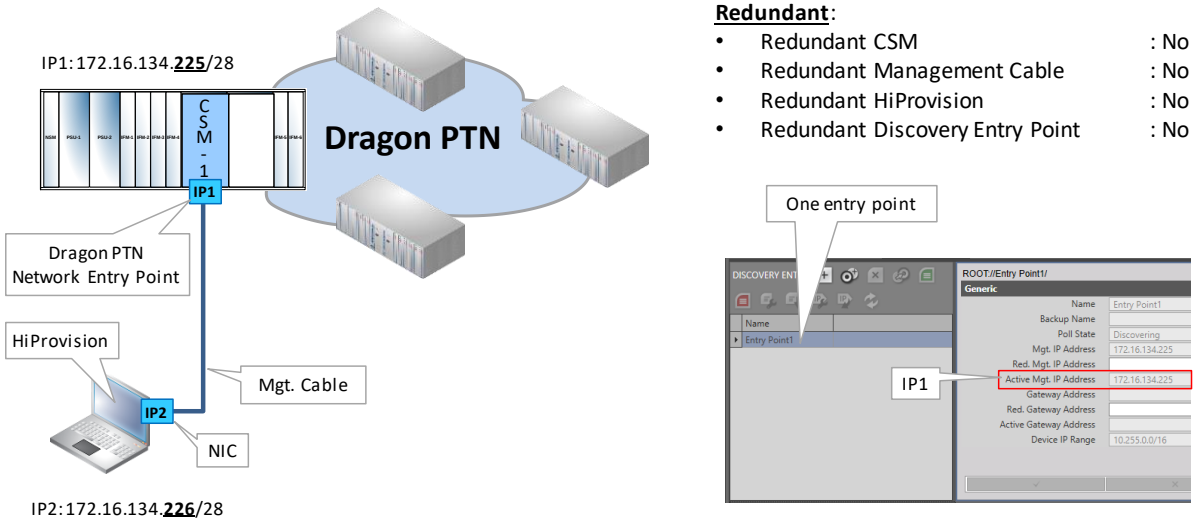
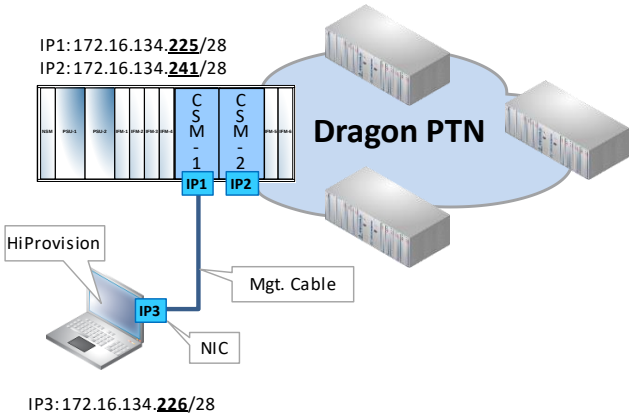


Figure 90 Use Case 0: No Redundancy at All

11.3 Use Case 1: CSM Redundancy Only – Single Cable

CAUTION: The case below is supported if HiProvision is connected to the Active CSM, either directly or via a router/switch, see Use Case 2. If HiProvision is connected to the Standby CSM, and you perform a load action, the network will be unreachable for a few minutes. To avoid this, swap the standby and active CSM via HiProvision (see §2.5.5) before loading.



Redundant:

- Redundant CSM : Yes
- Redundant Management Cable : No
- Redundant HiProvision : No
- Redundant Discovery Entry Point : No

Figure 91 Use Case 1: CSM Redundancy Only – Single Cable

11.4 Use Case 2: One HiProvision PC with Direct Dual Entry Point in One Node

The HiProvision PC with 2 NICs is directly connected via two management cables to a node with redundant CSMs. If the active CSM fails, the standby CSM takes over to keep the node alive.

Configuration:

- One IP address on both NICs in the HiProvision PC, see §2.1.3;
- Two redundant entry points in HiProvision, see §2.5.2 and §2.5.5;

HiProvision connectivity is protected against:

- one CSM failure or a single cable break.

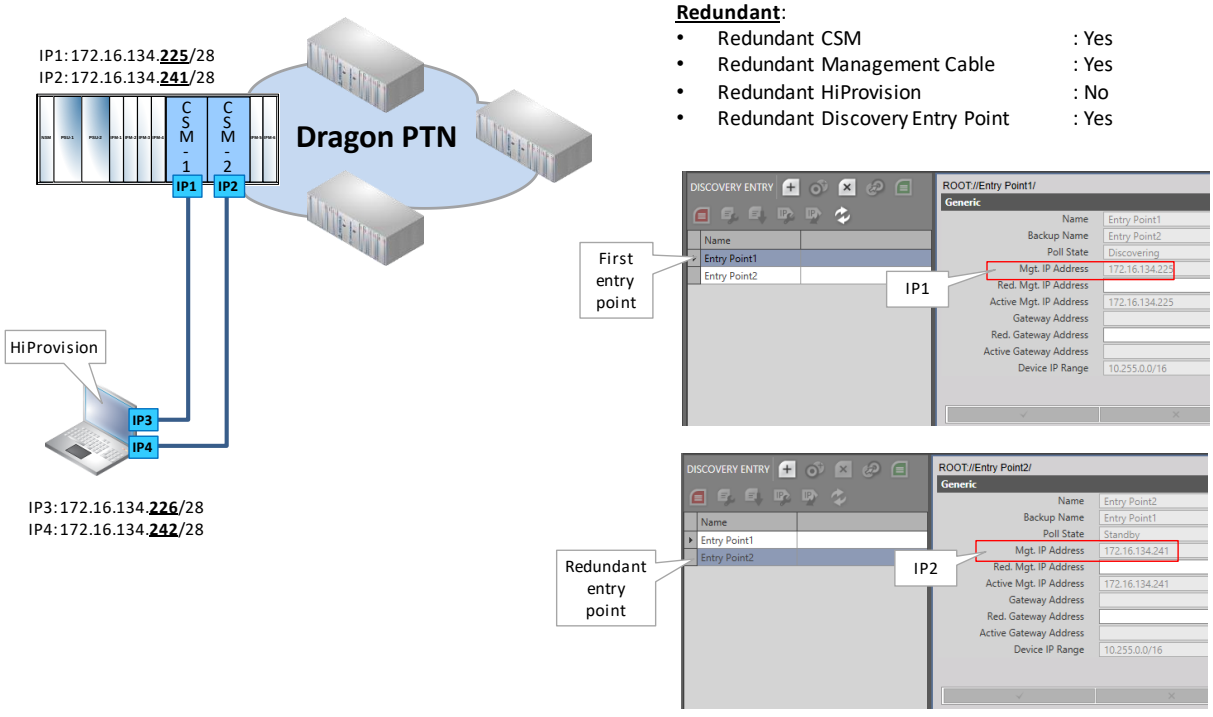


Figure 92 Use Case 2: One HiProvision PC with Direct Dual Entry Point in One Node

11.5 Use Case 3: One HiProvision PC with Direct Dual Entry Point in Two Nodes

The HiProvision PC with 2 NICs, is directly connected via two management cables to two nodes with one CSM in each node. If the first node fails (first entry point), the network can still be configured/monitored via the second entry point.

Configuration:

- One IP address on both NICs in the HiProvision PC, see §2.1.3;
- Two redundant entry points in HiProvision, see §2.5.2 and §2.5.5;

HiProvision connectivity is protected against:

- one CSM failure or a single cable break.

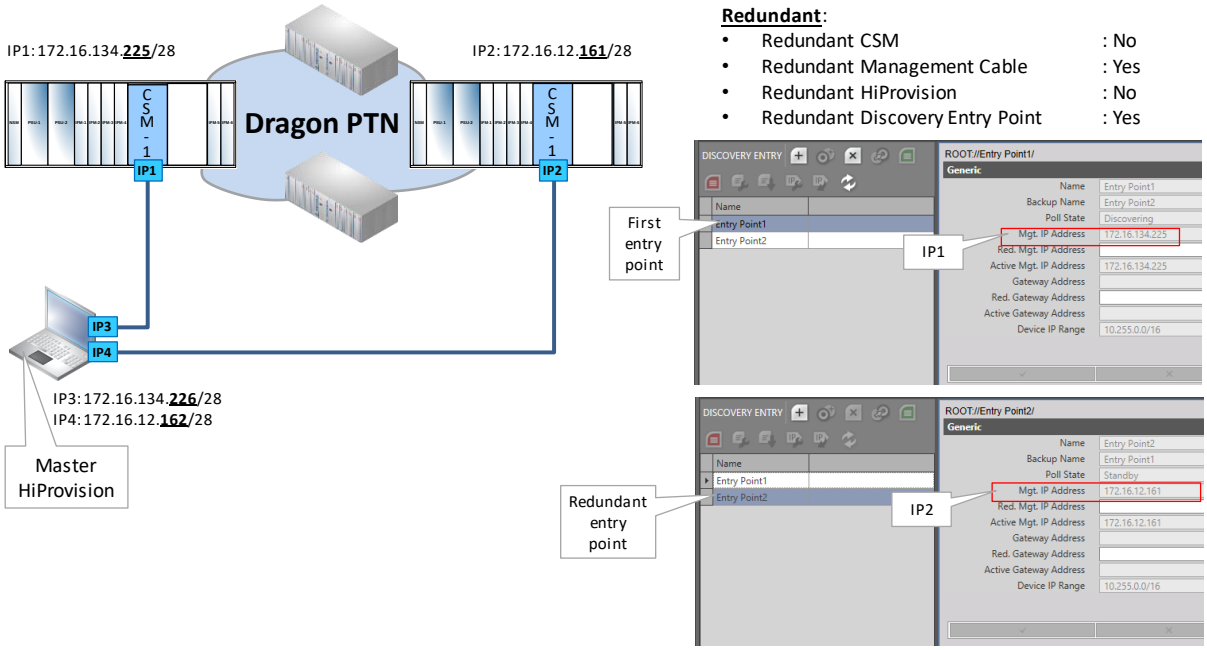


Figure 93 Use Case 3: One HiProvision PC with Direct Dual Entry Point in Two Nodes

11.6 Use Case 4: One HiProvision PC with Dual Entry Point via Switch

The HiProvision PC with 1 NIC, is directly connected via one management cable to a switch. The switch has a double connection to a node with redundant CSMs. If the active CSM fails, the redundant CSM takes over to keep the node alive.

Configuration:

- Two IP addresses on one NIC in the HiProvision PC, see §2.1.3 and §2.1.3b;
- Two redundant entry points in HiProvision, see §2.5.2 and §2.5.5;

HiProvision connectivity is protected against:

- one CSM failure or single cable break between switch and node.

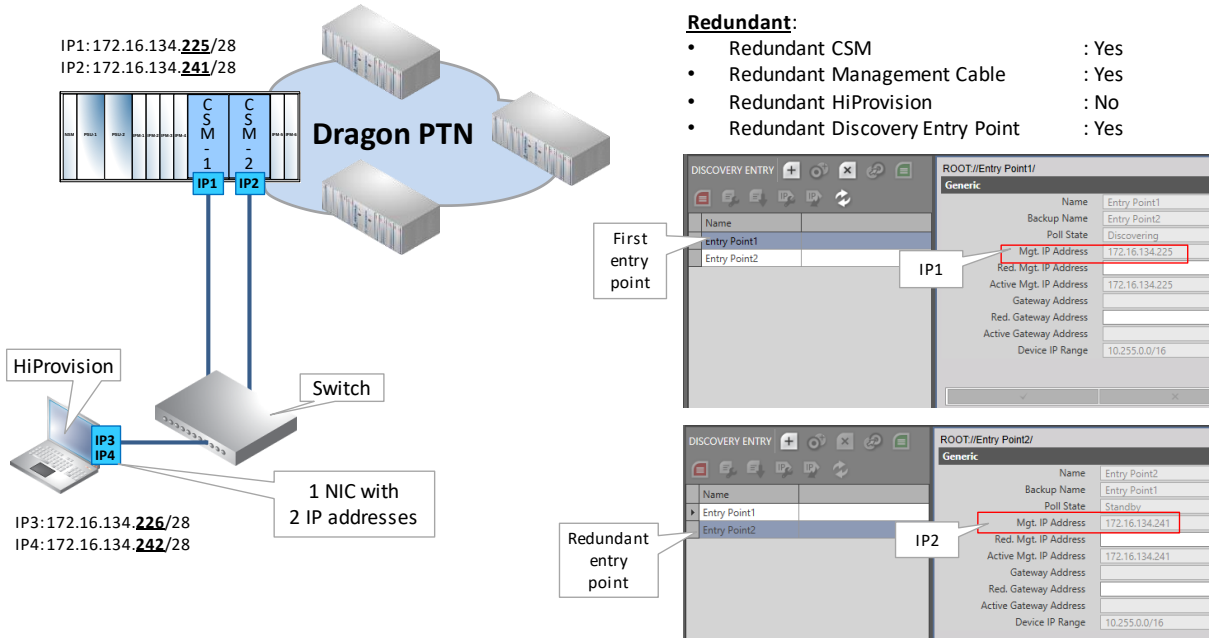


Figure 94 Use Case 4: One HiProvision PC with Dual Entry Point via Switch

11.7 Use Case 5: Redundant HiProvision PCs with Single Entry Point

Two redundant HiProvision PCs, each having 2 NICs, are directly connected via one management cable to a node with only one CSM. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

- One IP address on both NICs on both HiProvision PCs, see §2.1.3;
- One entry point on the MASTER HiProvision PC, see §2.5.2;

HiProvision connectivity is protected against:

- A HiProvision PC break, a connected node breakdown, a CSM failure or a cable break. The node of a broken CSM goes down but connectivity remains. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

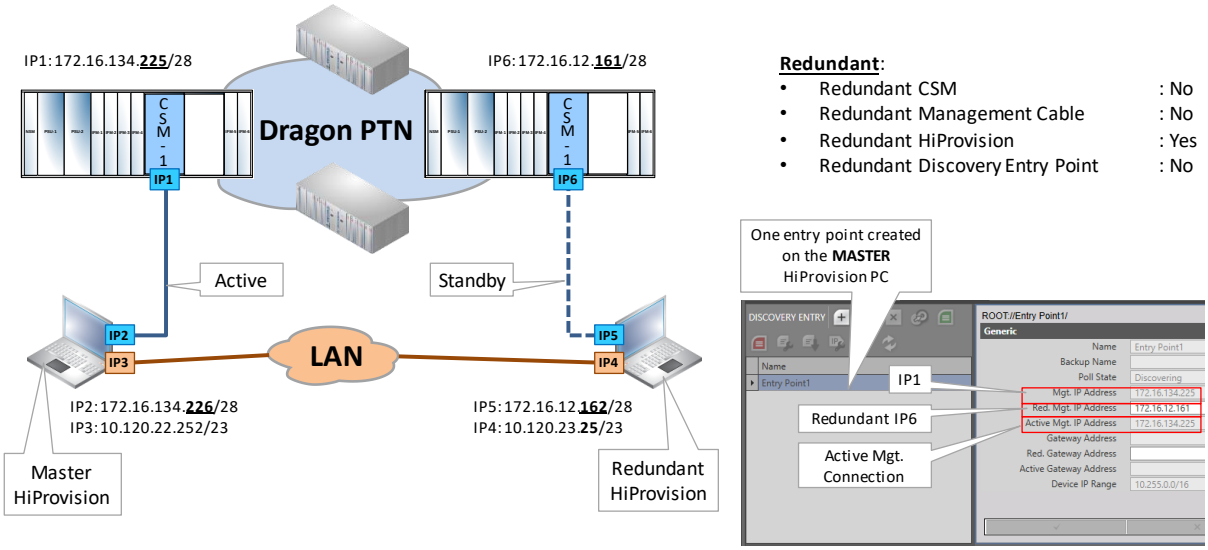


Figure 95 Use Case 5: Redundant HiProvision PCs with Single Entry Point

11.8 Use Case 6: Redundant HiProvision PCs with Dual Entry Point via Switch

Two redundant HiProvision PCs, each having 2 NICs are each directly connected via one management cable to a dedicated switch. Each switch has a double connection to a node with redundant CSMs. If an active CSM fails, the redundant CSM takes over to keep the connected node alive. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

- Two IP addresses on one NIC in each HiProvision PC, see §2.1.3 and §2.1.3b;
- Two redundant entry points on the MASTER HiProvision PC, see §2.5.2 and §2.5.5;

HiProvision connectivity is protected against:

- a HiProvision PC break, a connected node breakdown, a CSM failure or cable break somewhere between HiProvision PC and node. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

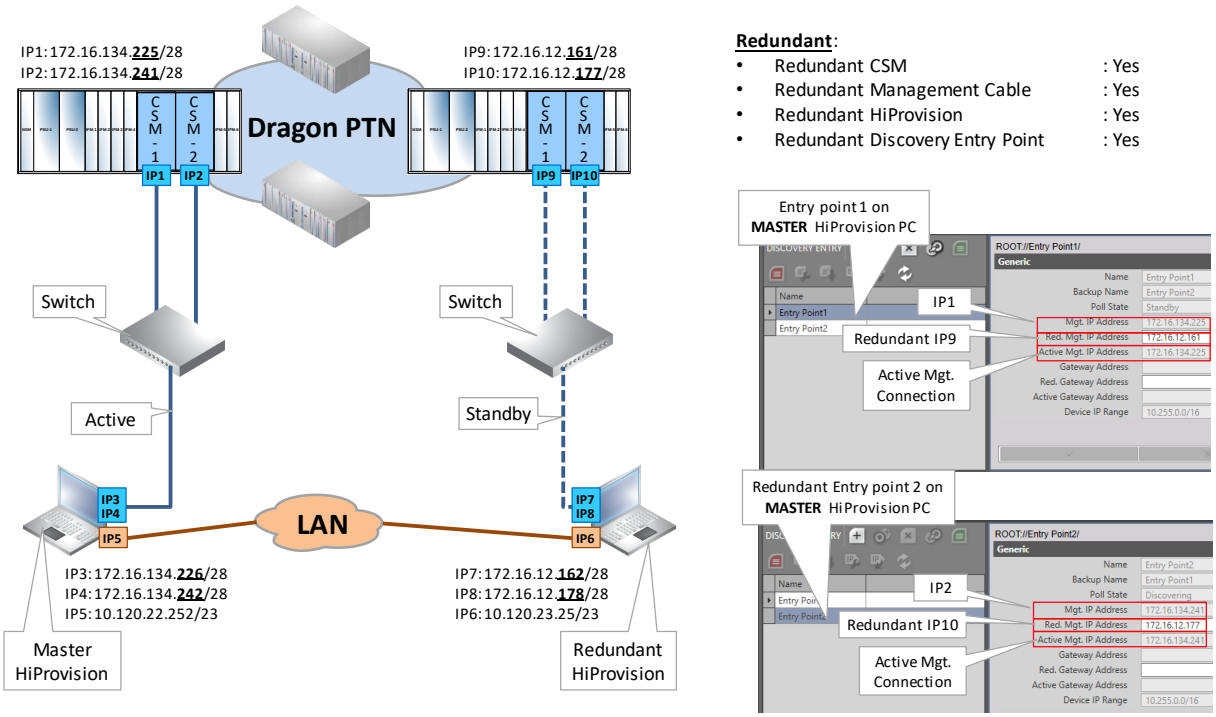


Figure 96 Use Case 6: Redundant HiProvision PCs with Dual Entry Point via Switch

11.9 Use Case 7: Redundant HiProvision PCs with Direct Dual Entry Point

Two redundant HiProvision PCs, each having 3 NICs are each directly connected via two management cables to a node with redundant CSMs. If an active CSM fails, the redundant CSM takes over to keep the connected node alive. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

- One IP address on three NICs in each HiProvision PC, see §2.1.3;
- Two redundant entry points on the MASTER HiProvision PC, see §2.5.2 and §2.5.5;

HiProvision connectivity is protected against:

- a HiProvision PC break, a connected node breakdown, a CSM failure or a single cable break somewhere between one HiProvision PC and the connected node. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

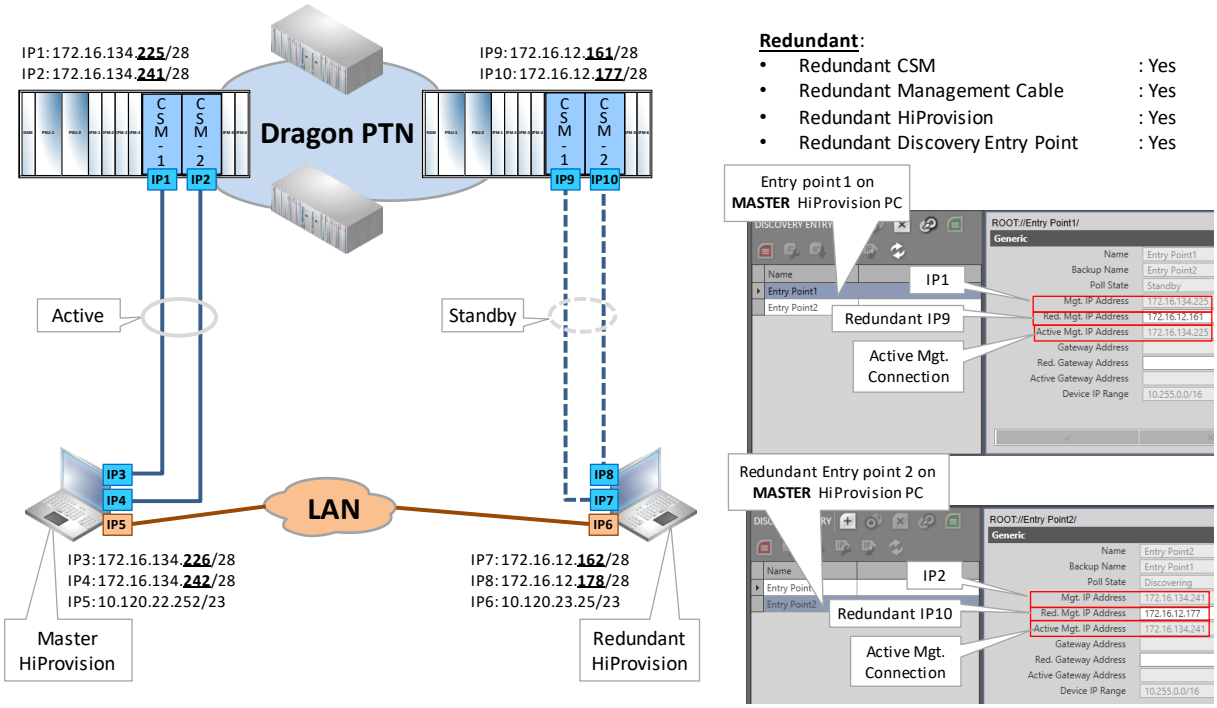


Figure 97 Use Case 7: Redundant HiProvision PCs with Direct Dual Entry Point

11.10 Use Case 8: One HiProvision PC with Dual Entry Point via Router

The HiProvision PC with 1 NIC, is directly connected via one management cable to a router. The router has a double connection to a node with redundant CSMs. If the active CSM fails, the redundant CSM takes over to keep the node alive.

Configuration:

- One IP address on one NIC in the HiProvision PC, see §2.1.3;
- Two redundant 'routed' entry points in HiProvision, see §2.5.2;
- Gateway configuration in the both the Redundant Entry Points;
- Gateway configuration in the CSM front IP Addresses;
- Static Routes on the router, see an example in §2.5.6e;

HiProvision connectivity is protected against:

- one CSM failure or single cable break between router and node.

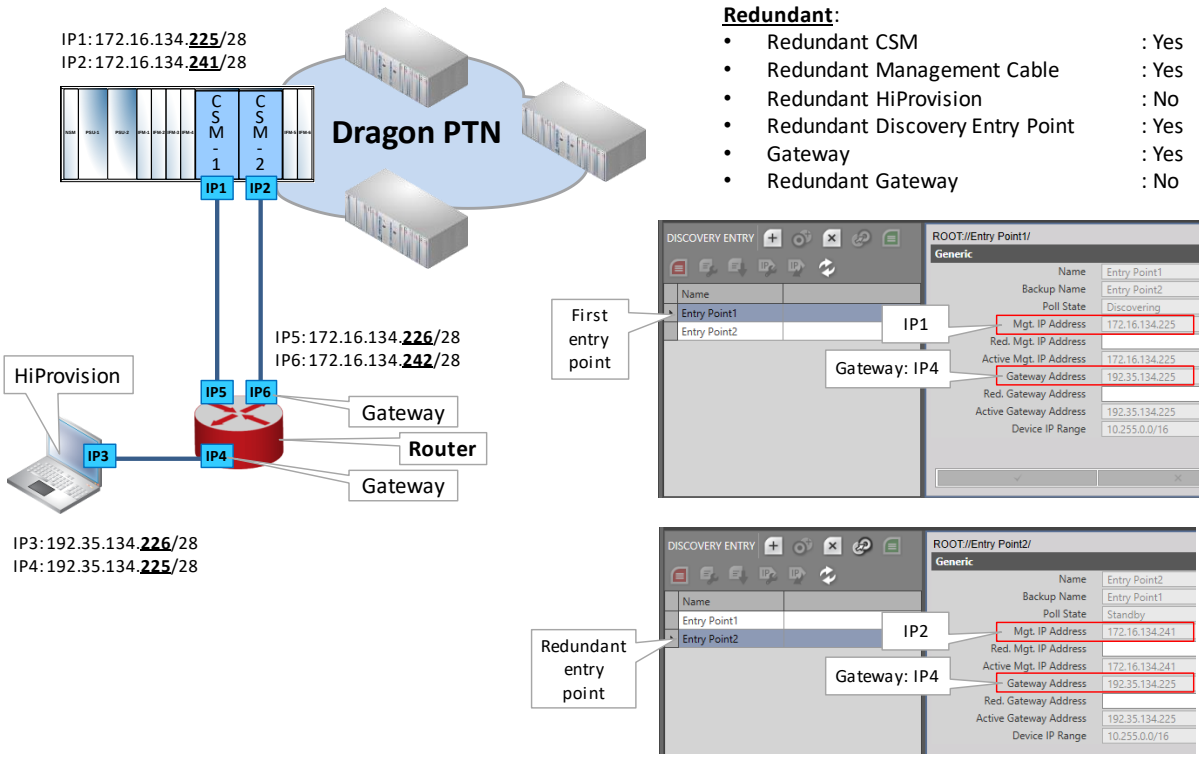


Figure 98 Use Case 8: One HiProvision PC with Dual Entry Point via Router

11.11 (Future) Use Case 9: Redundant HiProvision PCs with Dual Entry Point via Router

Two redundant HiProvision PCs, each having 2 NICs are each directly connected via one management cable to a router. Each router has a double connection to a node with redundant CSMs. If an active CSM fails, the redundant CSM takes over to keep the connected node alive. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

- One IP address on one NIC in each HiProvision PC, see §2.1.3;
- Two redundant 'routed' entry points in HiProvision, see §2.5.2;
- Gateway configuration in the both the Redundant Entry Points;
- Gateway configuration in the CSM front IP Addresses;
- Static Routes on the routers, see an example in §2.5.6e;

HiProvision connectivity is protected against:

- A HiProvision PC break, a connected node breakdown, a CSM failure or cable break somewhere between HiProvision PC and node. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

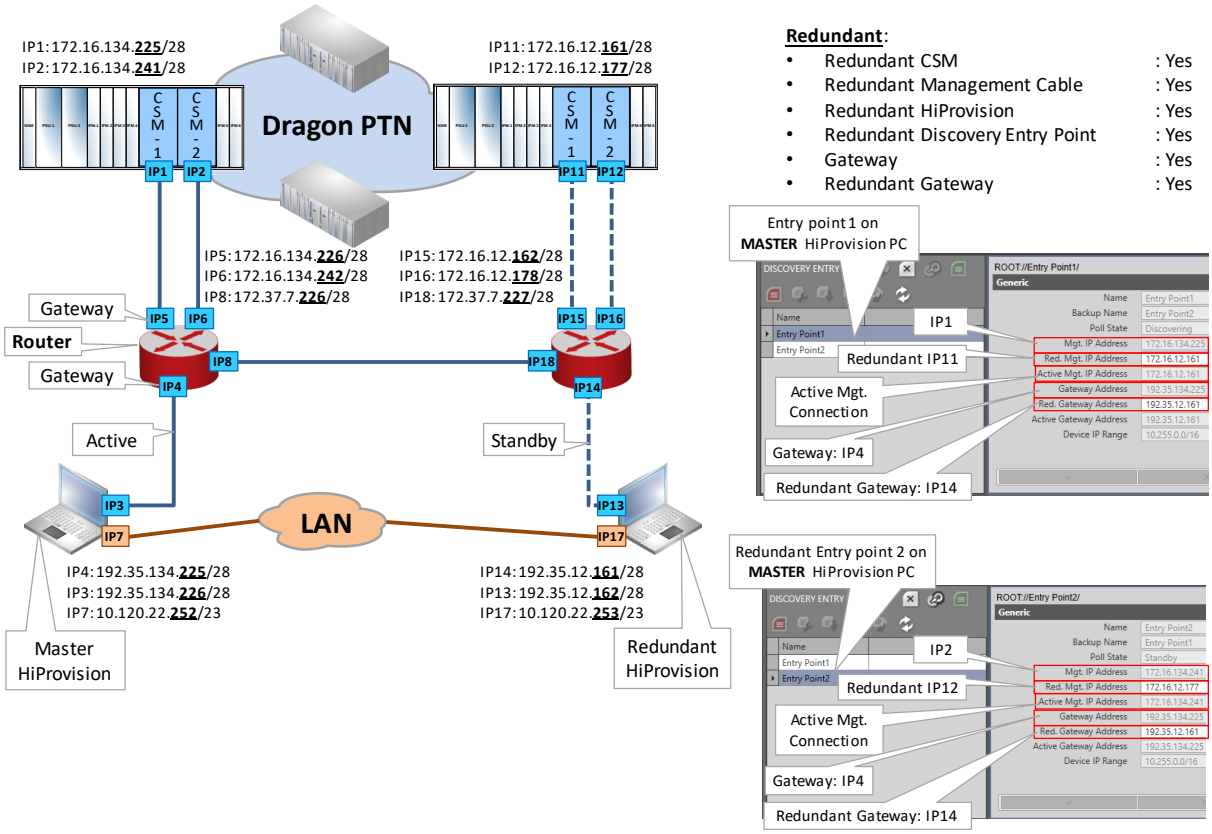


Figure 99 Use Case 9: Redundant HiProvision PCs / Dual Entry Point / Redundant Router

12. SOFTWARE/HARDWARE/FIRMWARE OF THE NETWORK ELEMENTS

12.1 General

Via HiProvision, it is possible to upgrade or downgrade software/firmware at once on multiple modules in the live network. The upgrade/downgrade process can be monitored by a progress bar per module.

It is also possible to list all the active and backup firmware versions on all the modules in the network. Furthermore, validation on this firmware version list can be done to make sure that all the same module types have the same firmware version. An alarm can be raised when firmware inconsistencies or incompatibilities occur.

CAUTION: To improve Dragon PTN security, as of Dragon PTN Release 3.1, only signed firmware
() can be loaded into the network. Signed firmware is firmware that has been factory encrypted with a special signature or certificate.

There are three upgrade procedures:

- Normal Upgrade (§12.3): Can be used for any module including redundant CMSs in one node.
- In Service Upgrade (§12.4): Can only be used for upgrades of redundant CSMs in one node. This is the advised way for redundant CSMs and has less downtime than the Normal Upgrade Procedure.
- Gradual Upgrade the network (§13): Upgrade one part of the network first, later on (days, weeks, …) upgrade the remaining part of the network. During this upgrade, both the current and new firmware versions run together in the same network.

Basically, following major steps are required in the entire process in HiProvision:

- Upgrade (wizard);
- Commit (wizard);
- Switchover (wizard), only for 'In Service Upgrade' procedure with redundant CSMs;
- Accept (wizard);
- Reload network configuration into the node after a CSM firmware update;

The general principle is as follows:

- All available firmware images are stored as an individual zip file in the folder 'C:\FtpRoot\Firmware'. An FTP server, running on the HiProvision PC, uses this folder as a source folder to transfer zip files to the node.

CAUTION: Make sure that a firewall on the HiProvision PC is totally switched off otherwise the FTP cannot send the software to the nodes!

- HiProvision can instruct the modules to fetch a new firmware image;

- Fetched firmware images will overwrite the current standby or backup firmware on the module. When the fetch is complete, a module will wait for a commit command from HiProvision before it will switch to its new firmware image;
- After receiving the commit command, the module will reboot with its new image. The module will wait for an additional accept command from HiProvision. When the accept command is not sent within 20 minutes, the module will automatically reboot and switch back to its previous image.
- For an overview or general example of a 'Normal Upgrade', see the example below:
  - Up till now, a module has two firmware versions onboard with v1.1.6 the active version (=A) and v1.1.5 the backup version (=B);
  - Upgrade: The operator wants to upgrade the module to signed firmware version v1.1.7. Via the upgrade wizard, the desired firmware version must be selected.
  - Upgrade: Only if the firmware is signed ( ), the upgrade wizard will overwrite the backup version v1.1.5 in the module with the new version v1.1.7.
  - Commit: Next, this new version must be committed via the commit wizard. It means that the module will reboot with the new version as the active version for the chosen module. The previous active version will now become the backup version.
  - Next, if the new version is accepted via the accept wizard within 20 minutes, the new version stays the active version. If it is not accepted within 20 minutes, the module reboots automatically and falls back to the previous active version v1.1.6 for this module;

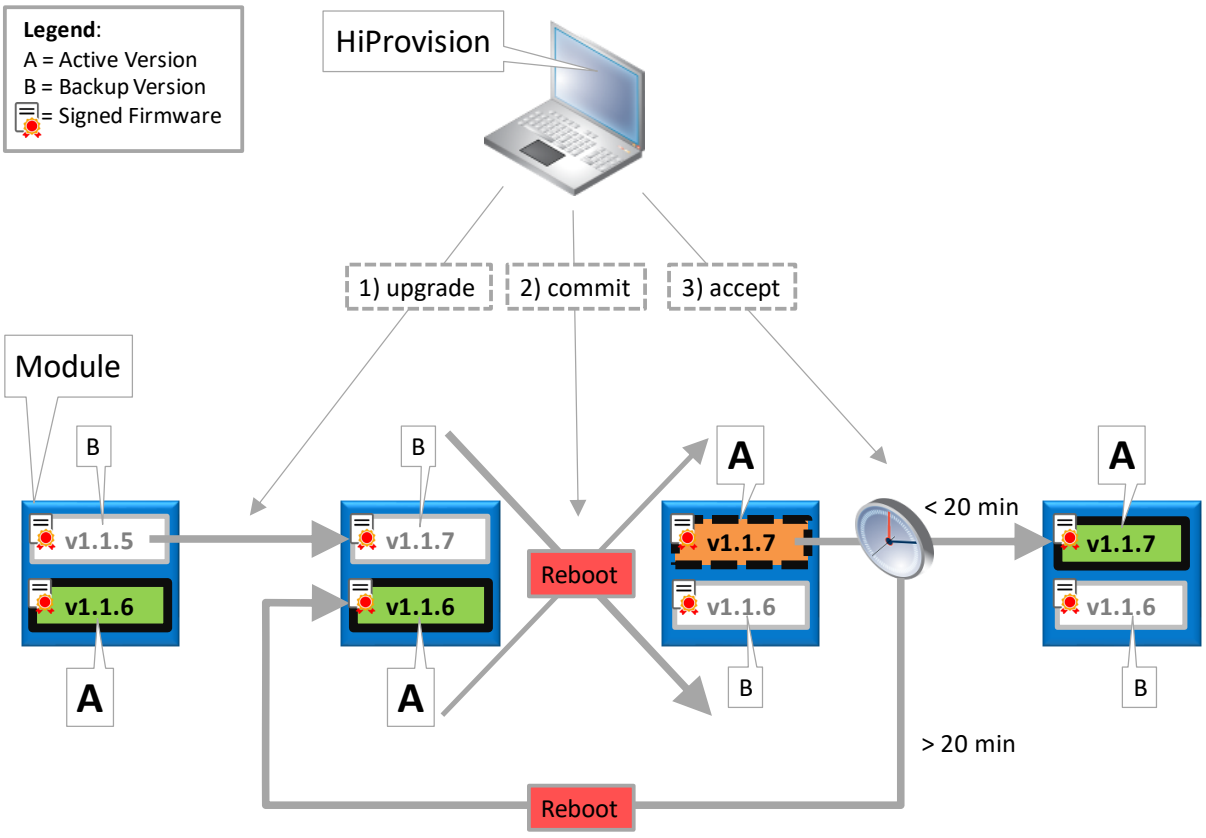


Figure 100 Normal Upgrade: Firmware Upgrade Example: Upgrade to v1.1.7

12.2 Firmware Upgrade

The firmware tools can be found via clicking the tile Dashboard → Tools → Software Tile. The screenshot below pops up. In the figure below, the most important buttons are indicated. The upgrading status can be followed in the column 'Upgrade Status'. The entire top menu, buttons and Upgrade Status is explained in the tables below.

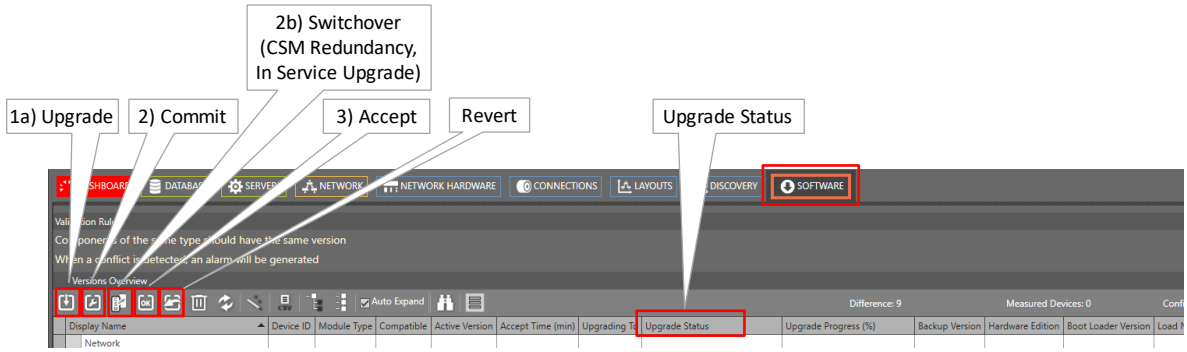
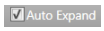


Figure 101 Software/Firmware Action Buttons

Table 17 Software/Firmware Buttons

Item	Short Description
	**Upgrade**: Starts a wizard to upgrade modules to a selected firmware image.
	**Commit**: Commits the pending upgrades, modules or nodes will swap to another image and will reboot.
	**Switchover (only In Service Upgrade, for redundant CSMs)**: Performs the switchover to make the Standby CSM the active one and vice versa. This switchover should be performed when the new firmware is already downloaded to both CSMs and committed. See §12.4.
	**Accept**: Accepts the committed upgrades, if not accepted in time, modules will switch back to their previous version.
	Reverts to the backup version. Clicking this button opens a wizard to let modules and/or nodes revert to their backup version. Selected modules/nodes in this wizard will reboot and start up with their backup version.
	Can be used to early interrupt and clear up an Upgrade or a Revert procedure. A reset causes the IFM or CSM to fall back to the original load from where the Upgrade or Revert was started. - IFM: can be resetted if its state is different from 'Wait for Accept' or 'No Upgrade Planned'; - CSM: can be resetted if its state is different from 'No Upgrade Planned';
	Refreshes all data.
 (future)	Starts a wizard to set the validation rules.
	Exports to a CSV file.
	Expands/Collapses all entries in the table.
	**Checked/Unchecked**: Auto expands/collapses new discovered devices in the table list.
	Search functionality to sort/group network elements in a better way. When using the search, the network elements are by default grouped by Module Type. In this way, you get a better overview to see if all the modules of a same type (e.g. CSM) have the same firmware version.
	Shows the allowed HiProvision firmware versions in your Network. Only firmware versions of products listed in this window will be verified by HiProvision. If a firmware in your network does not match the firmware in this

Item	Short Description
	list, a critical alarm will be shown in the Alarms Tile and configuration actions in your network will be limited! See also §13.8 and §13 for more information.
Device Count	**Difference**: Indicates the count difference between measured devices in the live network and configured devices in the HiProvision database. The difference should be 0 just to make sure that no device is forgotten when upgrading firmware! **Measured Devices**: Indicates how many devices are measured in the live network. **Configured Devices**: Indicates how many devices are configured in the HiProvision database.

Table 18 Upgrade Status Overview

Status	Description
Normal Upgrade (§12.3) / Normal Revert(§12.5)	
No Upgrade Planned	The module is not involved in an upgrade, commit or accept step. This status can turn in an 'Upgrading' status. It is also the new state of the module after accepting a committed upgrade.
Upgrading	The module is in the upgrade process, it means that at this moment, the backup firmware version is being overwritten by the new or target firmware version. This status will finally turn into the 'Wait for Commit' status.
Wait for Commit	The upgrade has been finished, the module is waiting for a commit to reboot and activate the new firmware version.
Rebooting	The module is rebooting due to a commit or not accepting within 20 minutes;
Wait for Accept	The module reboots after a commit and turns into a Wait for Accept status. You have 20 minutes to accept this new firmware version, otherwise the module will reboot automatically and fall back to its previous active version. The remaining accept time is shown in the field Accept Time (min).
Commit Failed or not accepted	You have not committed within the required 20 minutes or the commit has failed for some reason. As a result, a fall back occurs to its previous active version.
In Service Upgrade (§12.4) / In Service Revert (§12.6)	
In Service Wait for Commit (on active CSM)	The active CSM has performed an upgrade (upgrade wizard) and has been committed (commit wizard) with upgrade type 'In Service Upgrade'. As a result, the active CSM reboots the standby CSM and goes into the state 'In Service Wait for Commit'. The current active CSM is waiting to become the standby CSM with the new upgraded load as active load.
In Service Wait for Switchover (on standby CSM)	The Standby CSM is ready to become the active CSM (with the new upgraded load as active load) and is waiting for a switchover command.
In Service Wait for Accept	The standby CSM was in the state 'In Service Wait for Switchover' and performed a switchover via the Switchover wizard. At this time, the standby CSM has become the active one and vice versa. The new active CSM is waiting to be accepted.
In Service Wait for Revert (only in 'In Service Revert' Procedure)	The active CSM reverts the standby CSM and waits itself for further instructions.
In Service Load Install Failure	The In Service Upgrade or in Service Revert procedure has failed.

12.3 Normal Upgrade

12.3.1 Step 1: Upgrade

Purpose: Load a new firmware version into one or more modules in the network.

NOTE: Downgrade = upgrade to a lower version;

NOTE: For Redundant CSMs, this method is called the 'Normal Upgrade' procedure;

Click the upgrade button (see Figure 101) to start the upgrade wizard. The list below summarizes every page in the wizard:

- About: Click Next>>;
- Select Firmware Image: select Module Type and the Upgrade Version. The Upgrade Version drop-down list will read out the 'C:\FtpRoot\Firmware' folder.

NOTE: If you need a firmware version that is not available in this list, you might download a new version for a module from the Portal via https://hiprovision.hirschmann.com → Shortcuts → Downloads. Once you have the firmware image, save or copy the entire zip file in the 'C:\FtpRoot\Firmware'. Do not rename or unzip the file. Close and reopen the Upgrade wizard.

- Module Selection: by default, all the modules in the list are selected for an upgrade. To unselect one or more modules, select the module(s) in the list and click the unselect button  .
- Review: The selected modules will be shown: if ok, click Start Upgrade. The upgrade wizard closes and starts the upgrade process which can be followed by the upgrade status and upgrade process bar.

  NOTE: The firmware must be signed (). If the firmware is unsigned or incorrectly signed, the Upgrade step will fail. As a result, the firmware can not be downloaded into the network. Make sure to get the correct signed firmware!

- In the example below, the 16-E1-L module in Node1/Slot2 is upgraded from v1.0.13 to v1.0.14. It means that v1.0.14 will be initially stored as backup version on the module prior to activating it (= committing and accepting) to become the active version.

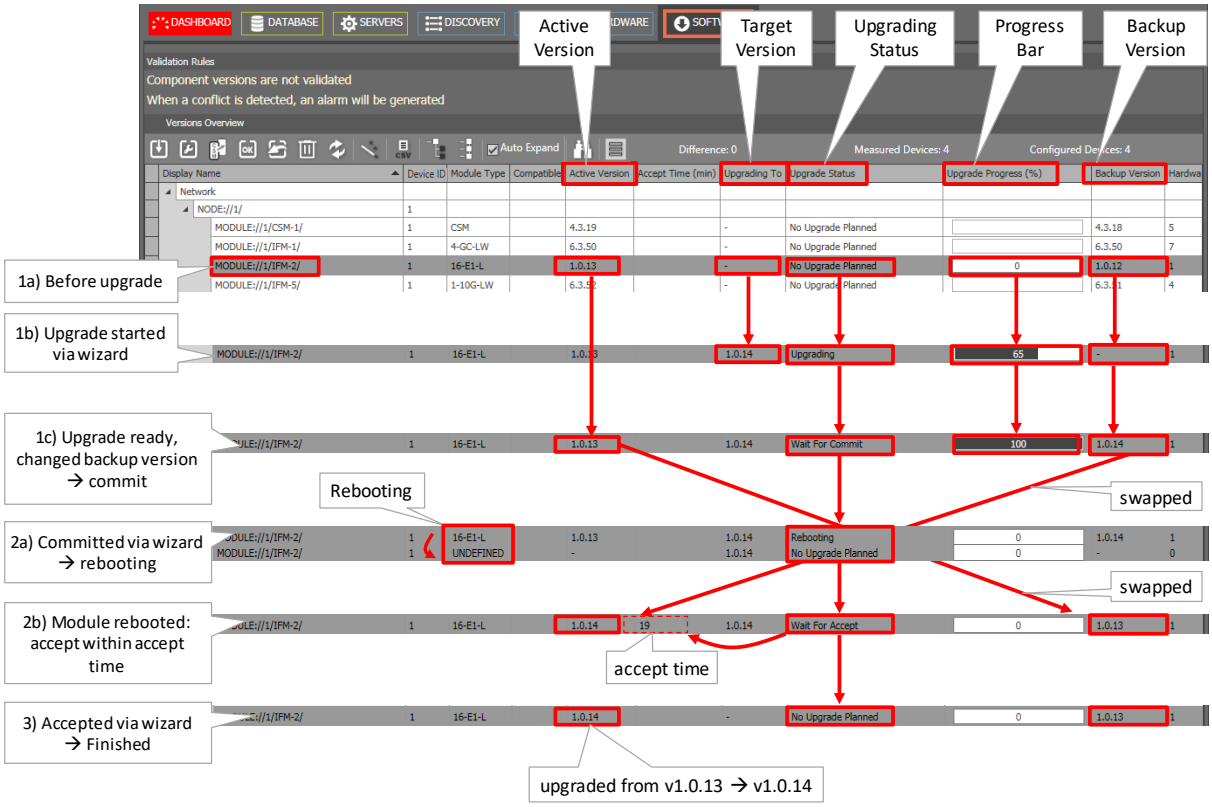


Figure 102 Step1: Upgrade Firmware

12.3.2 Step 2: Commit

Purpose: Swap to the new pending upgraded firmware version;

Click the commit button (see Figure 101) to start the commit wizard. The list below summarizes every page in the wizard:

- Info Page: Click Next>>;
- Module Selection:
  - by default, all the modules in the list are selected for a commit. To unselect one or more modules, select the module(s) in the list and click the unselect button .
  - Configuration action (only relevant for CSM firmware upgrades):
    - keep configuration (=default): The existing configuration on the CSM is kept, no extra (re)load of the configuration is necessary afterwards;
    - clear configuration: clears the CSM or node configuration, see §6.1;
    - reset configuration (only in Normal Upgrade procedure): resets the CSM or node configuration, see §6.2;
  - Upgrade Type: select 'Normal Upgrade'
    - Normal Upgrade (=default): select this value in the 'Normal Upgrade' procedure.
    - In Service Upgrade: this option is only visible for the active CSMs when redundant CSMs are being upgraded. Select this value only when you want to upgrade the redundant CSMs via the enhanced 'In Service Upgrade' procedure. More info on this feature and the Upgrade Type toggle button can be found in §12.4.

- Review: The selected modules will be shown: if ok, click Commit. The commit wizard closes and commits the selected pending upgrades. A reboot warning will pop-up, see figure below. Click Ok to continue;

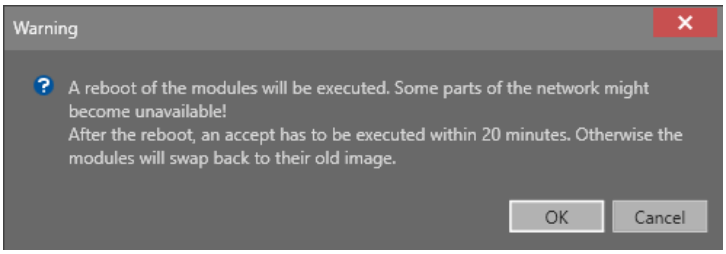


Figure 103 Commit Reboot Warning

- Result: commit was sent successfully, modules will reboot. Click Close;
- In the example below, after a commit, Node 1/slot2/16-E1-L is rebooting to swap the active and backup version. After the reboot, the status turns into 'Wait for Accept' and the backup version has become the active version and vice versa. The remaining accept time is shown in the field 'Accept Time' (min) and starts with 20 minutes.

NOTE: A 'wait for commit' never times out. If you have uploaded for example a wrong version, a rollback is not available but the 'Step1:Upgrade' must be executed again with the correct version.

Figure 104 Step 2: Commit Firmware

12.3.3 Step 3: Accept

Purpose: Accept the new activated firmware version to keep it active without falling back after 20 minutes to the previous active version;

Click the accept button (see Figure 101) to start the accept wizard. The list below summarizes every page in the wizard:

- About: Click Next>>;
- Module Selection: by default, all the modules in the list are selected for an accept. To unselect one or more modules, select the module(s) in the list and click the unselect button  .
- Review: The selected modules will be shown: if ok, click Accept. The accept wizard closes and accepts the committed upgrades.

- Result: accept was sent successfully, modules will not reboot after 20 minutes and will not fall back to the previous active version. Click Close;

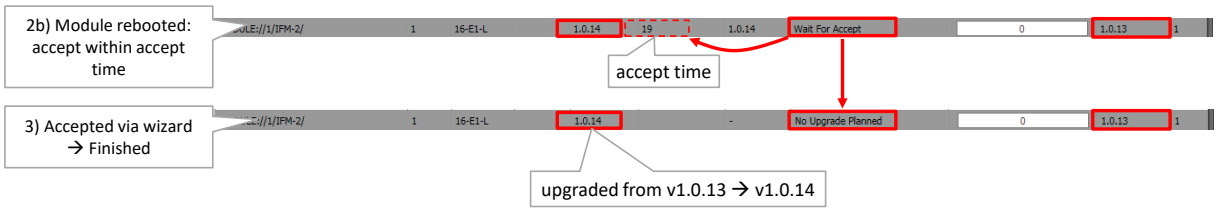


Figure 105 Step3: Accept Firmware

12.3.4 Step 4: Reload Network Configuration

Only perform this step when both conditions below are fulfilled:

- the CSM FW has been upgraded;
- In the Commit (wizard) phase, the 'Configuration action' for this CSM was set to:
  - Clear configuration;
  - Reset Configuration;

NOTE: To load the network configuration, see §7.

12.4 In Service Upgrade (Redundant CSMs Only)

The 'In Service Upgrade' procedure is an enhanced way to upgrade redundant CSMs. It takes less downtime than the normal upgrade procedure for redundant CSMs.

- In service upgrade: downtime is only a few seconds. As a result, running services in that node will only go out of service for a few seconds, actually it is only the switchover time from the standby ← → active CSM;
- Normal upgrade: downtime is a few minutes;

Prerequisites:

- both CSMs have the same active firmware version;
- both CSMs have the same backup firmware version;
- both CSMs must be in synchronization. It means that one CSM must be in the Active state, and the other one in the Standby state.

Suppose the general example scenario below:

- Node100/CSM-1 = Active (active FW version = A, backup FW version = B)
- Node100/CSM-2 = Standby (active FW version = A, backup FW version = B)
- Purpose: Hitless upgrade both the CSMs to FW version C:

Find below a summary of the steps, and a flow chart figure with the different commands and resulting 'Upgrade Status' for each step.

1. Upgrade CSM-1/2: download FW C to both CSMs;
2. Commit CSM-1: Commit active CSM-1 via upgrade type 'In Service Upgrade';

NOTE: The Upgrade Type toggle button in the commit wizard has only a meaning when upgrading Redundant CSMs. This button allows to set (or toggle) the Upgrade Type to 'In Service Upgrade' at once for multiple selected CSMs. Make sure to select first the desired CSMs via selecting the entire 'Upgrade Type' column (= all CSMs) or select some individual CSM records before clicking this toggle button.

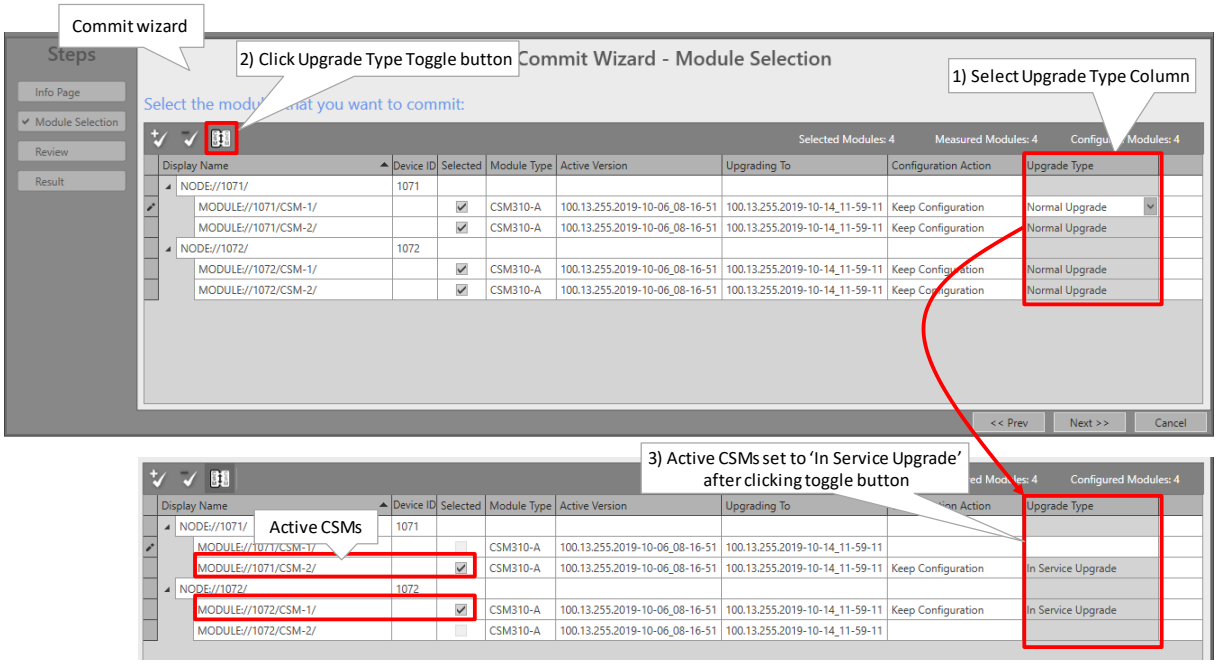


Figure 106 Commit Wizard: Use the Upgrade Type Toggle Button

3. (CSM-1 will automatically reboot CSM-2 via an internal commit);
4. CSM-2 reboots;
5. Perform a switchover. After the reboot of CSM-2, make the standby CSM-2 the active one (and CSM-1 the standby one) via the Switchover wizard. This wizard lists all the standby CSMs in the 'Wait for switchover' state. Select the standby CSM-2 that must become active.

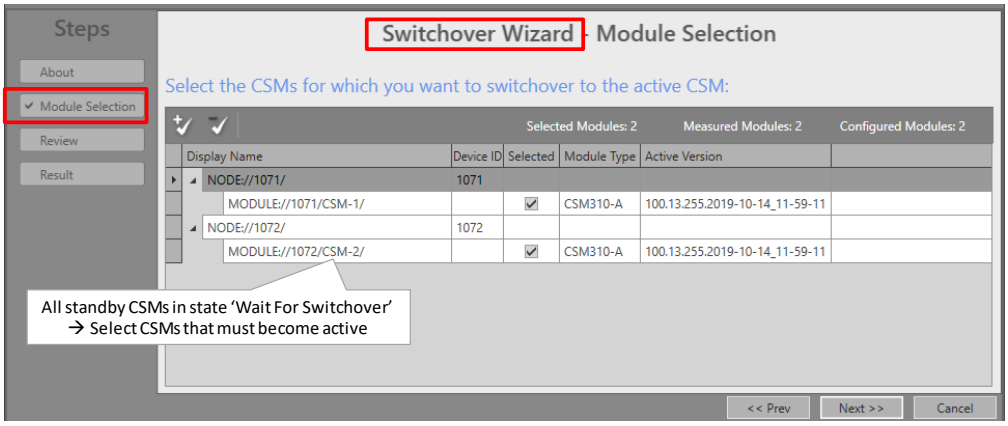


Figure 107 Switchover Wizard

6. CSM-2 becomes the active CSM, with the new active load FW version C;
7. Accept CSM-2;
8. (CSM-1 reboots);
9. (CSM-1 receives an internal Accept);
10. Both CSMs are ready and up and running, CSM-2 = active, CSM-1 = standby, both CSMs have load FW C as active load.

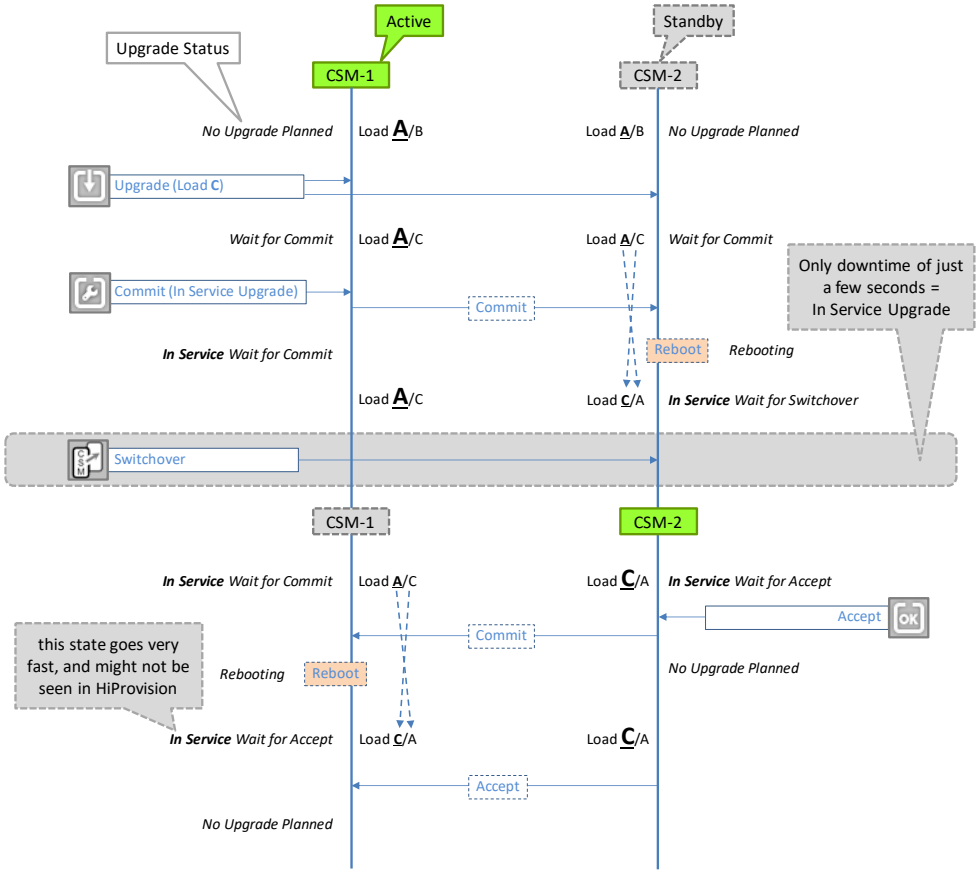


Figure 108 In Service Upgrade: Flow Chart with State Indications

12.5 Normal Revert to Backup

Purpose: Revert or fall back to the backup version.

CAUTION: 'Revert to Backup' on a CSM or IFM reverts only the firmware version. The configuration data on the other hand will be cleared and must be loaded again into the network.

Click the revert button (see Figure 101) to start the 'Revert to backup version' wizard. The list below summarizes every page in the wizard:

- About: Click Next>>;
- Module Selection: Select the modules via clicking the Selected checkbox. To unselect one or more modules, select the module(s) in the list and click the unselect button .
  - Revert Type: select 'Normal Revert'
    - Normal Revert (=default): select this value in the 'Normal Revert' procedure.

- In Service Revert: select this value in the 'In Service Revert' procedure, see §12.6.

NOTE: The Revert Type toggle button must only be used when using the 'In Service Revert' procedure with Redundant CSMs, see §12.6.

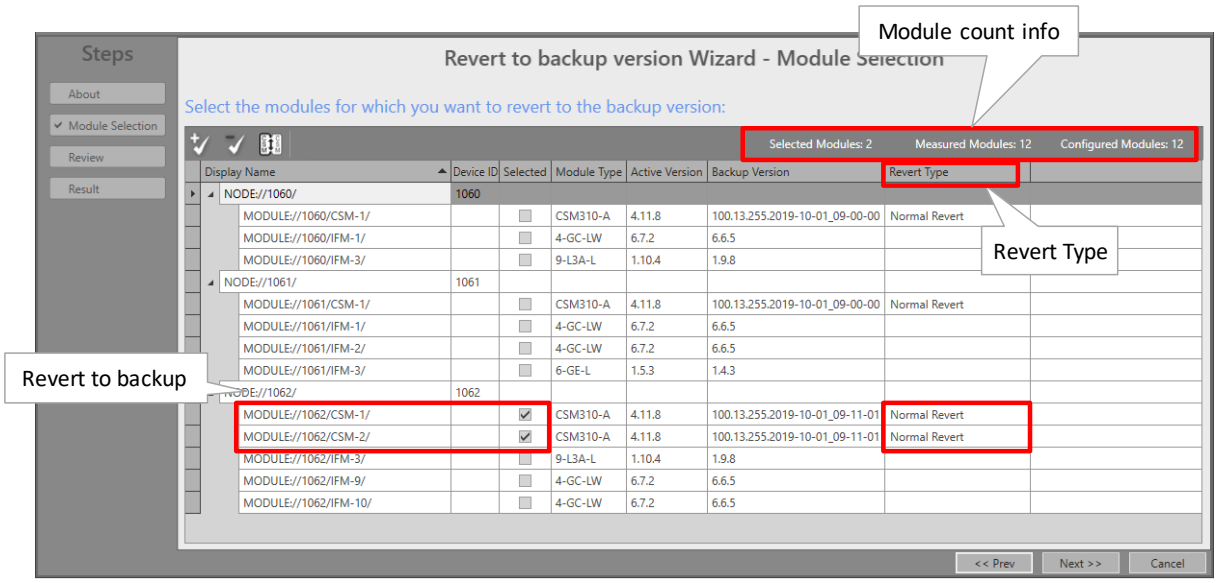


Figure 109 Revert to Backup Version

- Review: The selected modules will be shown: if ok, click Revert To Backup Version. A revert command will be sent to the network to initiate the revert action;
- Result: Revert command was successfully sent, the revert action has been started and the progress for each selected module can be followed in the versions overview list in the Software tab. Click the Close button to close the wizard. In the version overview list, press the refresh button from time to time, for faster progress feedback.

12.6 In Service Revert to Backup (Redundant CSMs Only)

Purpose: Revert or fall back to the backup version e.g. when something went wrong during the loading of a new firmware version.

CAUTION: 'Revert to Backup' on a CSM reverts only the firmware version. The configuration data on the other hand will be cleared and must be loaded again into the network.

The 'In Service Revert' procedure is an enhanced way to revert Redundant CSMs from the active load to the backup load, and make the backup load again the active one. It is more performant and takes less downtime than the normal revert procedure.

- In Service Revert: downtime is only a few seconds = the time to switch over Active←→ Standby CSM;
- Normal Revert: downtime is a few minutes;

Prerequisites:

- both CSMs have the same active firmware version;

- both CSMs have the same backup firmware version;
- both CSMs must be in synchronisation. It means that one CSM must be in the Active state, and the other one in the Standby state.

Suppose the general example scenario below:

- Node100/CSM-1 = Active (active FW version = C, backup FW version = A)
- Node100/CSM-2 = Standby (active FW version = C, backup FW version = A)
- Purpose: Hitless revert both the CSMs to backup FW version A

Find below a summary of the steps, and a flow chart figure with the different commands and resulting 'Upgrade Status' for each step.

1. Revert: Revert active CSM-1 via upgrade type 'In Service Upgrade';

   NOTE: The Revert Type toggle button in the Revert wizard has only a meaning when reverting Redundant CSMs. This button allows to set (or toggle) the Revert Type to 'In Service Revert' at once active CSMs that have a standby CSM. Make sure to select all records via selecting a row + CTRL + A (= all records) or select some individual CSM records before clicking this toggle button. After setting to 'In Service Revert', select the 'Selected' checkbox for the CSMs that must be reverted. You could also use the filter (right-click Display Name header cell → Filter Editor) to filter out the CSMs first.

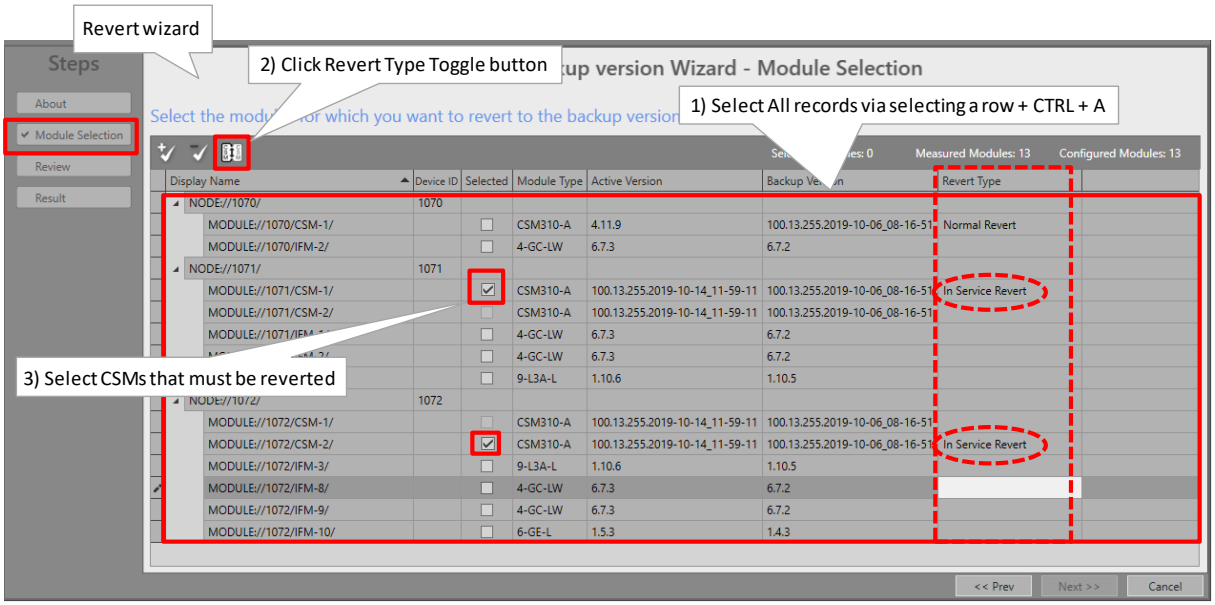


Figure 110 Revert Wizard: In Service Revert

2. (CSM-1 will automatically reboot CSM-2 via an internal commit);
3. CSM-2 reboots;
4. After CSM-2 reboot, perform a switchover via the Switchover wizard. Select Standby CSMs that must become active (=CSMs in the state 'Wait for switchover'). This wizard lists all the CSMs in the 'Wait for switchover' state;
5. CSM-2 becomes the active CSM with FW version A as active load;
6. Accept CSM-2;
7. (CSM-1 reboots);

8. CSM-1 receives an internal Accept;
9. Both CSMs are ready and up and running, CSM-2 = active, CSM-1 = standby, both CSMs have load FW A as active load.

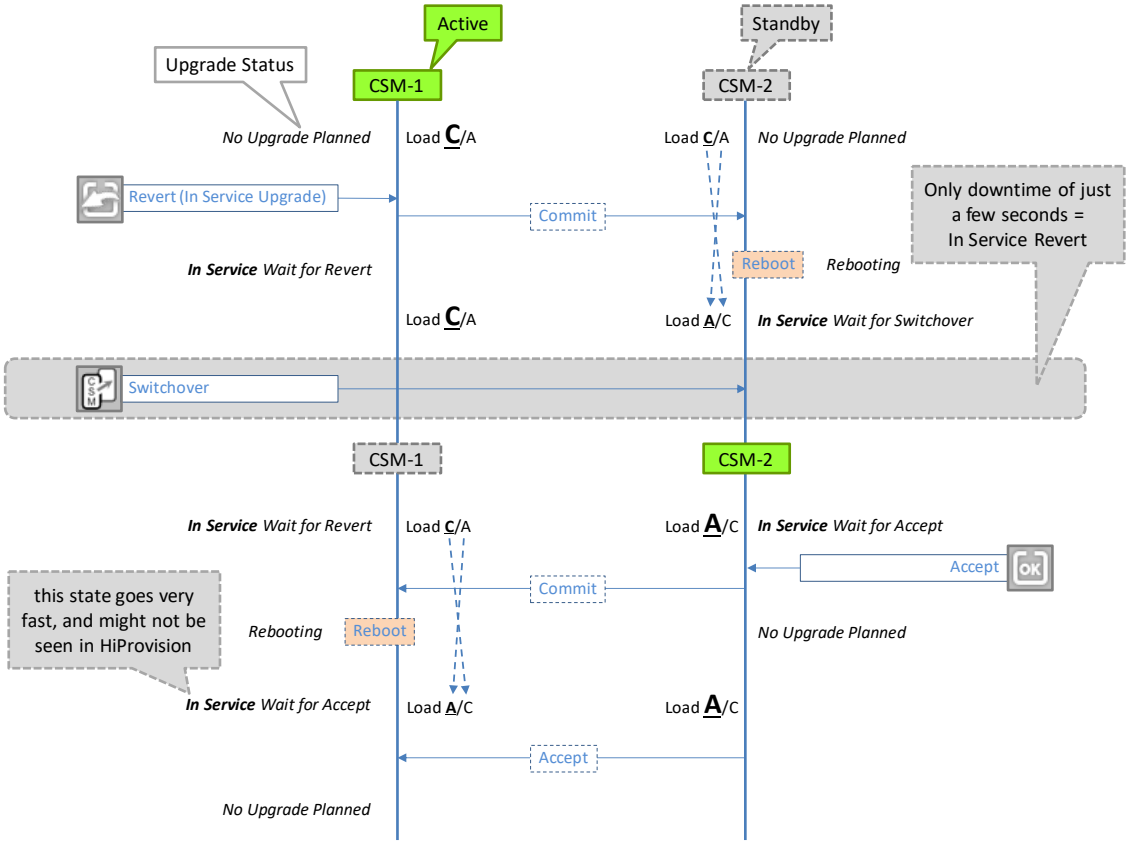


Figure 111 In Service Revert: Flow Chart with State Indications

12.7 Validation Rules (Future)

It is possible to validate if all the modules of the same type have the same firmware version. Click the validation rules button  in Figure 101. A window pops up, select 'Make sure…'.

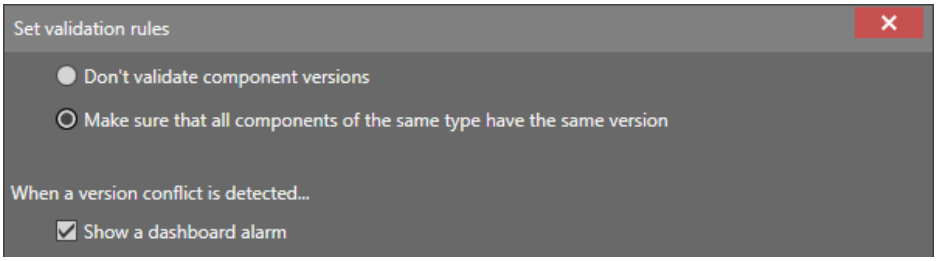


Figure 112 Firmware Validation Rules

After clicking OK in this window, the validation starts immediately. The results of the validation will appear in the compatible column.

When alarming is activated in the figure above, alarms will be generated as well when incompatible versions are detected, see figure below. Incompatibilities can be solved by upgrading or downgrading firmware versions as described in the paragraphs before.

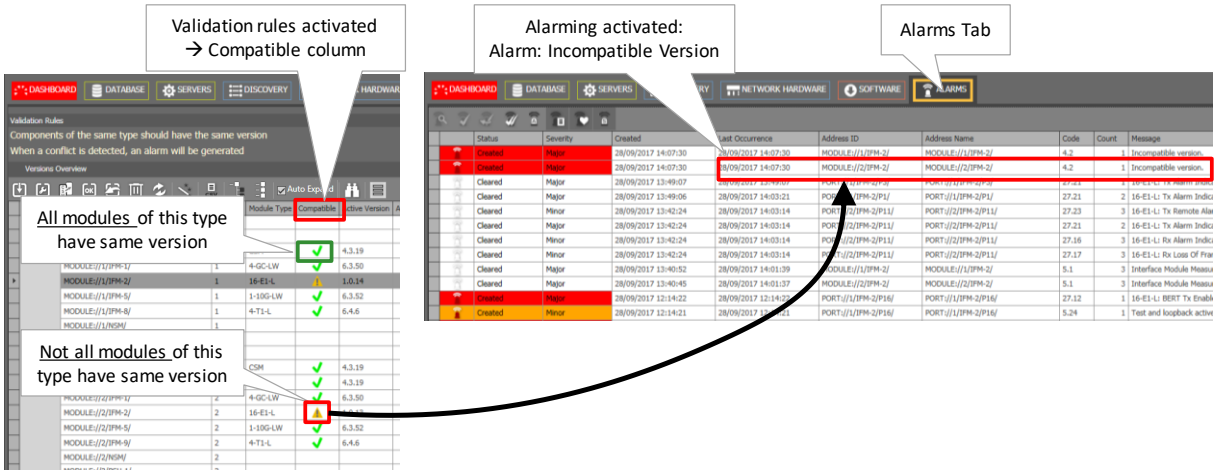


Figure 113 (In)Compatible Firmware Versions and Alarming

12.8 Reporting

Reporting information is available via the Reporting Engine Add-on, see §17.4.

12.9 Hardware Edition of Dragon PTN Modules

The hardware edition of the Dragon PTN modules has been factory set and cannot be changed. It can be read out via the Dashboard → Software tile → Hardware Edition, see figure below.

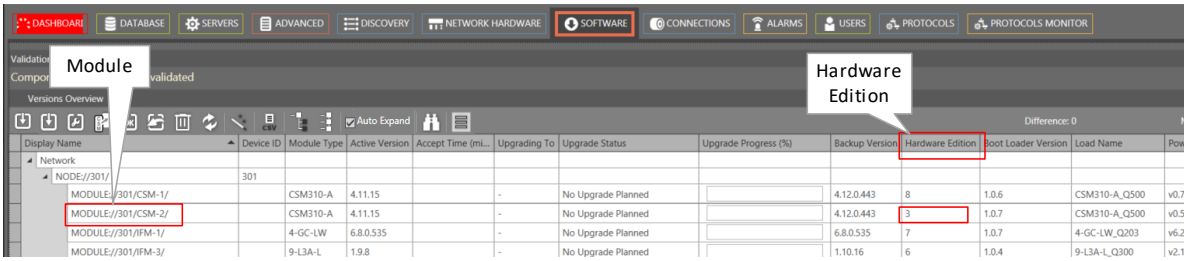


Figure 114 Hardware Edition of Dragon PTN Modules

13. GRADUAL UPGRADE OF THE NETWORK (MIXED NETWORKS)

13.1 General

CAUTION: This is an expert feature! It must only be used temporary during the upgrade phase of your network. Each HiProvision PC can fully monitor its own connected network part, but has limited configurations actions in it.

Prerequisites:

- Two HiProvision PCs are required;
- When two HiProvision PCs are already available due to HiProvision redundancy, the HiProvision redundancy feature must be turned off during this upgrade;

In a Dragon PTN network, it is possible to gradually upgrade the HiProvision version and CSM firmware in your network from e.g. v1 up to v2. It means that you can first upgrade one part of the network while leaving the other part of the network untouched up and running. So during the gradual upgrade, your network will have both v1 and v2 running together in the same network (=mixed network). This is possible because the network will be logically separated into two network parts. In this way, it allows to test the v2 for a while on just a small part of your network, or do the upgrade step by step making sure not to bring down the entire network at once. Once the upgrade in the first part has been finished, the remaining part of your network can be upgraded to e.g. v2.

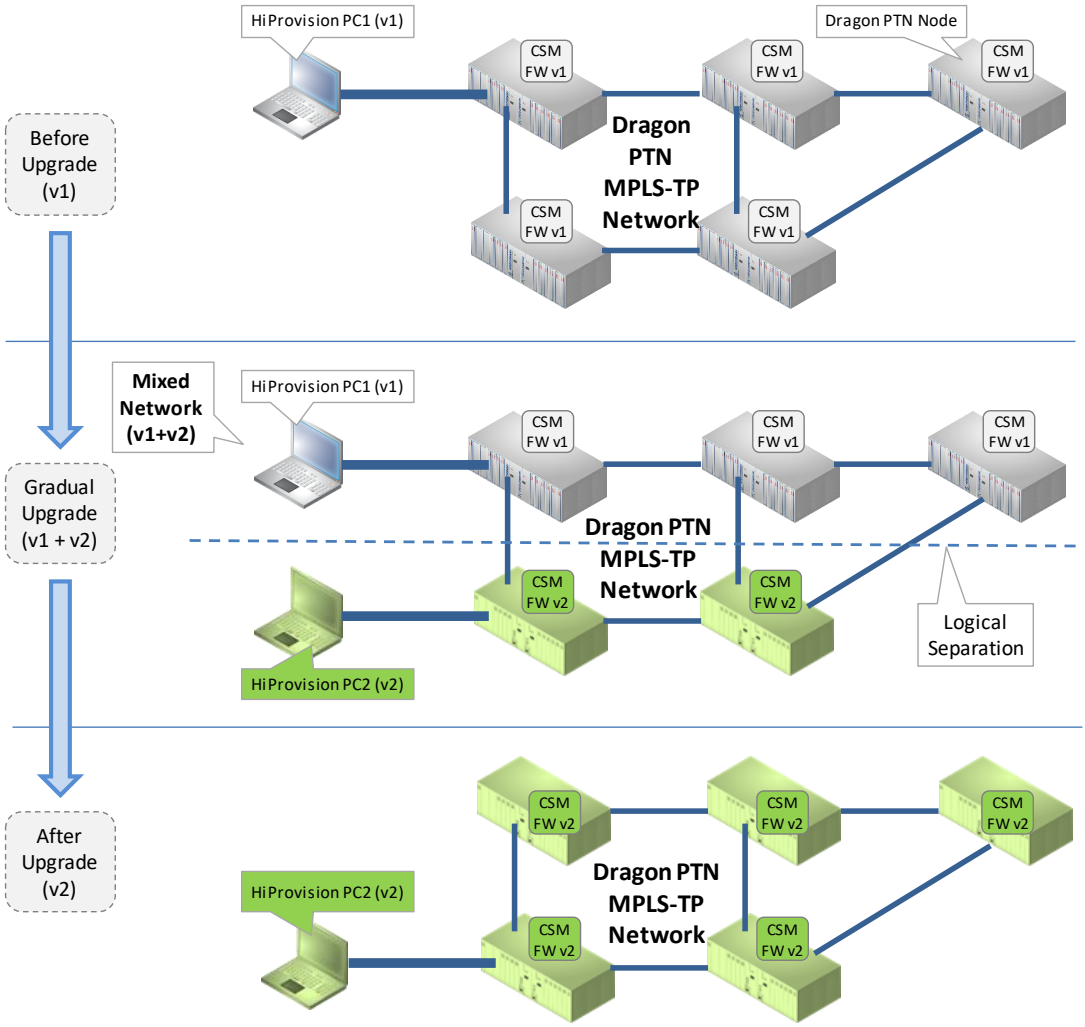


Figure 115 Gradual Upgrade the Dragon PTN Network

13.2 Configuration: Gradual Upgrade the Network

13.2.1 Use Case1: Network without Redundant HiProvision PC

An example network is shown in the figure below: HiProvision PC1 is running HiProvision version1 (v1) and the CSMs have firmware version1 (v1):

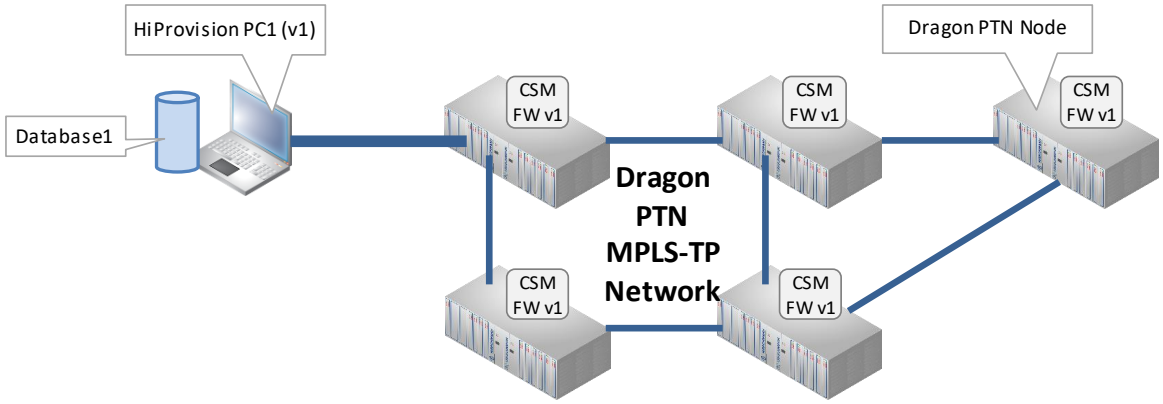


Figure 116 Use Case1: Example Network

Follow the steps below to set up a mixed network:

1. Install a second HiProvision PC2 with a new HiProvision version (v2) different from HiProvision PC1 (v1). Reuse the same serialkey and license pack (*.dat file) from the HiProvision PC1;
2. On HiProvision PC2: follow 'Steps for a Basic Setup' (§2), connect this PC to the Dragon PTN network;

   NOTE: PC2 can be connected to any node in the entire network regardless the installed firwmware versions on the node.

3. On HiProvision PC1: Make a backup of the database. Export this database onto a USB stick.
4. On HiProvision PC2: Import this database from the USB stick, restore and activate the database. See §Table 13 how to perform database handlings;
5. On HiProvision PC2: Start the servers after restoring and activating the database;

CAUTION: No database syncing between two HiProvision PCs! It is advised to do as little configurations actions as possible on each HiProvision to keep both databases as similar as possible.

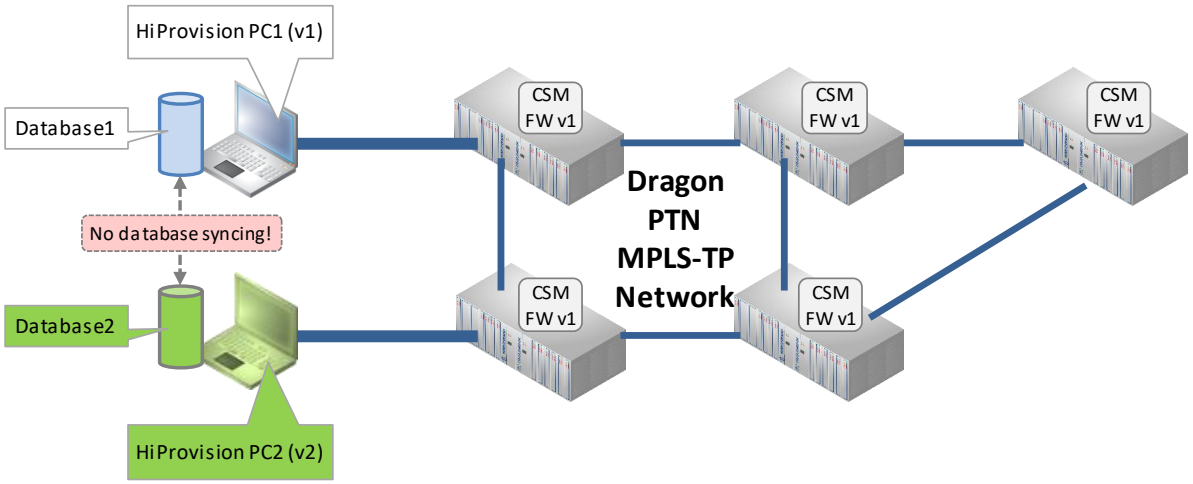


Figure 117 Use Case1: Connect HiProvision PC2

6. On HiProvision PC2: Load the new CSM firmware v2, different from CSM firmware v1 into some nodes. This load action causes the network to logically split into two parts: Network Part1 and Network Part2. A split means that nodes with CSM FW v1 are only reachable for HiProvision PC1 and nodes with CSM FW v2 are only reachable for HiProvision PC2.

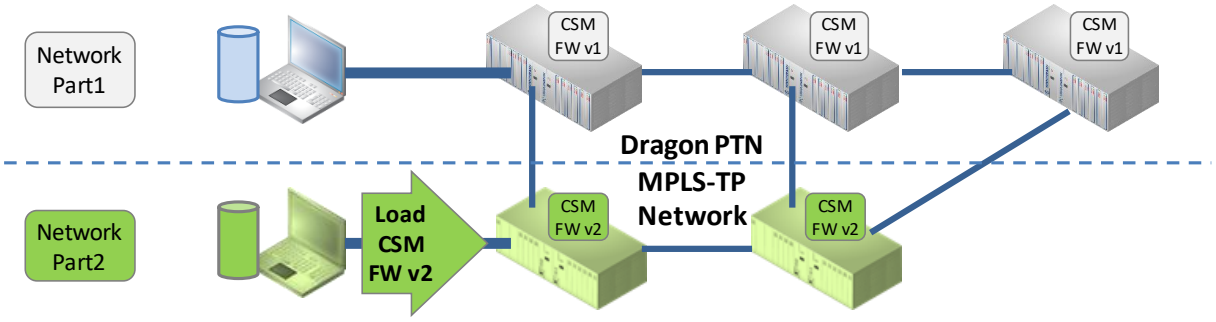


Figure 118 Use Case1: Load CSM FW v2

7. Due to this load action, critical alarms 'Node is blocked, incompatible FW version(s) detected' wil be raised in both HiProvision PC1 and HiProvision PC2:
   - In HiProvision PC1 for the nodes in Network Part2, because these nodes have an invalid firmware for HiProvision PC1;
   - In HiProvision PC2 for the nodes in Network Part1, because these nodes have an invalid firmware for HiProvision PC2;

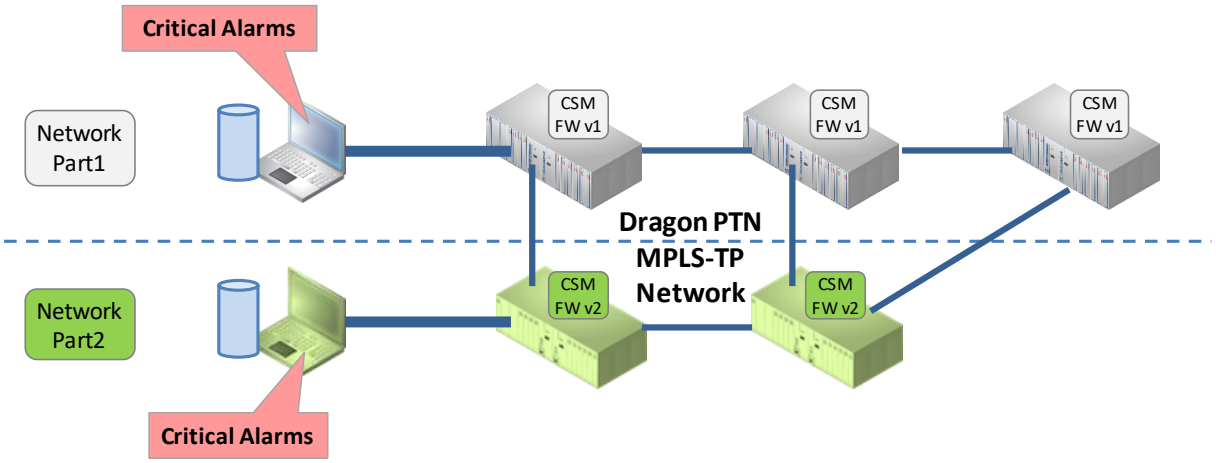


Figure 119 Crital Alarms Raised in both HiProvision PCs

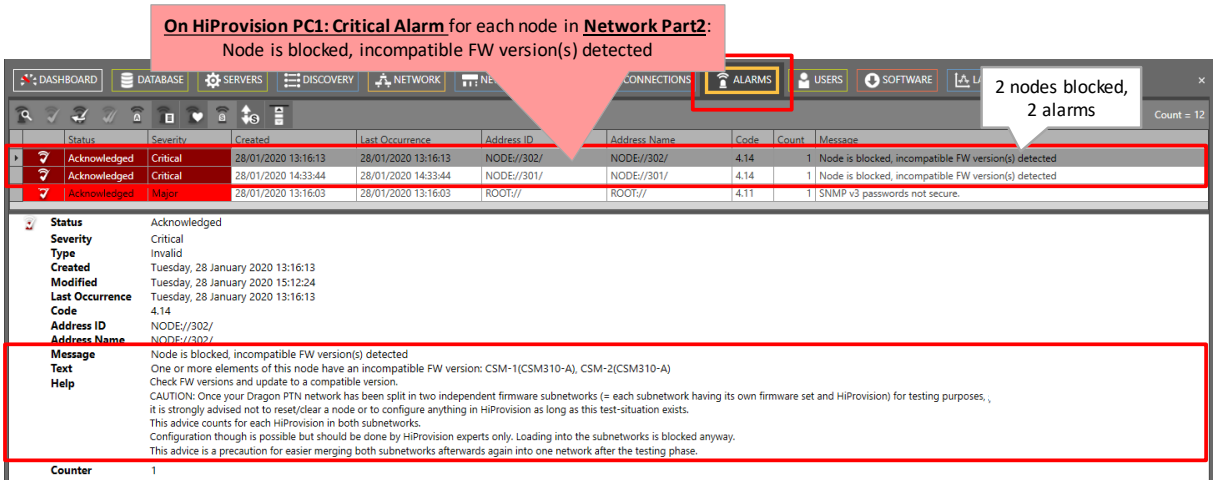


Figure 120 Critical Alarms on HiProvision PC1

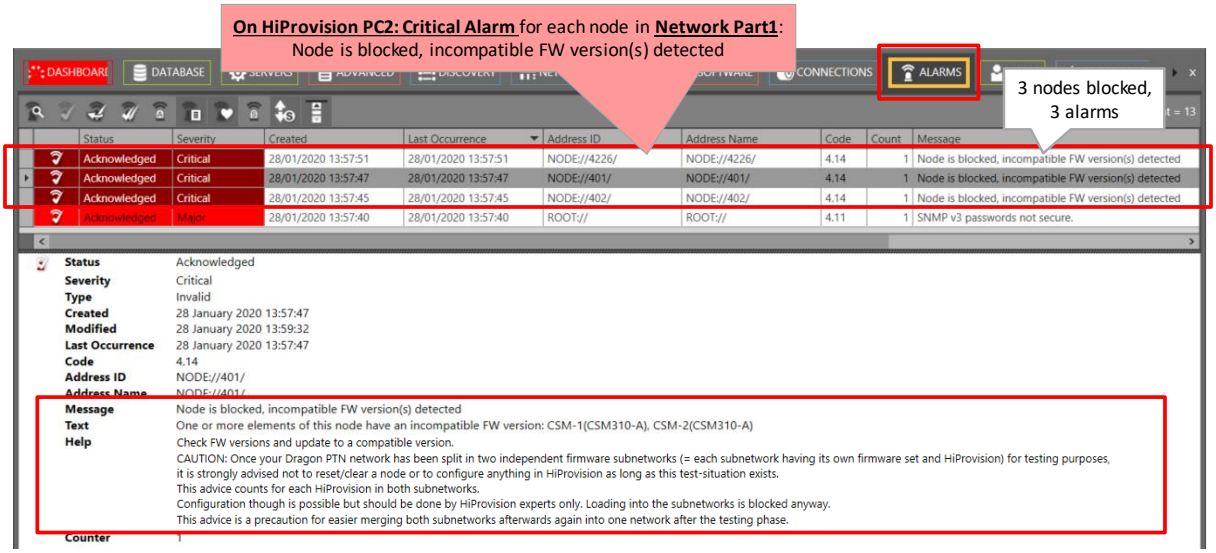


Figure 121 Critical Alarms on HiProvision PC2

8. This mixed network state should be temporary. Each HiProvision PC can fully monitor its own connected network part, but has limited configurations actions in it. The network is logically separated into two parts. Nodes in Network Part2 are unreachable for HiProvision PC1 and nodes in Network Part1 are unreachable for HiProvision PC2.

CAUTION:
- the entire network remains reachable in both HiProvision PCs for DCN (§13.4) and firmware uploading (§13.5)
- load configurations into the network are very limited (§13.6)!

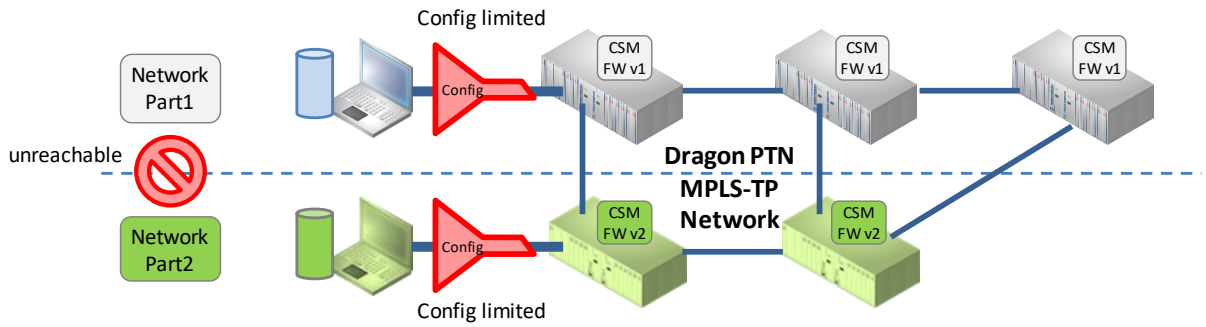


Figure 122 Unreachability, Configuration Actions Limited

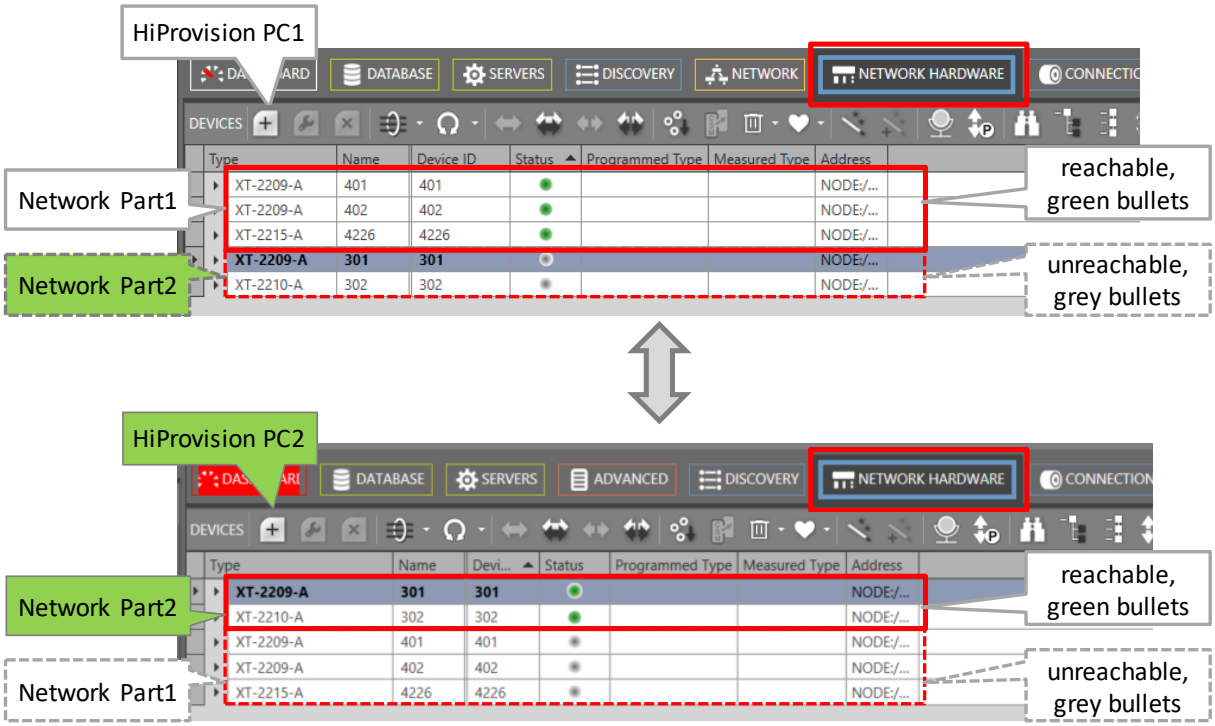


Figure 123 Unreachability per HiProvision PC

9. If the upgrade in one part of the network is finished and tested, you can either upgrade the entire network or just go back to the old version, see §13.3.

13.2.2 Use Case2: Network with Redundant HiProvision PCs

This case is very similar to Use Case 1 but the HiProvision PC2 is already available now, installed up and running. And also the database on HiProvision PC2 is already the same and in sync with the database on HiProvision PC1. Follow the actions below:

1. Stop the HiProvision redundancy on the master PC (e.g. HiProvision PC1) via the Dashboard → Servers Tile → Click ;

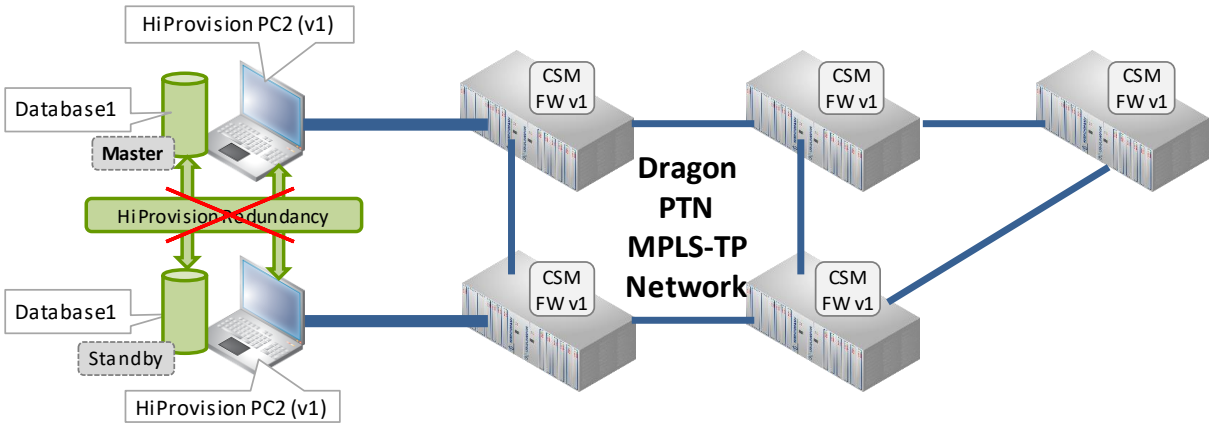


Figure 124 Stop HiProvision Redundancy

2. Install a new HiProvision v2 on the standby PC (e.g. HiProvision PC2).
3. Go to Use Case1 (§13.2.1) and skip steps 1→4 and continue with step 5.

13.3 Leave the Mixed Network, Finish the Gradual Upgrade

Your mixed network could be intended (via the Gradual Upgrade configuration steps) or accidental (via uploading a wrong firmware version or by installing a CSM with a wrong firmware version).

- Two options to leave an intended mixed network:
  - Go back to the old firmware version (v1) → §13.3.1
  - Upgrade the entire network to the new firmware version (v2) → §13.3.2
- Solve an accidental mixed network → §13.3.3

13.3.1 Intended Mixed Network: Go Back to Old Firmware Versions (v1)

If you decide after a while (hours, days, …) to leave the mixed network and go back to a network with only v1 again, follow the steps below:

1. The database on HiProvision PC1 is considered as the most accurate database out of the two databases. No further database actions needed, database already OK;
2. On HiProvision PC1: Load the old CSM firmware v1 into all the nodes of Network Part2;
3. As a result:
   - the critical alarms on HiProvision PC1 disappear immediately;
   - the entire network runs back in the old firmware v1;
   - full configuration is possible again (via HiProvision PC1) in the entire network;
4. Was HiProvision Redundancy active before?:
   - No: Disconnect HiProvision PC2 from the Dragon PTN network;
   - Yes:
     - Shutdown HiProvision v2 on HiProvision PC2 and start up HiProvision v1 again on that PC.

- Leave HiProvision PC2 connected and start HiProvision Redundancy on HiProvision PC1 again via Dashboard → Servers Tile → Click  . HiProvision PC1 remains the old master.

CAUTION: When activating HiProvision Redundancy again, make sure to activate it on the correct PC. That PC including its database will be used as master. The database on the other standby PC will be lost due to HiProvision Redundancy.

13.3.2 Intended Mixed Network: Upgrade Entire Network to New Version (v2)

If you decide after a while (hours, days, …) to leave the mixed network and progress to a network with only the new v2, follow the steps below:

1. The database on HiProvision PC1 is considered as the most accurate database out of the two databases. Export this database from HiProvision PC1 and import it on the HiProvision PC2;
2. On HiProvision PC2: Load the new CSM firmware v2 into all the nodes of Network Part1;
3. As a result:
   - the critical alarms in HiProvision PC2 disappear immediately;
   - the entire network runs in the new firmware v2;
   - full configuration is possible again (via HiProvision PC2) in the entire network;
4. Was HiProvision Redundancy active before?:
   - No: Disconnect HiProvision PC1 from the Dragon PTN network;
   - Yes:
     - Shutdown HiProvision v1 on HiProvision PC1;
     - Install a new HiProvision v2 on HiProvision PC1, so that both PCs are running HiProvision v2;
     - Start up HiProvision v2 on HiProvision PC1 with the correct database;
     - Leave HiProvision PC2 connected and start HiProvision Redundancy on HiProvision PC2 via Dashboard → Servers Tile → Click  . HiProvision PC2 will be the new master.

13.3.3 Solve an Accidental Mixed Network

The critical alarms indicate nodes with a wrong CSM firmware version. There are two options to solve this:

- Replace the erroneous CSM with a CSM having an allowed CSM firmware version (§13.6);
- Load an allowed CSM firmware version into the erroneous CSMs;

After these actions, the critical alarms just disappear automatically and full configuration is possible again over the entire network.

13.4 Discovery Tile: Entire Network Reachable for Discovery (DCN)

For monitoring and configuration, both network parts are unreachable to each other. But for DCN in the Discovery Tile, the entire network (Network Part1 + Network Part2) remains reachable. So the entire network is always measured in both HiProvision PCs. Both HiProvision PCs always know the entire network.

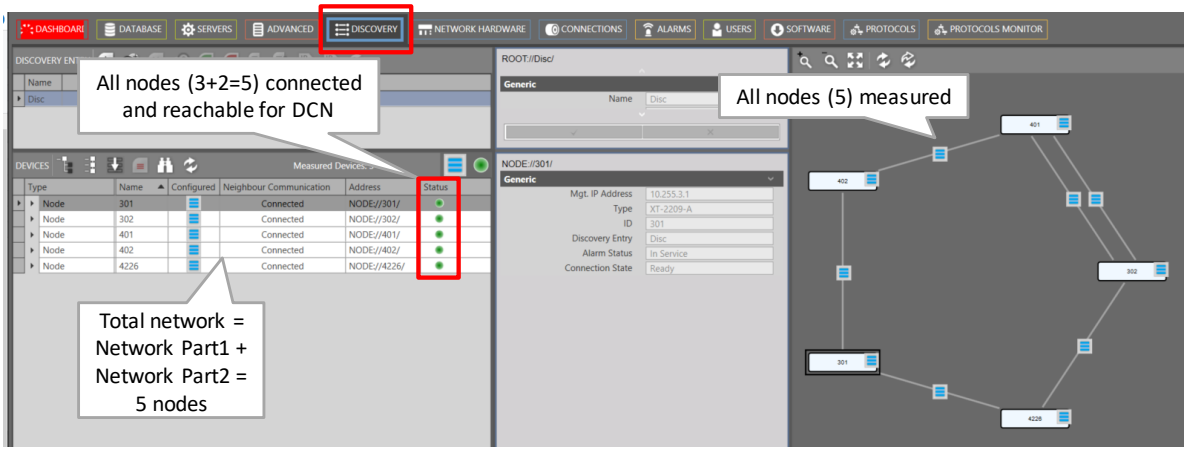


Figure 125 Discovery Tile: Entire Network Reachable for DCN

13.5 Software Tile: Create/Remove the Split in the Network via Firmware Uploading

The entire network (Network Part1 + Network Part2) remains reachable for the Software tile. As a result, both HiProvision PCs can upload new firmware to any node in the entire network at any time.

- Create a split in the network: one of both HiProvision PCs must upload new CSM firmware that is not allowed in the other HiProvision PC.
- Remove a split in the network: one of both HiProvision PCs must upload new CSM firmware that is allowed by both HiProvision PCs. If all the nodes in the network have the same CSM firmware, the network split will be removed, and full configuration is possible again.

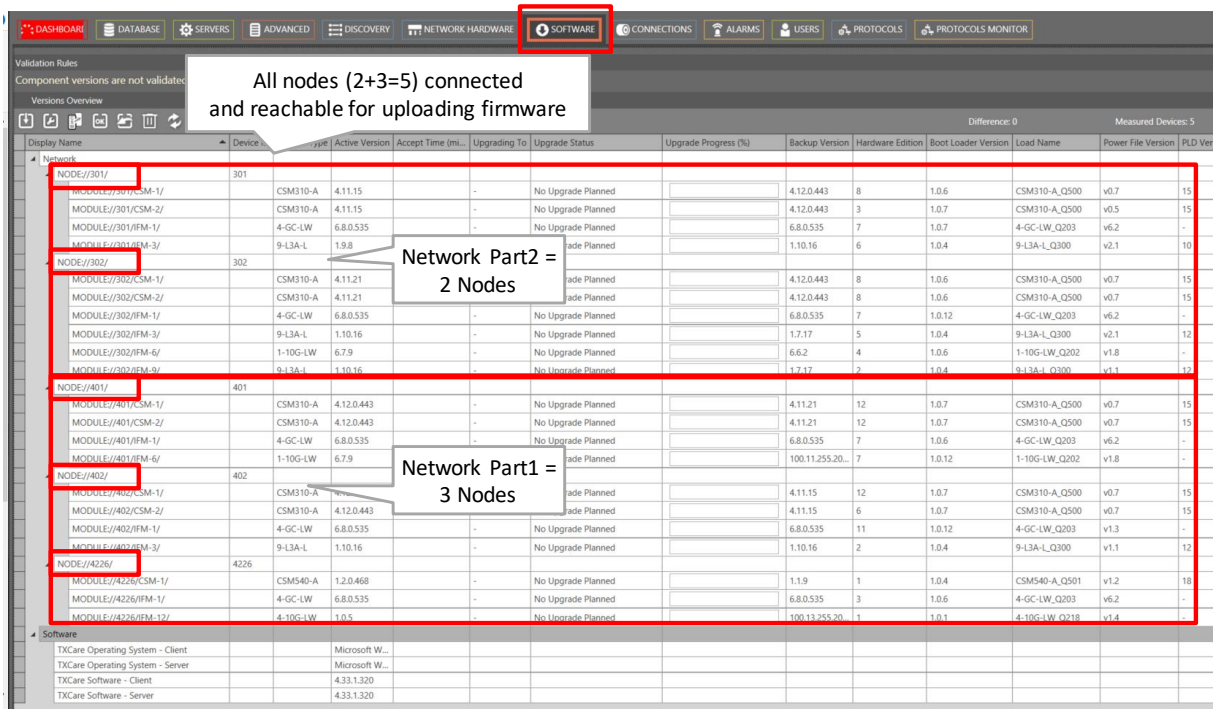


Figure 126 Software Tile: Entire Network Reachable for Uploading Firmware

13.6 Limited Configuration Actions on Reachable Nodes

CAUTION: It is advised to perform no configuration changes in a mixed network. The entire network remains reachable for DCN (§13.4) and firmware uploading (§13.5).

In a mixed network setup, some configurations action in HiProvision are possible if an action does not change the timestamp in the node. The timestamp in the node reflects the latest moment in time that something was loaded by HiProvision into the node.

Offline, full configuration is possible, but when you want to load configuration changes into the live network, some configuration actions might be blocked (see table below) in order to keep both databases on both HiProvision PCs as similar as possible.

If at least one of the load actions is not allowed (Action Possible = '---'), nothing will be loaded at all and the load manager will show the screen below.

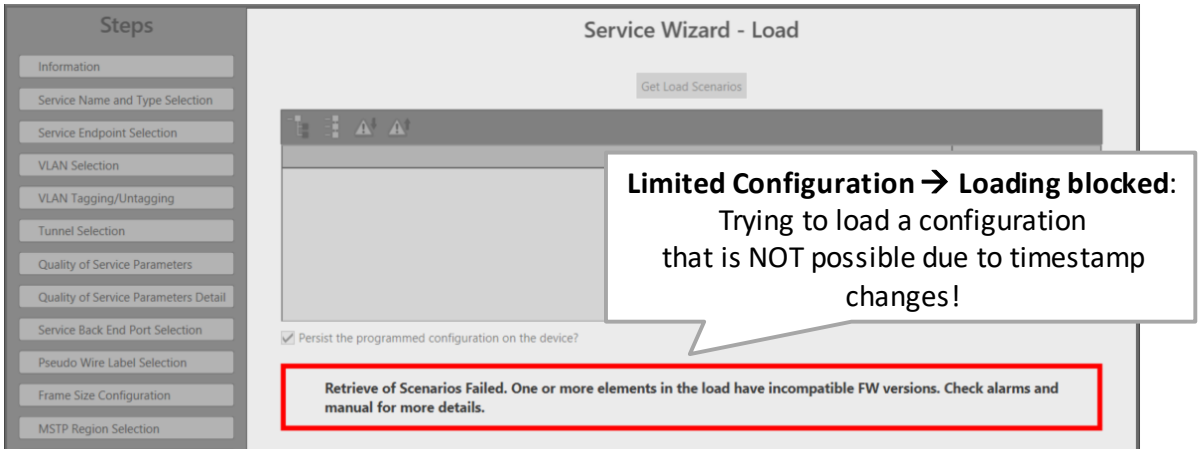


Figure 127 Limited Configuration: Some Configuration Actions are Blocked

NOTE: For the HiProvision's unreachable part of the network, no configuration/monitoring action is possible at all.

Table 19 Limited Configuration Actions Towards Reachable Nodes

Configuration Action	Changes Timestamp	Raised Alarm	Action Possible
Note: ✓= Yes; --- = No			
Modify tunnels and services	✓	Configuration Mismatch	---
Configure Static MAC/sticky MAC/MAC Limit	✓	Configuration Mismatch	---
Configure loopback interface	✓	---	---
Delete a loopback interface (Alarm is cleared after clicking load scenarios although no load scenarios are generated)	✓	Configuration Mismatch	---
Configure port mirroring	---	Node configuration changed	✓
Delete IFM from node	✓	Interface module type present in node but deleted in DB	---

Configuration Action	Changes Timestamp	Raised Alarm	Action Possible
Delete CSM from node	---	---	✓
Add IFM to the node	✓	Interface module configured type Mismatch Alarm	---
Clear a node	✓	Connection Alarm	---
Reset a node	✓	Connection Alarm	---
Configure MACSec	✓	MacSec configuration mismatch	---
CSM Switchover	---	CSM switchover occurred	✓
Clear network approvement	---	Node configuration changed	✓
Apply default SNMP password	---	Node configuration changed	✓
Change SNMP passwords	---	Node configuration changed	✓
All configurations in Protocols Tile	✓	Configuration Mismatch	---
Modify admin status of front or Backend ports	---	Admin Status mismatch	✓
Modify negotiation settings	---	Negotiation Mismatch	✓
Configure QoS classification	---	QoS Classification Mismatch	✓
Configure Storm control	---	XX Storm control mismatch	✓
Configure PoE	---	PoE admin status mismatch PoE Port Power Priority mismatch PoE Port Power Class Mismatch	✓
Configure IEEE1588 Settings	---	1588 Enable Mismatch 1588 Encapsulation Mismatch 1588 Reset Engine Mismatch	✓
CSM Switchover	---	CSM switchover occurred	✓
Create/Delete/Modify LAG	✓	---	---
Port mode – LAN/WAN setting	✓	Admin Status mismatch BPDU Guard mismatch	---
Create Layout	---	---	✓

13.7 Is My Network a Mixed Network?

Your network is a mixed network if one or more critical alarms ‘Node is blocked, incompatible FW version(s) detected’ are visible in the Alarms tile. The result is that your configuration actions in the entire network are very limited (see §13.6).

If this alarm is not visible in the Alarms tile, your network is OK, not mixed and conform the allowed firmware versions for your HiProvision version.

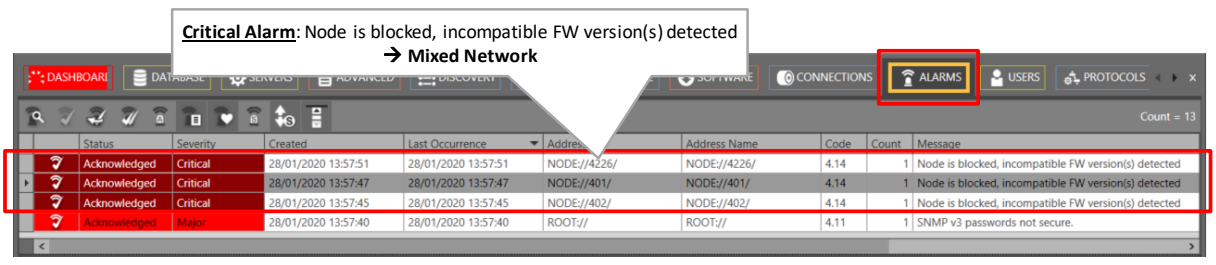


Figure 128 Critical Alarm: Mixed Network

Your network could be an intended mixed network (via the Gradual Upgrade configuration steps) or by accident (via uploading a wrong firmware version or by installing a CSM with a wrong firmware version).

13.8 Which Firmware Versions Are Allowed in My Network?

HiProvision knows which firmware versions are allowed in your network. Once you load an unallowed firmware version in your network, HiProvision will show a critical alarm as mentionned in previous paragraphs.

The allowed HiProvision firmware versions can be found via Dashboard → Software Tile → Click button in the menu bar. Only firmware versions of products listed in this window will be verified by HiProvision. Currently, only the CSM is listed, so only CSM firmware incompatiblities can lead to mixed network that introduces a logical separation into the network.

The asterisk in the figure below indicates a wildcard. So for CSM310-A, e.g. 4.12.1 and 4.12.2 are allowed, 4.13.1 is not allowed and would lead to a logical separation into the network.

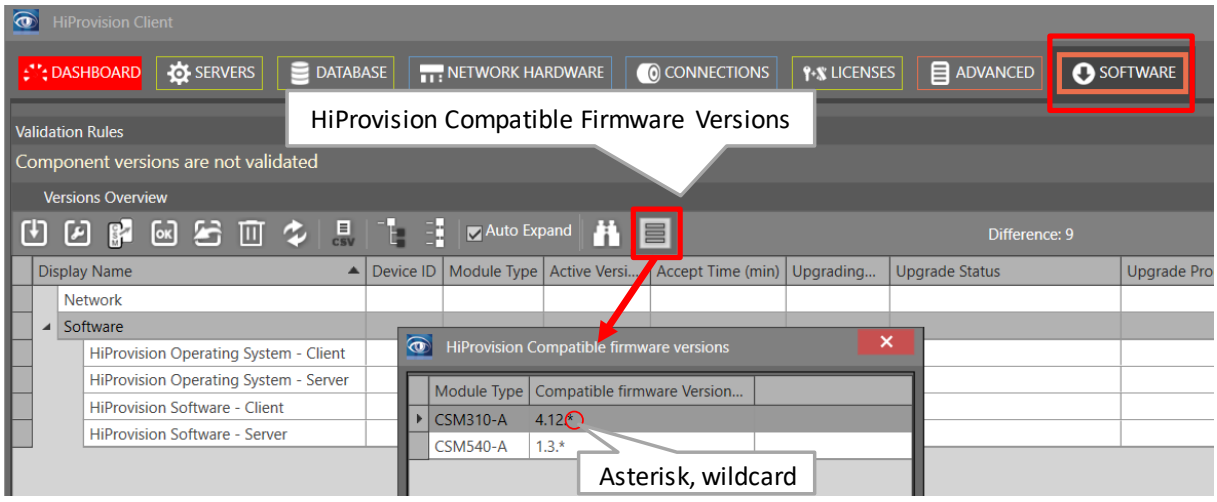


Figure 129 HiProvision Compatible Firmware Versions

14. REMOTE CLIENT/SERVER

14.1 General

Prerequisite: HiProvision must be fully installed on both the server and remote client PC;

Before a remote client/server system can be used or started, it must be configured first. This configuration depends on how the remote client is connected to the server. A remote client can talk to the server via:

- the DCN Channel;
- the DCN Channel with redundant discovery entry point;

- a LAN:
  - Programmed Ethernet service over the Dragon PTN network;
  - connection via an external LAN;

§14.2 shows some example use cases, whereas §14.3 describes how to configure them.

Directly after this configuration has been done, the remote client/server system will be up and running automatically. Later on, if you have to start the remote client/server again after it was shut down, follow the steps in §14.4.

14.2 Example Use Cases

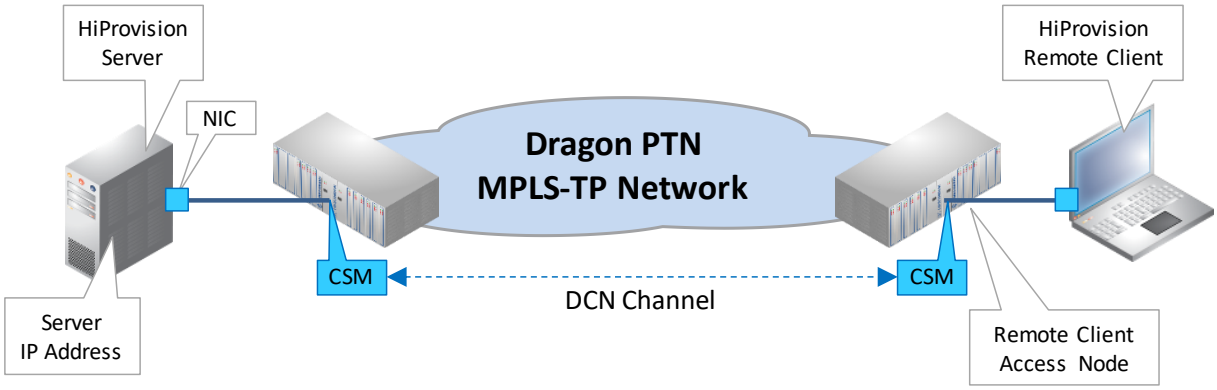


Figure 130 Client-Server Connection: DCN Channel

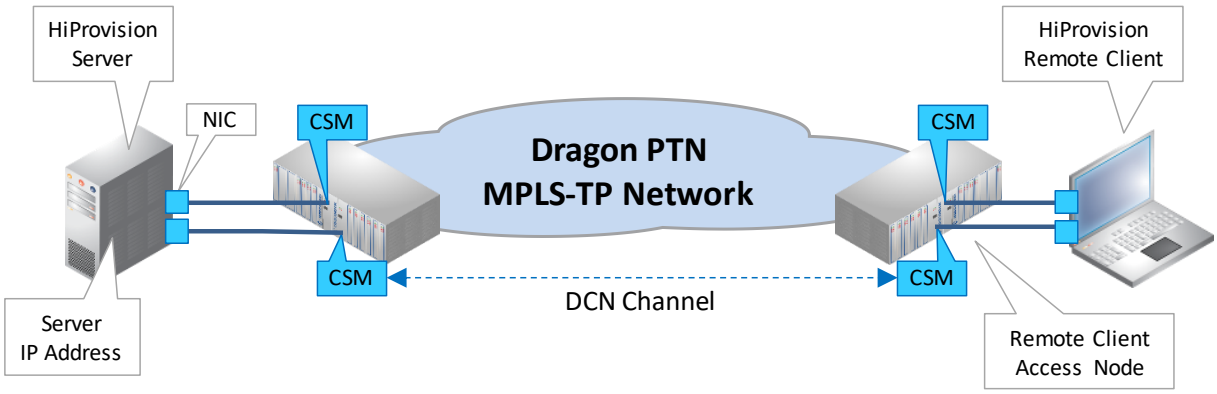


Figure 131 Client-Server Connection: DCN Channel with Redundant Discovery Entry Point

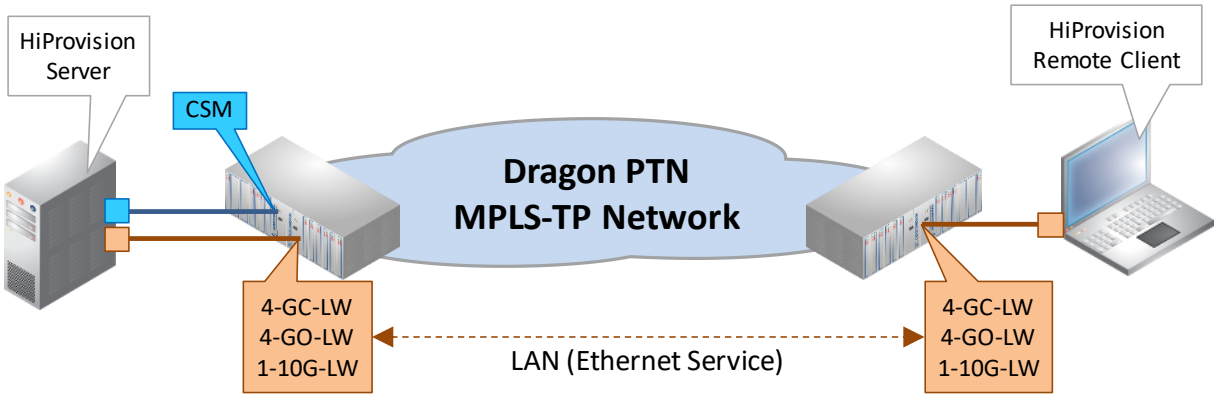


Figure 132 Client-Server Connection: LAN (Ethernet Service)

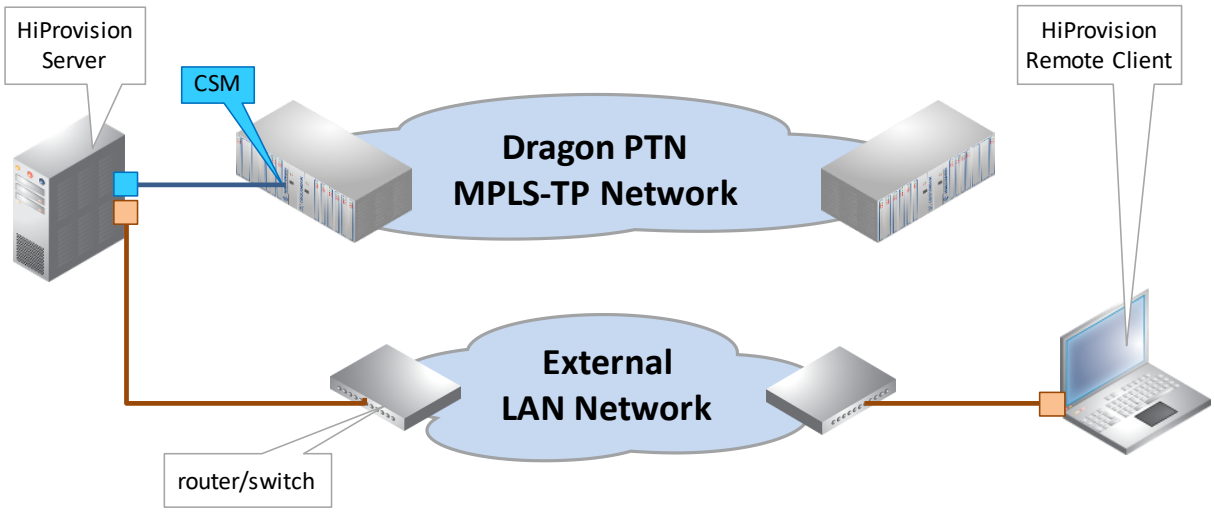


Figure 133 Client-Server Connection: LAN (External LAN)

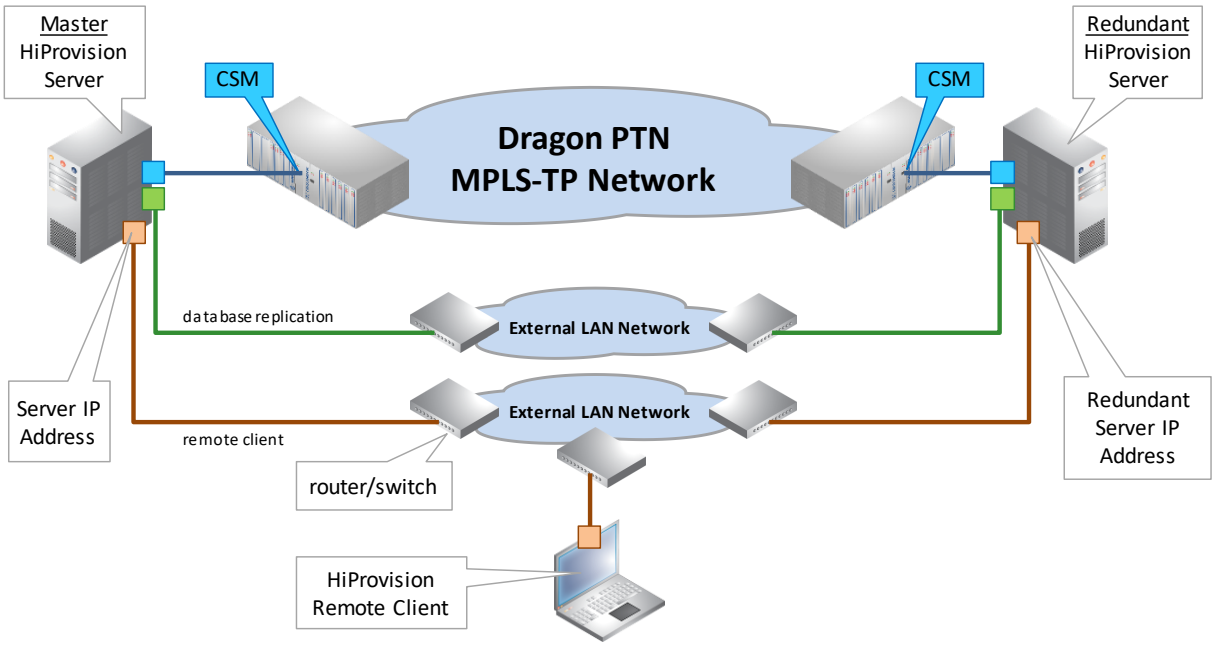


Figure 134 Client-Redundant Server Connection: LAN (External LAN)

14.3 Configuration

Follow the steps below to configure a remote client setup, first on the server PC and next on the remote client PC.

14.3.1 Step1: On the HiProvision Server PC

Prerequisites: HiProvision has been initialized, has discovered the network with the correct entrypoints (§2.5, §11) and is up and running (HiProvision Agent (see §3) and Client have been started);

1. If the remote client must connect to the server via a LAN, provide an extra NIC on the server PC and connect this extra NIC to :
   - an Ethernet Port on an IFM to provide/use the Ethernet service (see Ref. [2Eth] in Table 1);
   - an External LAN network in any other case;
2. If the remote client must connect to the server via the Dragon PTN network (with either one or two (=redundant) discovery entry points):
   - DCN Channel: Indicate the access nodes for the remote client via Dashboard → Servers Tile →  . Select the node(s) and click the  button to make these nodes accessible via a CSM for the remote client;
   - Ethernet Service: program an Ethernet service between IFMs that support the Ethernet Service (see Ref. [2Eth] in Table 1) to interconnect the HiProvision server(s) and the remote client;
3. Close the 'HiProvision Client', only the 'HiProvision Agent' is allowed to run;

14.3.2 Step2: On the HiProvision Remote Client PC

CAUTION: Do not start the 'HiProvision Agent' or stop the HiProvision Agent (see §3), only the 'HiProvision Remote Client' is allowed to run on the remote client PC;

1. Start the 'HiProvision Remote Client' via double-clicking this icon on the desktop;
2. For a first time start of the 'HiProvision Remote Client', the connection with the server will fail;
3. The Servers tile is always unlocked, no need to log in yet;
4. In the Dashboard → Servers Tile, click the  button, the figure below pops up:

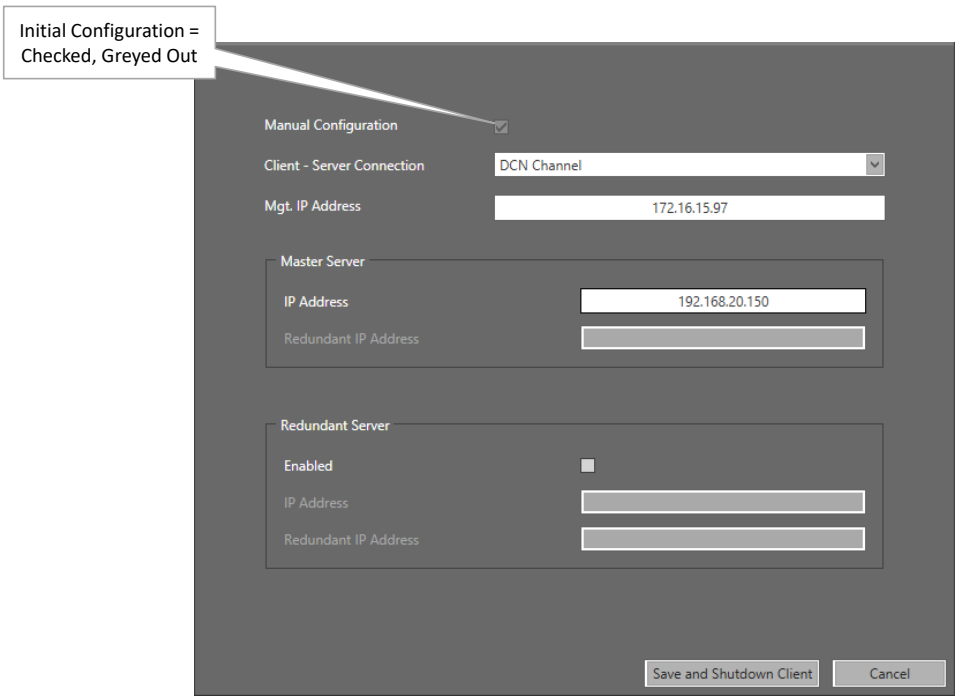


Figure 135 Remote Client Via DCN Channel

5. The 'Manual Configuration' checkbox is checked and greyed out for a first time configuration. The IP addresses have to be filled out manually. Later on, when the remote client has been configured and this setup is opened again, some IP addresses might be detected automatically in case of HiProvision Redundancy and Manual Configuration is unchecked.
6. Client - Server Connection:
   - LAN: Select this option when the remote client communicates to the server via an Ethernet service over the Dragon PTN Network or via an external LAN network. Make sure that this PC is connected to:
     - an Ethernet Port on an IFM that supports the Ethernet service (see Ref. [2Eth] in Table 1);
     - an External LAN network in any other case;
   - DCN Channel: Select this option when the remote client PC is connected one CSM and using the DCN path to communicate to the server;
   - DCN Channel with Redundant Discovery Entry Point: Select this option when the remote client PC is connected to two CSMs and using the DCN path to communicate to the server;
7. (Only with DCN Channel) Mgt. IP Address: Fill out the IP address of the node or the CSM to which the remote client PC has been connected;
8. Master Server:
   - IP Address: IP address of the NIC in the HiProvision Server PC that is communicating with the Remote Client;
   - Redundant IP Address: (only when 'DCN Channel with Redundant Discovery Entry Point' was selected) IP address of the NIC in the HiProvision Server PC that is connected to the second CSM (=redundant entry point);
9. Redundant Server:

- Enabled: Check this checkbox if you have a redundant HiProvision server;
- IP Address: IP address of the NIC in the Redundant HiProvision Server PC that is communicating with the Remote Client;
- Redundant IP Address: (only when 'DCN Channel with Redundant Discovery Entry Point' was selected) IP address of the NIC in the Redundant HiProvision Server PC that is connected to the second CSM (=redundant entry point);

10. Click Save and Shutdown Client. The client will shut down;
11. Start the 'HiProvision Remote Client' via double-clicking this icon on the desktop;
12. Log in;
13. The connection between the remote client and server(s) should be OK and visible after clicking the Servers tile. Your remote client will be operational to manage the Dragon PTN network. Starting the Remote Client/Server system as described in §14.4 is not necessary anymore. If the remote client would not work, verify that some ports are not blocked by a possible firewall, see §21.6;

14.4 Switchover GUI View from Redundant HiProvision Servers

In case of redundant servers and having configured the remote Client as described in previous paragraphs, the logical setup can be viewed via Dashboard → Servers tile.

The green line or 'viewing line' from the Remote HiProvision Client to the Server indicates which server is being viewed in the Remote Client. In the figure example below, the Remote client is viewing the Master HiProvision Server.

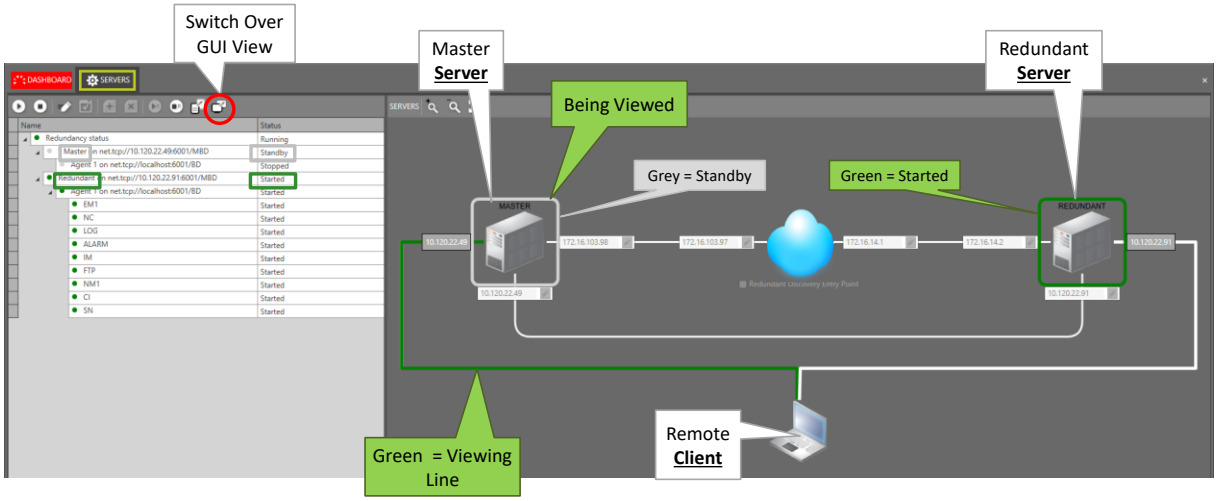


Figure 136 Remote Client Viewing Standby Server

The Master Server PC is in 'Standby' mode (= grey border). It is more interesting to view the 'Started' server PC (= green border). At this moment, the Redundant Server PC is the 'Started' one. Click the GUI switchover button to make the remote client view the other server. As a result in this example, the remote client views the 'Started' server. It could look as follows:

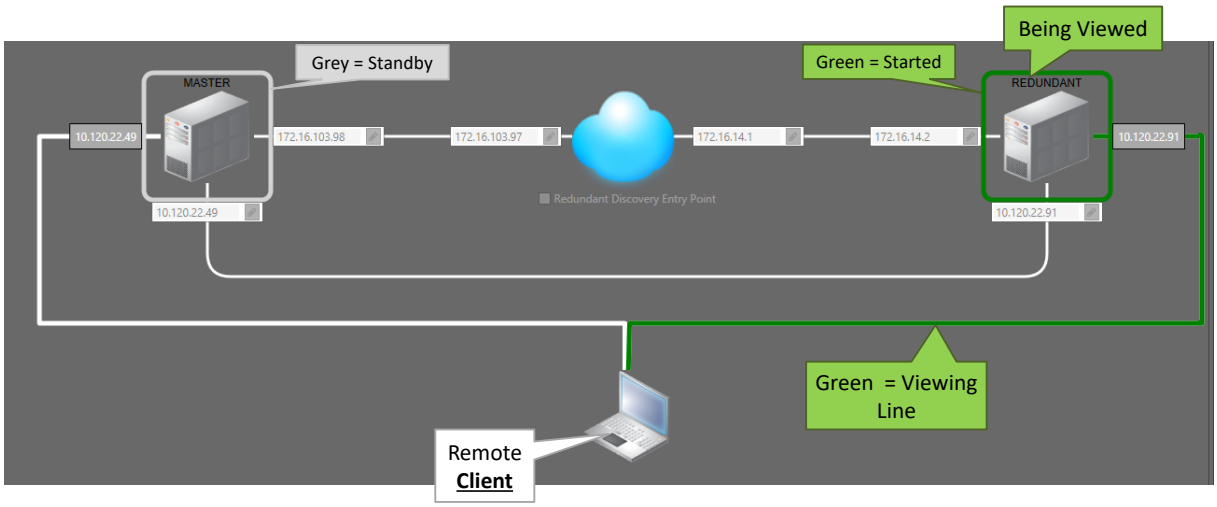


Figure 137 Remote Client Viewing Started Server

14.5 Start Remote Client/Server System

Prerequisite: the Client/Server system has been configured as described in previous paragraphs.

14.5.1 Step1: On the HiProvision (Master) Server PC

1. Start the 'HiProvision Agent', see §3;
2. (The 'HiProvision Client' does not have to be started).

14.5.2 Step2: On the HiProvision Remote Client PC

1. Start the 'HiProvision Remote Client' via double-clicking this icon on the desktop;
2. A login window pops up, log in;
3. After logging in, your remote client will be operational to manage the Dragon PTN network.

NOTE: The same user cannot be logged in together on both the local (on the server PC) and the remote client (on the remote client PC) at the same time. The last login on one PC will automatically log off the same user on the other PC;

CAUTION: when a load is started in the configuration load manager (§7) in a client, all the other (remote) client GUIs will freeze (no user action possible) until the load has finished in the client that initiated the load action. A popup will be shown on the frozen GUIs as in the figure below.

Figure 138 Please wait until loading is done

15. LAYOUTING HIPROVISION

15.1 Layouting Tables

15.1.1 General

A table example is shown in the figure below. You can lay out any HiProvision table in any tab. Following layout actions are possible:

- modify column order;
- sorting the columns;
- hiding/showing columns;
- grouping columns (not all tables)
- filter editor (not all tables);

Closing a tab or the GUI will save the changed layouts automatically for the logged in user. The next time that this user opens a tile, the saved table layouts for this tile will be active.

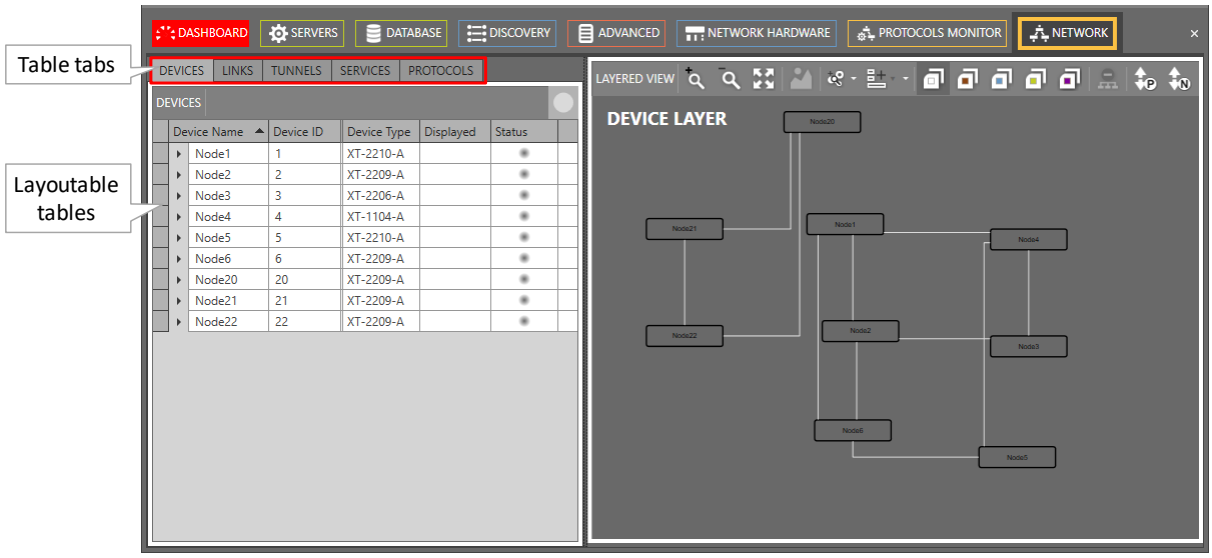


Figure 139 Layouting Tables

15.1.2 Layout Actions

The layout actions for a specific column can be invoked by right-clicking its header cell.

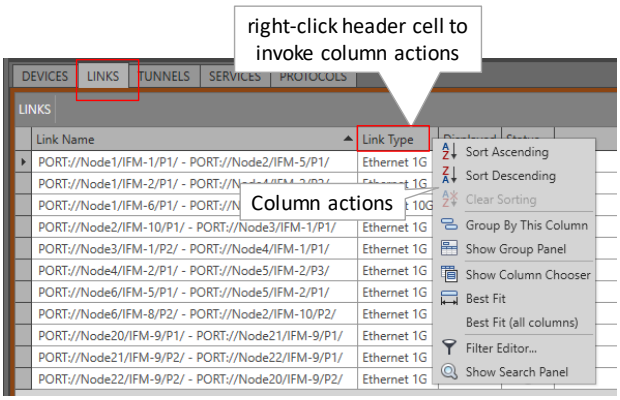


Figure 140 Invoke Column Actions

a. Column Order

The column order can be changed without the layout or column actions menu. Instead, it can be changed by dragging and dropping the column header cell before/after any other column. While moving the column, double-arrow indicators pop up when you can drop the dragged column into place.

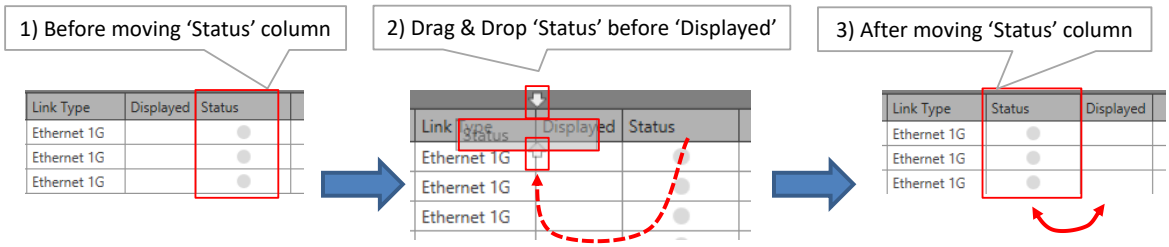


Figure 141 Table Layout: Column Order

b. Sorting Columns

Click 'Sort Ascending' or 'Sort Descending' in Figure 140 or left-click the header cell of the column a few times to sort the column.

c. Hide/Show Columns

Click 'Show Column Chooser' in Figure 140. Drag & drop a column header into Column Chooser and close the Column Chooser to hide a column.

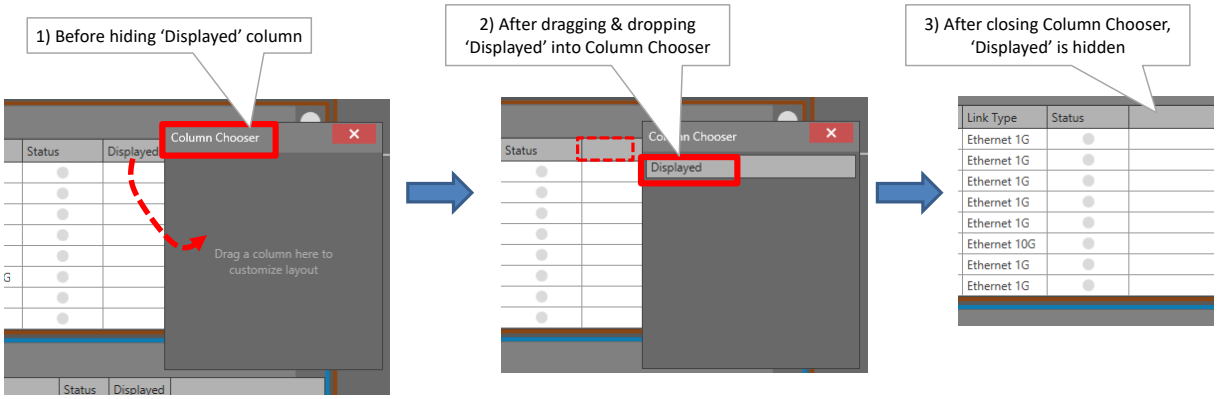


Figure 142 Table Layout: Hiding Columns

To show hidden columns, click 'Show Column Chooser' in Figure 140. Drag & drop a column header from the Column Chooser into the table header to unhide or show a hidden column. Close the Column Chooser. It is similar to the 'Hiding Columns' paragraph but in the reverse order.

d. Grouping/Ungroup Columns

Columns can be grouped for a better overview in the tables. Click the 'Show Group Panel' in the in Figure 140 to show the group panel. This panel will show which columns are grouped. If this panel is empty, none of the columns is grouped.

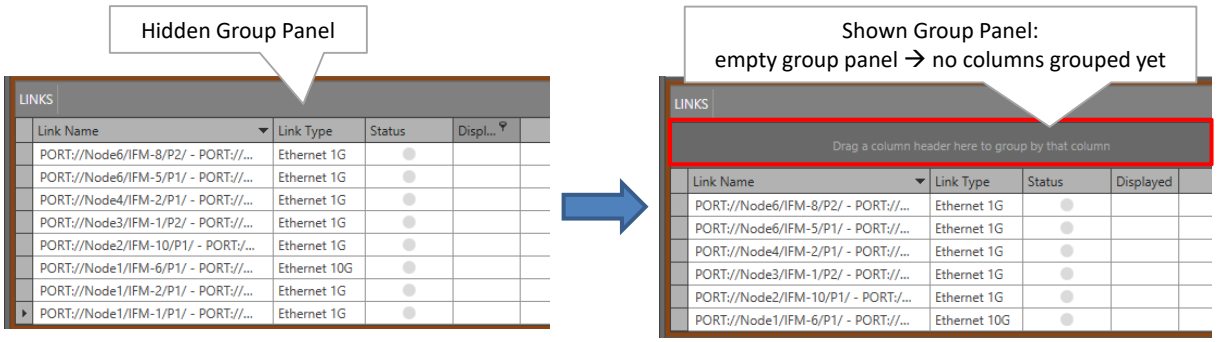


Figure 143 Hidden Group Panel / Shown Group Panel

To group a table by a column, follow one of the two actions below:

- click 'Group By This column' in the layout actions menu of this column;
- Drag the column header into the Group Panel.

As a result, the table will be grouped by this column and the column header appears in the Group Panel. It is possible to group additional columns as well by repeating previous action for additional columns. A grouping example is shown below.

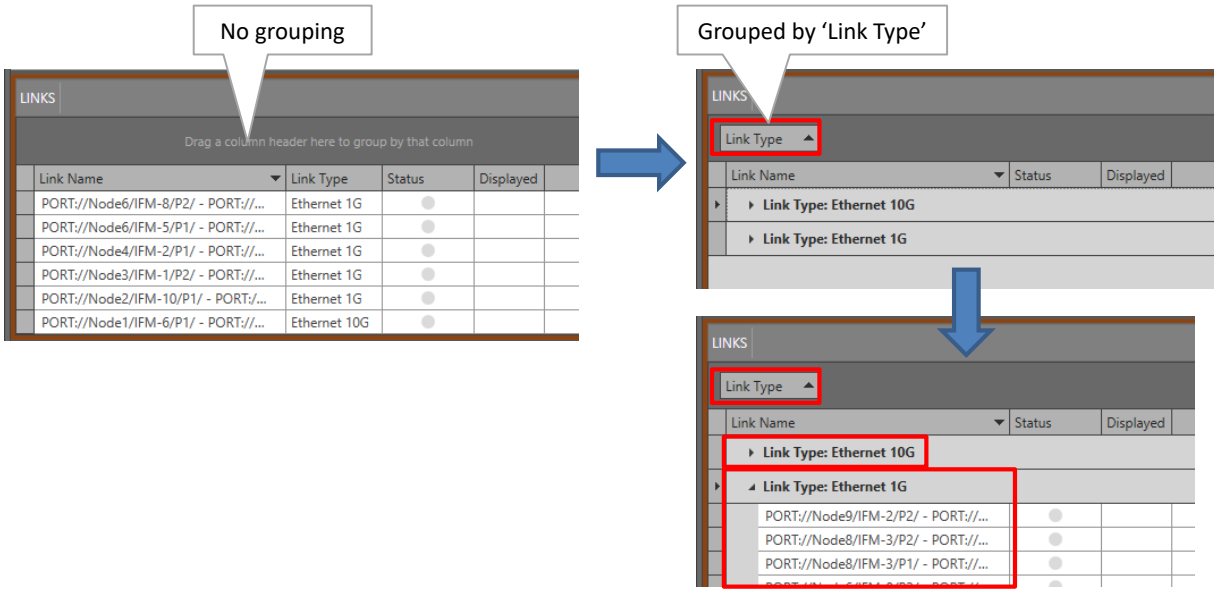


Figure 144 Example: Grouped By Link Type

To ungroup or to clear the grouping of columns, do one of the actions below:

- Drag and drop the column from the group panel into the header row of the table;
- Right-click the group panel and click 'Clear Grouping'.

e. Filter Tables

Tables can be filtered via creating one or more filters in a Filter Editor. Click the 'Filter Editor' in Figure 140 to show the Filter Editor.

In this editor, just click the required filter operators and fields and fill out the desired filter values. Click OK or Apply to create and activate the filter. Each time you adapt your filter or create a new one, the adapted/new filter will be stored in the History Filter List. Later on, you can apply these stored filters again by just selecting them from this History Filter List.

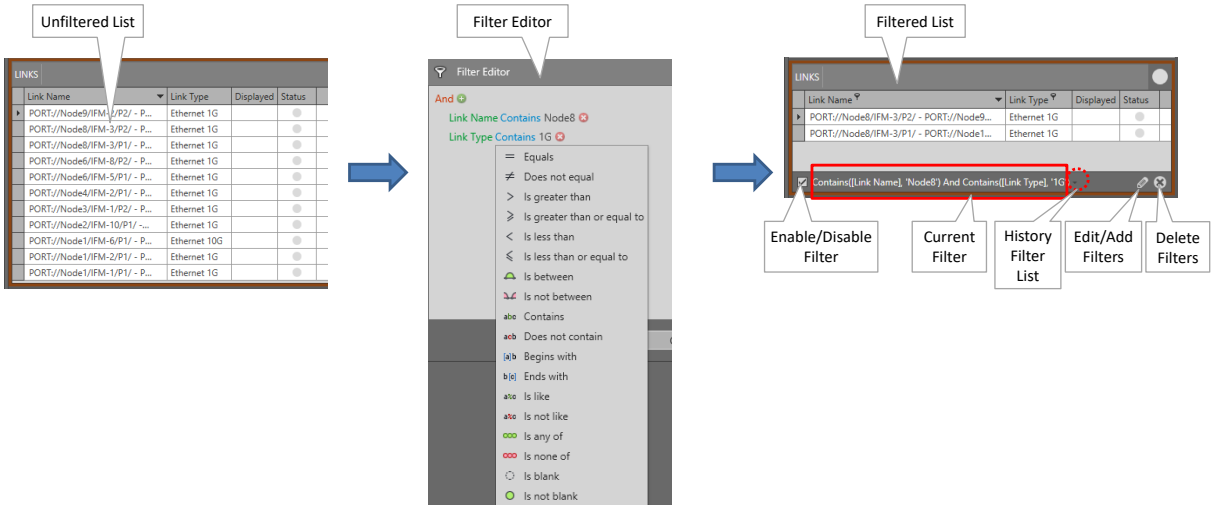


Figure 145 Filtering Tables

15.1.3 Restore Default Table Layouts

1. Go to Dashboard → Users (only allowed for administrators),
2. Select the user for which the table layouts must be cleared by expanding the 'Groups and users' and clicking the desired user row;
3. Click the trashcan icon to reset the customized table layouts.

CAUTION: this action will also reset or clear some other data, see Ref. [15] in Table 1.

4. Click OK to confirm;
5. If you open a tile now, it will restore the default table layouts;

15.2 Layouting Network Drawings

15.2.1 General

This paragraph describes how to place (or layout) the nodes and links into a desired place in relation to each other and/or in relation to an optional background picture. The layout is not fixed in relation to the HiProvision screen (*).

Multiple layouts can be created, saved and organized in one or more layout trees.

Some definitions:

- Layout Tree: A collection of layouts that is related to each other in different levels via nesting;
- Top Layout: The highest level or layout in a layout tree;
- Sub Layout: The child or lower level layouts of a top layout in a layout tree. Sub layouts are designed for tuning multiple views in the Large Network Monitor (see §16) and cannot be used elsewhere in HiProvision;
- Default Layout: The layout that is available in HiProvision from the start without a layout tree, top or sub layout being created. The default layout is an 'Orthogonal Device Layout'.
- Active Layout: The layout that is currently used in all the HiProvision screens that have a network drawing displayed (except for the Discovery and Large Network Monitor (=LNM) tiles). When no layout has been created yet, the default layout is the active layout.
- Device: Node;
- Object: Node (devices) or link;
- Hierarchy Node: a light green bullet in a layout or network drawing indicating a link with nodes in another layout, see further.

CAUTION:
- Only a top layout without sub layouts can be set as active layout;
- (*) The layouting area will center relatively to a boundary around all nodes in the layout. This happens after creating a new, opening or refreshing a layout, or simply after clicking the fit-content button  . When you create your layouts, backgrounds and objects (nodes and links) need to be put manually on top of each other. The background map needs to be resized to fit the boundary of all objects. The objects themselves need to be positioned on the background map. Different layouter options will be helpful here, as well as zooming in/out the entire layouting area.

To process layouts, go to Dashboard → Layouts.

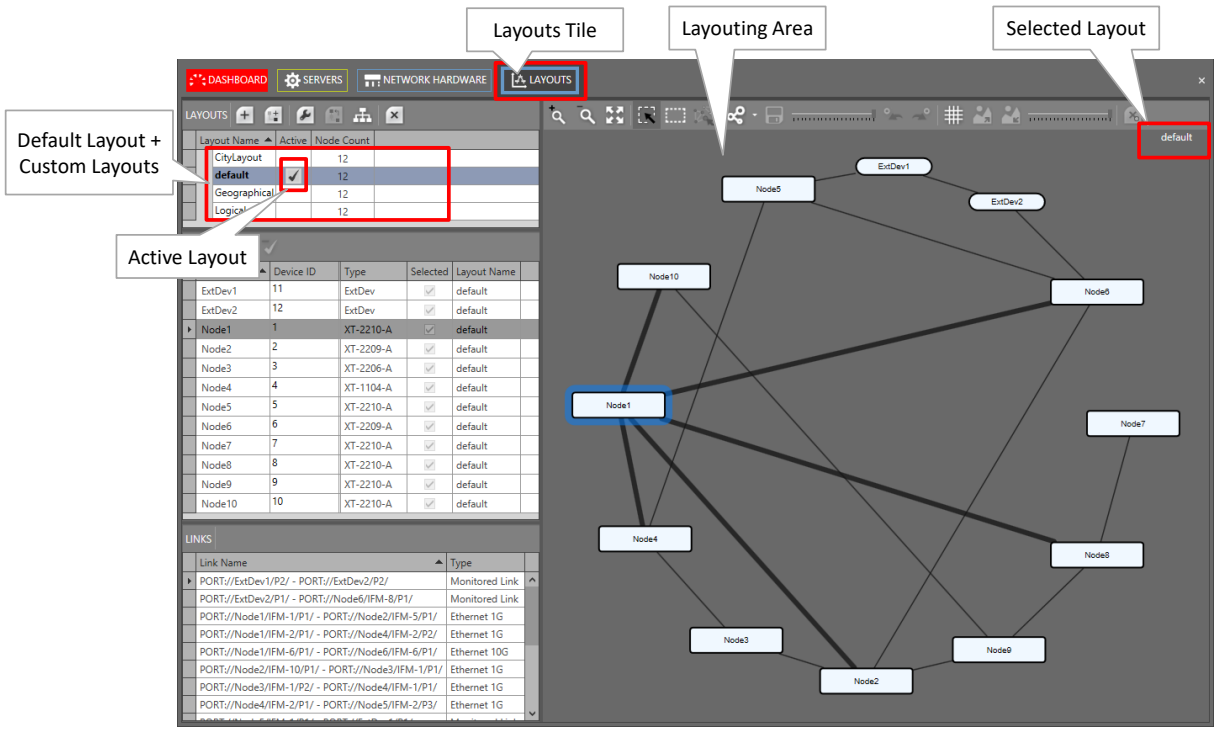


Figure 146 Layouting Network Drawings

NOTE: Layouts can be modified/deleted, but the last remaining layout cannot be deleted.

15.2.2 Layout Guidelines

There are many layout options but in most cases, following typical network layouts are desired:

- Geographical layout: network is mapped on a geographical map or ground plan etc...;
- Logical layout: network is layouted according to a logical network or company topology;
- Don't care: layout is not relevant at all, just use the default layout.

A short description how to set up such a layout can be found below.

NOTE: A full description of all the layout options can be found in §15.2.3. Other layout types can be created by creating new layouts and exploring all the layout options in this section.

a. Geographical Layout

1. Create a new layout (+) including a background picture (=map, ground plan...) of maximum 9 Mb via the Browse button. *.JPG and *.PNG files are allowed as background picture;

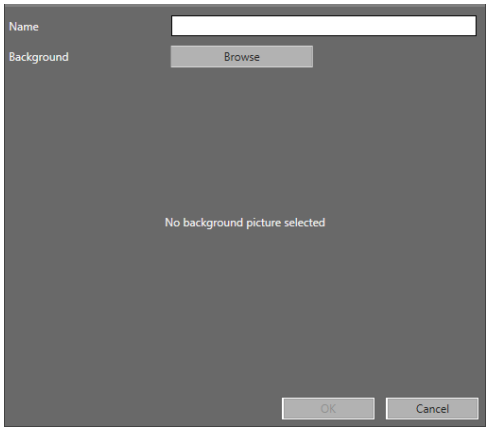


Figure 147 Create Layout

2. Resize the background picture until it has the desired size (/);
3. Apply some transparency to the background picture via the right-hand slider ( );
4. Position a node:
   - Select the desired nodes first:
     - Click (= single node select) and click one node so it highlights;
     - Click (= multi node select) and click/drag a rectangular selection area around the desired nodes. The selected nodes will be highlighted;
   - Position the selected node(s) via drag and drop into place according to the desired spot on the background picture;
5. After placing the nodes, your links layout could be messed up a bit. You can layout them better if desired. Exact geographical links are required?
   - Yes: Click first and drag and drop each link manually (create bends etc...) onto the exact location. You could still straighten up one link via selecting the link (bold black line) and clicking → Straight Link Layout;
   - No: choose one of the layouters ( ) below for an automatic link layout:
     - Straight Link Layout;
     - Orthogonal Link Layout;
     - Organic Link Layout;
6. Save the layout ( );
7. To activate this layout for the entire HiProvision (except for Discovery and Large Network Monitor), set this layout as 'Active' ( );

b. Logical Layout

1. Play around first with one of the automatic ( ) layouters listed below and select the layout that suits the best for your project:
   - Orthogonal Device Layout;
   - Circular Device Layout;
   - Organic Device Layout;
2. Fine-tune your layout further via drag/drop your devices and links manually as described in the previous paragraph §a;

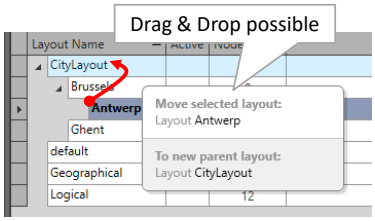
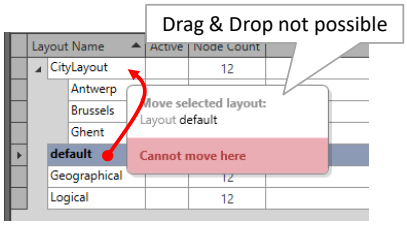
3. Save the layout ( );
4. To activate this layout for the entire HiProvision (except for Discovery and Large Network Monitor), set this layout as 'Active' ( );

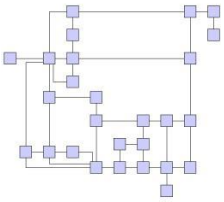
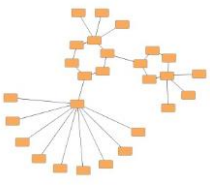
c. Don't Care

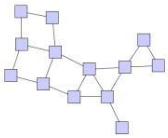
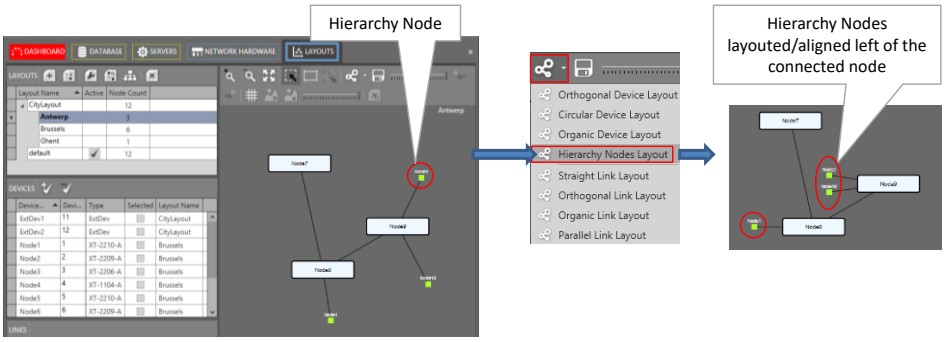
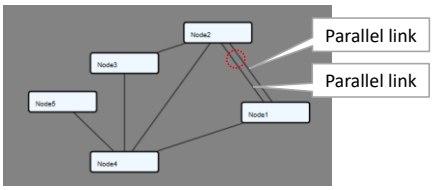
If the layout is not important at all, do nothing. HiProvision applies a 'default' layout to your network based on the automatic 'Orthogonal Device Layout' layouter ( ). This 'default' layout is by default 'Active' ( ) in the entire HiProvision (except for Discovery and Large Network Monitor).

15.2.3 Layout Menu and Options

Table 20 Layout Buttons

Button	Short Description
LAYOUTS	
	Create new (top) layout. This is a layout at the highest or top level.
	Create new sub layout for using in the Large Network tile (see §15.2.4). The sub layout will be created in the selected layout. Sub layouts can be created up to 10 levels deep starting from the top layout. Sub layouts cannot be created in the active layout. So if there is only the default layout (and as result, automatically the active layout), another top layout must be created first. The Node Count field indicates exactly how many nodes are involved in a specific sub layout. The Node Count is also visible in the sub layout icons in the network drawing. A maximum of 100 sub layouts can be created per top layout. Example to create sub layouts: see §15.2.4.
	Modify selected layout: Possibility to change the layout name and/or background picture.
	Move a sub layout (=reparenting): Move an existing sub layout from its parent to another parent layout within the same top layout in the layout tree. **Note**: Reparenting can also be done (without this button) by just drag & drop a sub layout to another parent layout. This drag and drop will show whether the drag & drop is possible.  
	Sets the selected top layout as active layout. Only layouts without sub layouts can be set as active because sub layouts are only meant for the Large Network tile (see §15.2.4). All the HiProvision screens that have a network drawing displayed, will display it according to the active layout. By default, the 'default' layout is active.
	Delete selected layout from the layout list. Neither the last remaining layout nor the active layout can be deleted.
Layouting Area	
/	Zoom in / Zoom out of the layouting area. CAUTION: Zoom in / Zoom out results will not be saved when saving the layout.
	Fit all nodes and links in the center of the layouting area. If your nodes and links look lost, click this button to bring them back in focus in the center of the layouting area.
	View mode: select **one object (node or link)** at a time, in this mode you can: - Drag & drop the entire layouting area in a specific position (CAUTION: this new position will not be saved). - Layout objects into place by drag & drop the selected object.

Button	Short Description
	- Click on single objects (node or link) to select them. A selected node has a blue-grey-blue border, a selected link is shown in a bold black line. A selected bend in a link shows a black bullet. - Create a bend in a link by drag & drop on the link where the bend must be made, see Figure 148. - Delete a bend in a link by selecting the bend and clicking , see Figure 149. NOTE: unselect the selection via clicking on the background.
	Selection mode: select multiple objects (node or link) at a time, in this mode you can: - Select multiple objects via a rectangular selection area. Links that have at least one end point in the selection area will be selected as well. - Click on single objects (node or link) to select them. A selected node has a blue-grey-blue border, a selected link is shown in a bold black line. A selected bend in a link shows a black bullet. - Layout objects into place by drag & drop the selected object or object group (=group of selected objects). NOTE: unselect the selection via clicking on the background.
	Selects all remaining network elements that are directly or indirectly (*) connected to an existing selection of network elements. For example by using this button, you can select a subnetwork in just 2 clicks: click1= select one element from the subnetwork, click2 = click this button. (*): indirectly means that the network element is connected via another network element to the current selection. NOTE: unselect the selection via clicking on the background.
	The layouter selector button provides a few automatic layouter methods that can be used optionally to optimize your layout. NOTE: You could layout your devices and links manually as described in / without a layouter. Layout only a part of your network? YES: - (advised) manual layout: select objects that must be layouted and then drag & drop manually; - automatic layout: select objects that must be layouted and select a layouter from the list. NO, entire network: - automatic layout: select a layouter from the list without selecting objects first. Layouters: Entire layouts (devices + links): - **Orthogonal Device Layout** (=default): produces compact drawings without overlaps, few crossings and few bends  - **Circular Device Layout**: produces interconnected ring and star topologies  - **Organic Device Layout**: produces a well-balanced distribution of nodes width edge crossings, similar to organic

Button	Short Description
	structures in outside nature.  - **Hierarchy Nodes Layout**: This layouter becomes active in sub layouts containing at least one hierarchy node. A hierarchy node is a light green bullet indicating the link with nodes in another layout. Clicking 'Hierarchy Nodes Layout' aligns the light green bullets nicely on the left-hand side of its connected node for a better overview. If you select... : - Nothing: the layouter layouts all hierarchy nodes; - an object (one or more nodes, one or more hierarchy nodes): the layouter layouts only the hierarchy nodes from the selected objects.  Link Layouts: Layouts the selected link in a straight/orthogonal/organic/parallel way. If no link is selected, ALL your links will be layouted accordingly. Devices are not touched. Use this option when you have layouted your devices manually and your links are messed up a bit. - **Straight Link Layout**: for straight links; - **Orthogonal Link Layout**: for right or squared angled links; - **Organic Link Layout**: for well-balanced distributed links; - **Parallel Link Layout**: a link that has a neighbor link between the two same nodes is called a parallel link, see figure below. If nothing is selected only all parallel links (and not single links) in the drawing will be affected. 
	Saves your layout.
	Undo previous action(s) / Redo undone action(s) on nodes and links. Clicking multiple times on this button undoes/redoes the next action in the history action list. This history action list will be cleared when a node or sub layout is added, deleted or moved to another layout.
 (1st)	Sets the sub layout group icon transparency. Only active if the selected layout has sub layouts. Set this slider to the left/right for maximal/minimal transparency. The transparency can be set per group icon.
	Hides/shows the data grid points in the layouting area. When the grid is on, layouting or dragging/dropping the links or bends in the link will be magnetized by the grid points.
	Only relevant if a background image has been inserted in the layout. Click  /  to increase / decrease the size of the background image, click as many times as needed until the desired size has been reached.

Button	Short Description
 (2nd)	Sets the background image transparency (if any). Only active if a background image has been inserted in the layout. Set this slider to the left/right for maximal/minimal transparency.
	Deletes the selected bend in a link. As a result, the link will be straightened up. A bend must be selected first in  mode by clicking the bend. A bend is only selected when a black bullet is visible on the bend. See Figure 149.

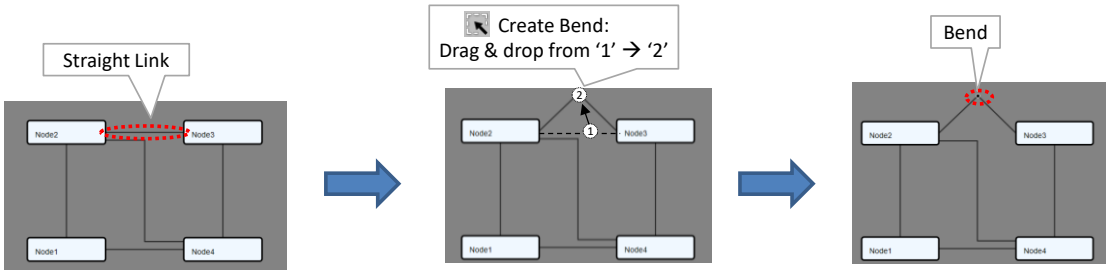


Figure 148 Create Bend

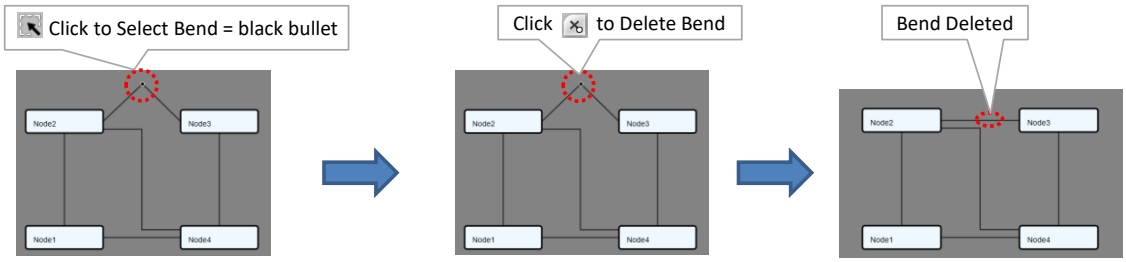


Figure 149 Delete Bend

15.2.4 Example Sub Layouts

As an example, we will show you how to map an example network with 12 nodes into sub layouts according to some cities. We will create a top layout 'CityLayout' first, next we will create sub layouts with the following Belgian cities: 'Antwerp', 'Brussels', 'Ghent'. Background maps are possible but not used in this example.

- CityLayout (=top → has 12 nodes: device [1,...,12]);
  - Brussels (=sub → has 6 nodes: device [1,2,3,4,5,6]);
  - Antwerp (=sub → has 3 nodes: device [7,8,9]);
  - Ghent (=sub → has 1 node: device [10]);
  - Device [11,12] remain in the 'top' CityLayout;

Without creating a top or sub layout, a default layout is always available from the beginning:

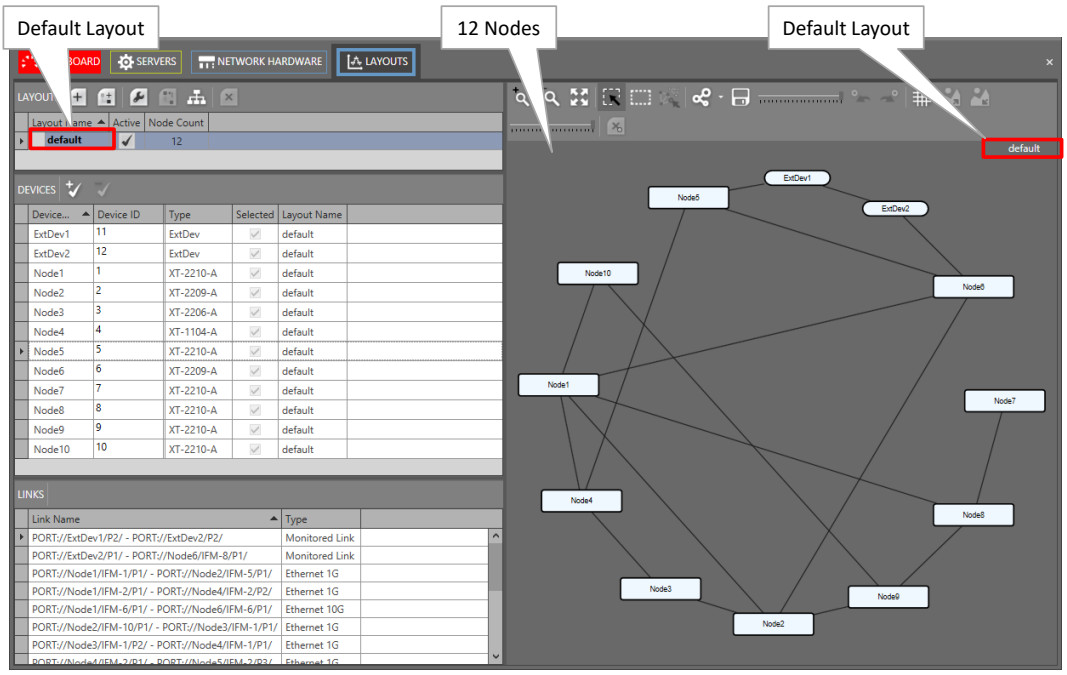


Figure 150 Before Sub Layout Creation

Follow the steps below to create a top and sub layouts:

1. 'CityLayout': Create a new top layout first via clicking and fill out 'CityLayout' in the Name field. Optionally, a background image can be added (not in this example);
2. 'Brussels': Select the 'CityLayout' line in the LAYOUTS table and click , fill out 'Brussels' in the Name field;
3. 'Antwerp': Select the 'CityLayout' line in the LAYOUTS table and click , fill out 'Antwerp' in the Name field;
4. 'Ghent': Select the 'CityLayout' line in the LAYOUTS table and click , fill out 'Ghent' in the Name field;
5. Give an initial layout via clicking and selecting Circular Device Layout;
6. The result looks like the figure below. No nodes have been mapped to a sub layout yet;

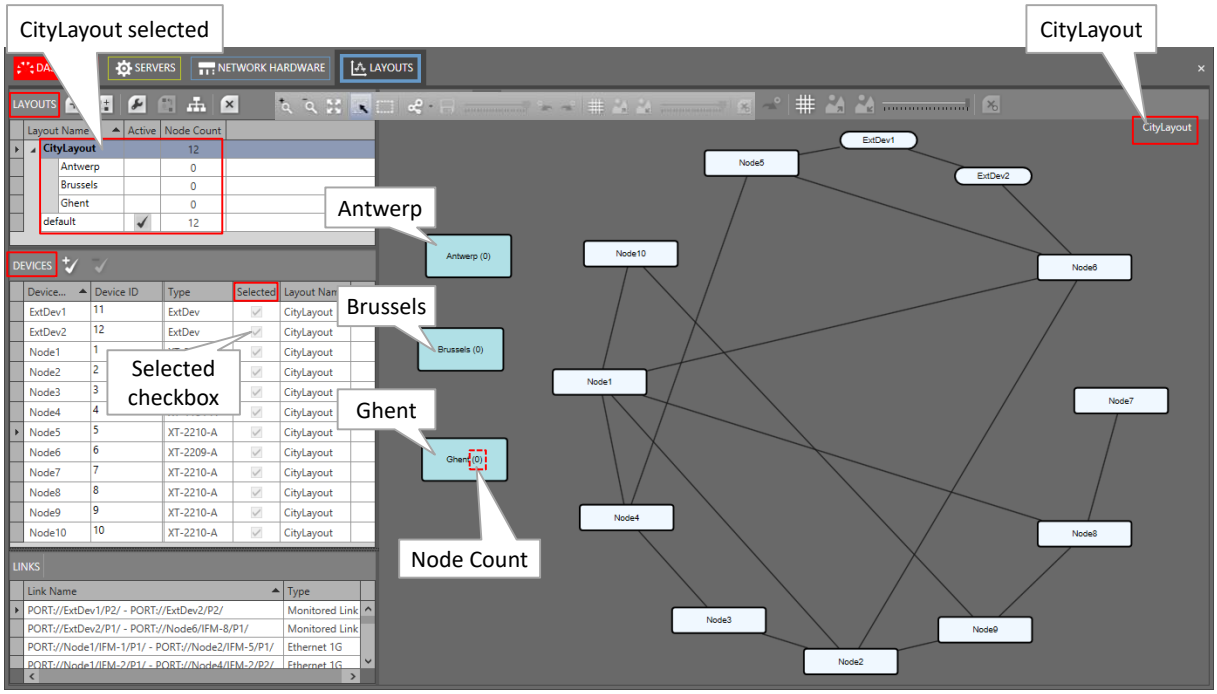


Figure 151 CityLayout View after Creation, No Mapping Yet

7. Map Node[1..6] into the sub layout 'Brussels' via one of the methods below:
   - **Method1**: Choose the sub layout 'Brussels' by clicking the 'Brussels' row in the LAYOUTS list. Map the nodes Node[1..6] into this layout by clicking its 'Selected' checkbox in the DEVICES list. 'Brussels' will appear in the Layout Name column;
   - **Method2**: In the parent layout 'CityLayout', select the Node[1..6] icon in the network drawing (in mode /) or select multiple nodes at once by dragging a selection area around them (in mode). Once the nodes are selected, press and hold the SHIFT key on your keyboard and drop the selected nodes onto the node group icon of the desired sub layout (e.g. + SHIFT + hoover it with selected nodes = . Drop handles turn into an entire icon border when zooming in more.);
8. Similar to above, map Node[7..9] into the sub layout 'Antwerp';
9. Similar to above, map Node[10] into the sub layout 'Ghent';
10. In this example, Node[11,12] remain in the parent 'CityLayout';
11. Verify all the top and sub layouts whether they are OK. If a layout is not OK (e.g. node icons on top of each other etc...), layout them until it is OK as described in §15.2.2. Save each layout by clicking the save button ;
12. Everything should be OK now. The final result could look as in the figure below;

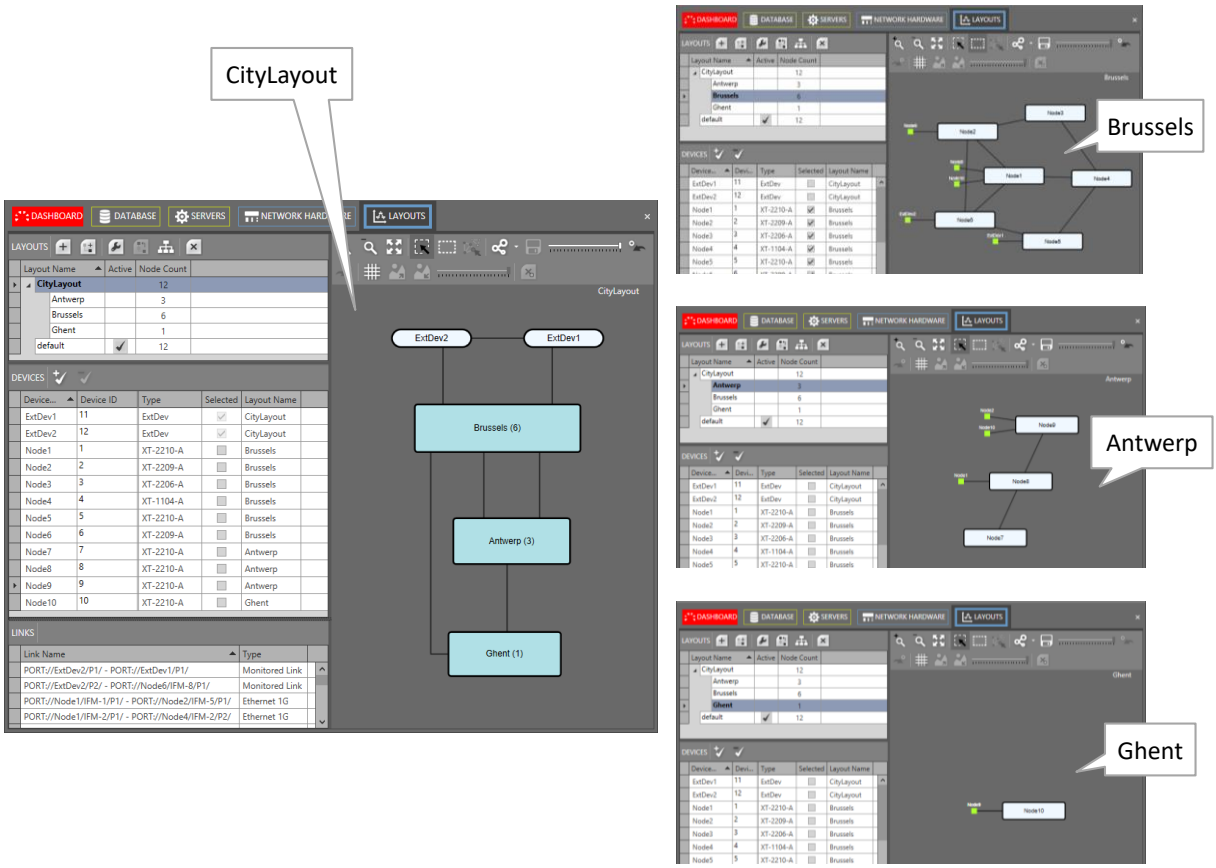


Figure 152 Final Result after Mapping Nodes into Sub Layouts

16. LARGE NETWORK MONITOR (=LNM)

16.1 Prerequisite

Divide the large network into smaller parts for better monitoring by grouping parts of the network in layouts and/or sub layouts. It can be done via the Dashboard → Layout tile (see also §15.2). The grouping could either be functional, geographical...

CAUTION: An LNM voucher or license must have been purchased and installed per serial key. Without these vouchers, only offline configuration is possible. See also §4.

16.2 General

The LNM allows to monitor large networks in an elegant way. This feature can be used via the Dashboard → (Monitoring) Large Network. An example can be found below.

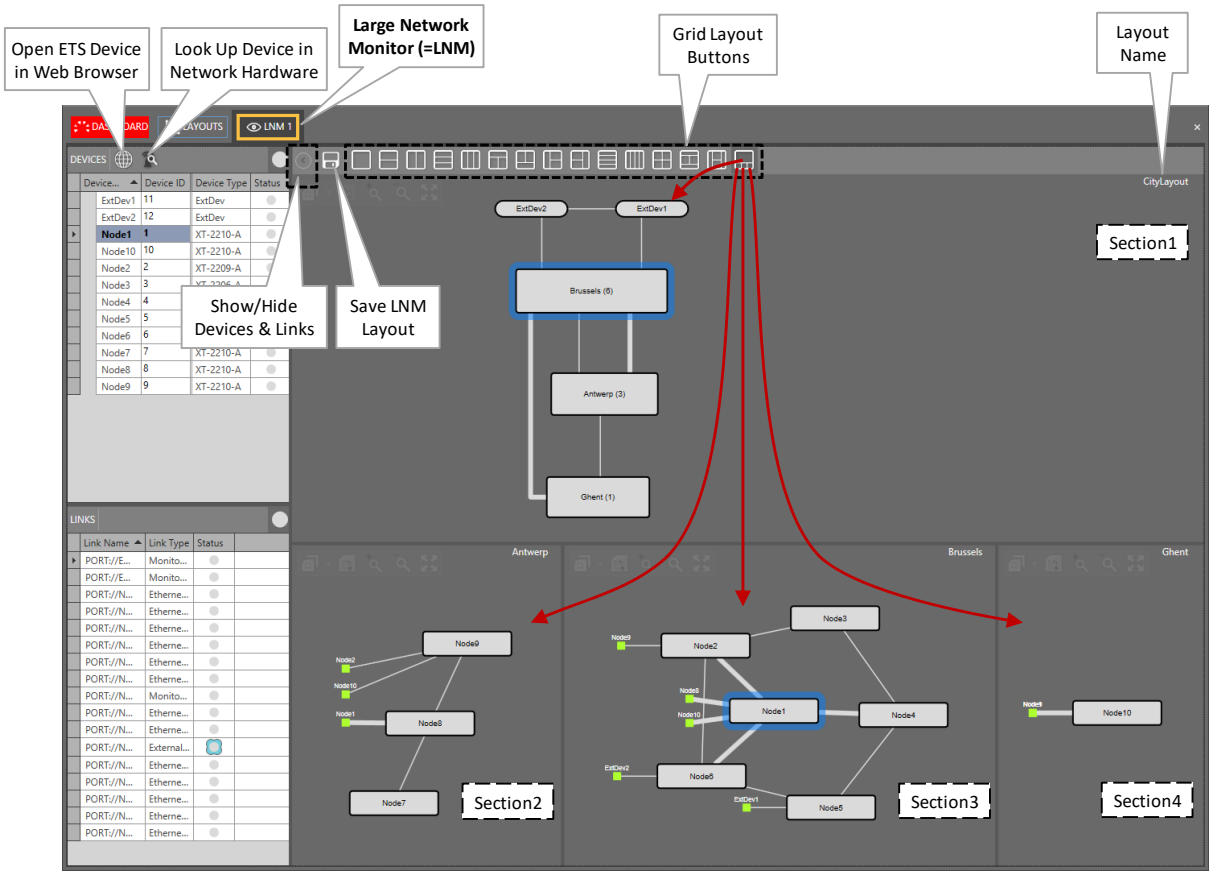


Figure 153 Large Network Monitor

16.3 Open Selected External Device in Web Browser

Select an External device from the list and click the button to open this External device in a web browser, see also §18.9.

16.4 Loop Up Selected Device in the Network Hardware Tile

Select a device from the list and click the button to navigate to or look up the selected device in the Dashboard → Network Hardware tile.

16.5 Selecting Grid Layouts

Different **grid layouts** are by default available. Each grid layout has one or more (up to four) grid sections and can be selected via the grid layout buttons. Swapping from one grid layout to another is possible in just one click via these buttons. The button can be used to show/hide the Devices and Links tables for a wider view without tables. Use the save button to save your optimized view after completing the next paragraphs.

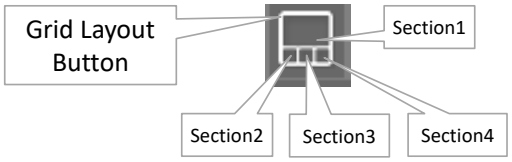


Figure 154 Layout Grid Button Example

16.6 Assign Layouts to Grid Sections

Each layout configured in the Layout tile can be assigned to any grid section via the layout selector . This selector and other buttons pop-up after hovering over the grid section. After having assigned a layout to a grid section, following buttons can be used per grid section:

- : 'Go back to Parent' button to navigate one level up or to assign the parent layout to this section;
- / : zoom in / zoom out buttons;
- : to fit and center your layout in the grid section or bring back the layout in focus when it looks lost beyond the section borders;

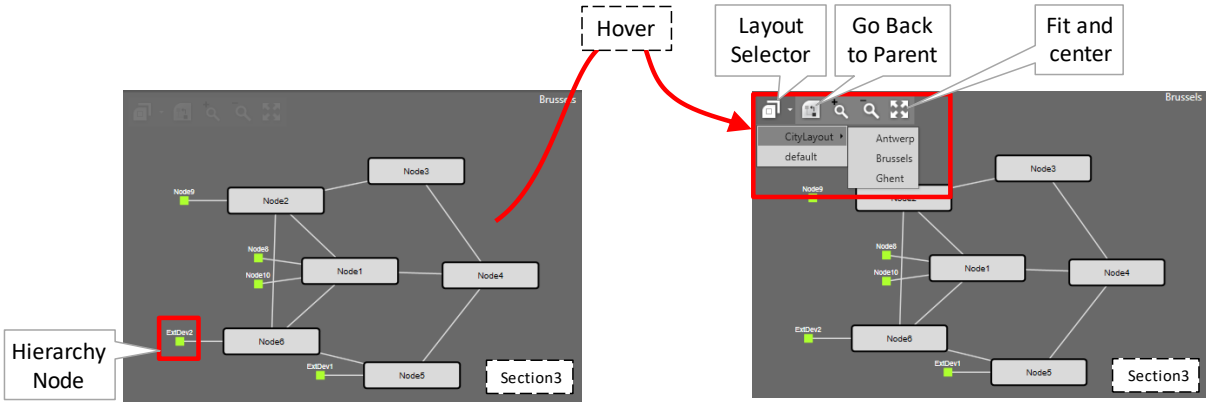


Figure 155 Grid Section: Layout Selector

NOTE: Make sure to save your layout via the save button after having it optimized. The Hierarchy Node (see §15.2.1) can be clicked to navigate one level up.

16.7 Multiple LNM Sessions

A maximum of 4 LNM sessions can be opened simultaneously. Each time you click the 'Large Network' tile, a new LNM session (or tab) will be opened, always starting with LNM1. Each LNM session can have its own grid layout as described in previous paragraphs. Each opened LNM session has its own dedicated shortcut (or checkbox) on the 'Large Network' tile. The first checkbox (most left) always refers to LNM1,..., the last checkbox (most right) always refers to LNM4.

NOTE: If no LNM session is opened yet and you want to open for example LNM3, you have to open the lower-numbered sessions LNM1 and LNM2 first.

You can jump to an LNM session by clicking its checkbox on the tile or its tab.

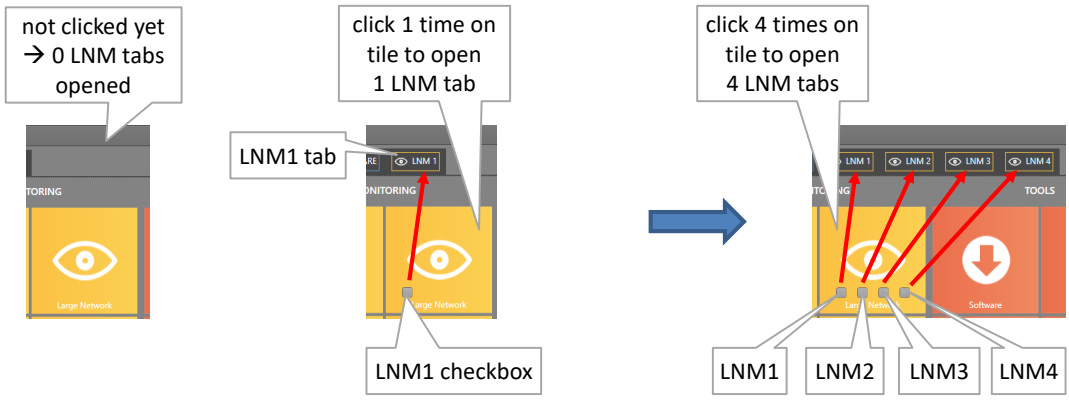


Figure 156 Multiple LNM Sessions

16.8 Large Network Monitor Live

The example screenshot below shows multiple LNM tabs (LNM1 and LNM2) with each tab its own grid layout. LNM1 shows a node rack background picture and country maps of Belgium including nodes and networks. LNM2 shows some more detailed network layouts per Belgian province. The node icon colors (red, green...) indicate the severest alarm color that is present in that node. For more info on LNM alarms, see §9.10.

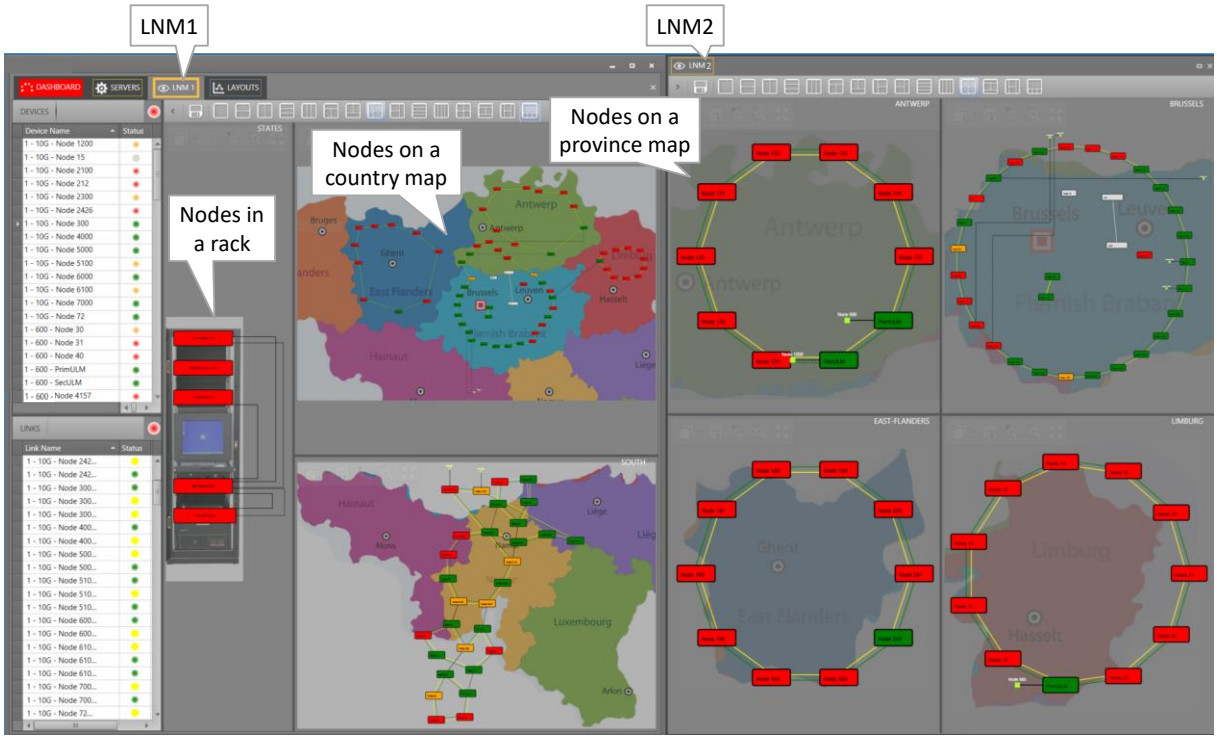


Figure 157 Large Network Monitor Live

17. ADD-ONS

17.1 General

Add-ons provide extra integrated functionality in HiProvision and require purchased vouchers or licenses to operate. The available add-ons can be found in HiProvision via Dashboard → (Tools) Add-ons and are shortly described in the paragraphs below.

17.2 CAR IP

The CAR IP (=Central Alarm Reporter IP) add-on is an alarm interface between HiProvision and a CAS (=Central Alarm System) or umbrella management system both connected through an Ethernet link (UDP). This add-on requires a 'CAR IP Add-on' voucher (see §4.2) or license that must be purchased. A general CAR IP example can be found in the figure below. Find more information on this add-on in manual Ref.[20] in Table 1.

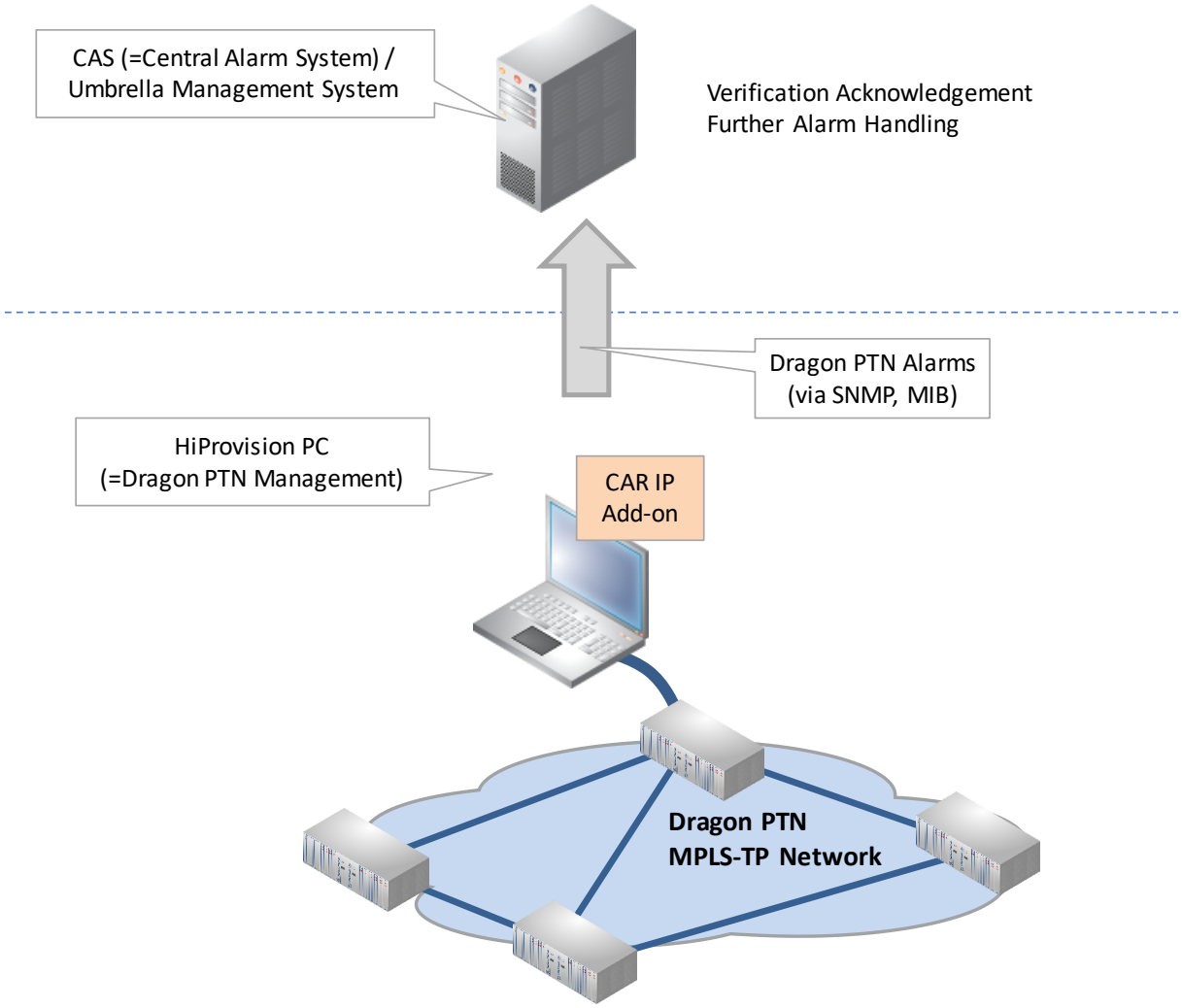


Figure 158 CAR IP Example

17.3 SNMP Northbound

This add-on provides alarm, counter and configuration status information from the Dragon PTN network through an SNMP (=Simple Network Management Protocol) interface to an upper management system (=umbrella system). This add-on requires an 'SNMP Northbound Add-on' voucher (see §4.2) or license that must be purchased. A general SNMP Northbound example can be found in the figure below. Find more information on this add-on in manual Ref.[21] in Table 1.

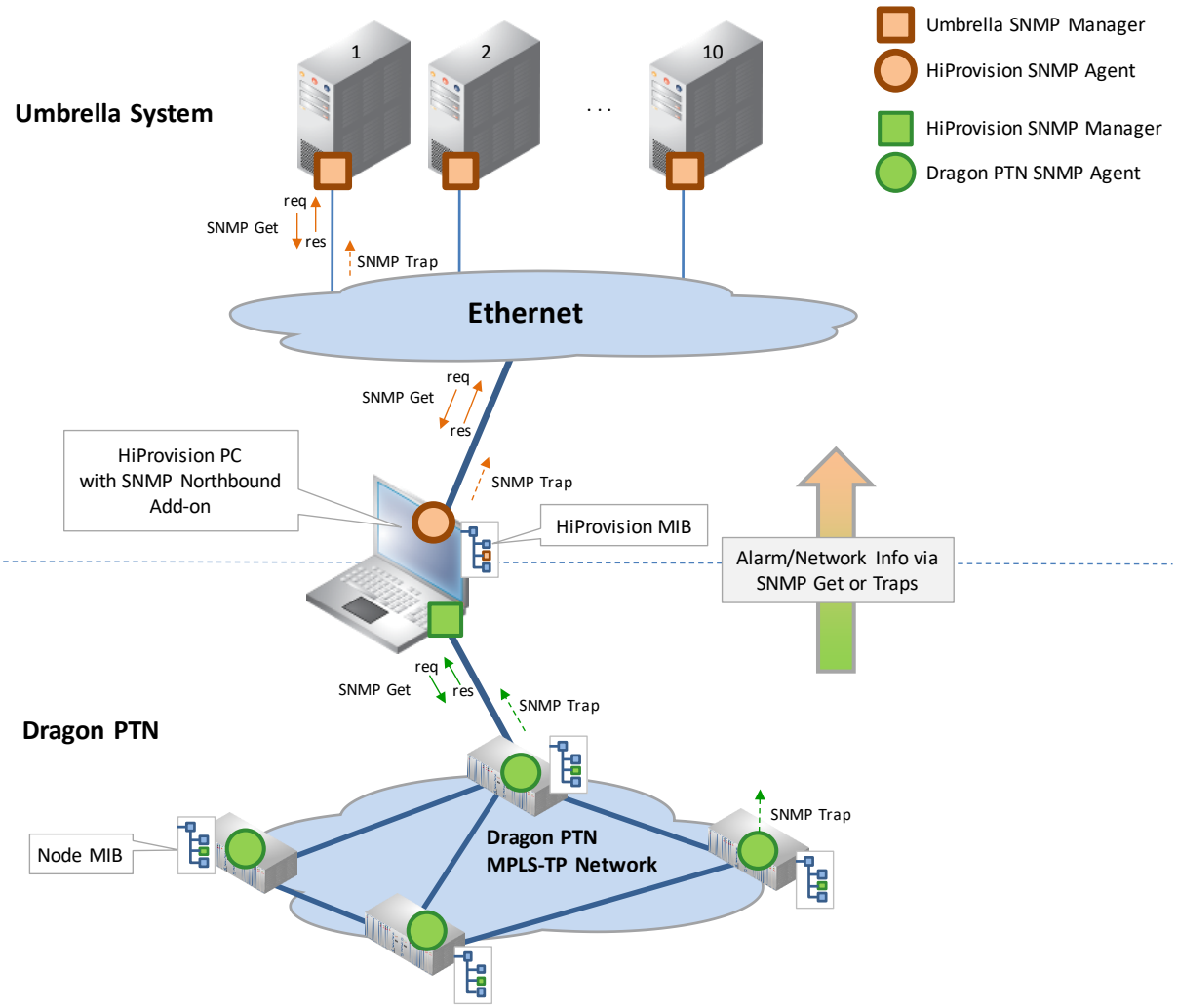


Figure 159 SNMP Northbound Example

17.4 Generic Reporting Engine

This add-on provides the possibility to generate different detailed Dragon PTN reports (template based), exported in different output formats. This add-on is by default available and does not require a license or voucher. A general Reporting Engine example can be found in the figure below. Find more information on this add-on in manual Ref.[25] in Table 1.

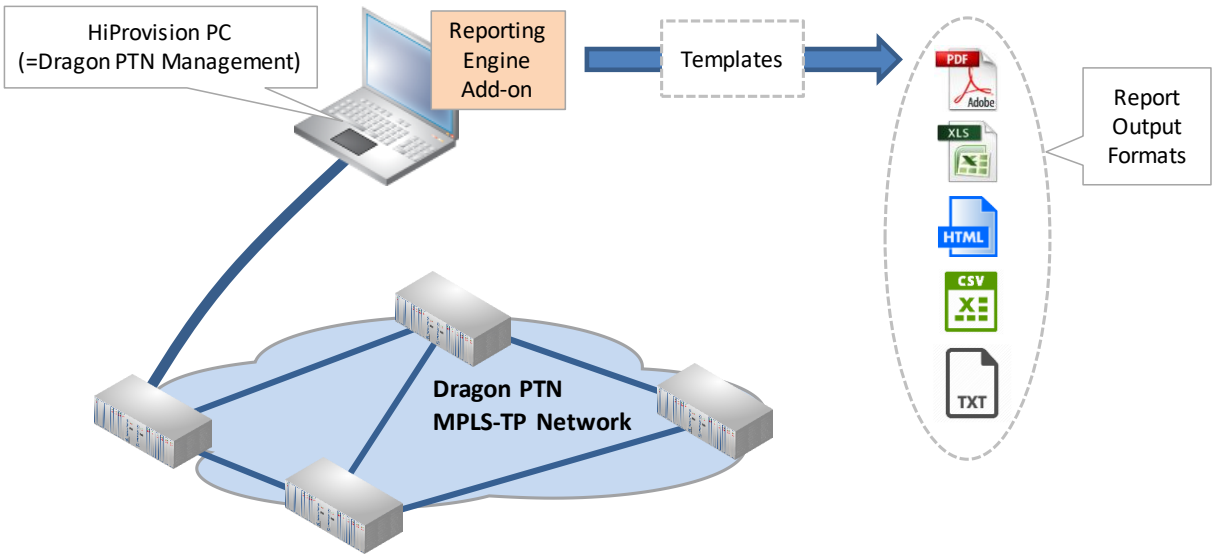


Figure 160 General: Reporting Engine

17.5 Permanent Monitoring

The Permanent Monitoring add-on allows advanced monitoring in the Dragon PTN network over a longer period of time of specific properties. This period of time is property dependent and depends on its sampling frequency. Extra alarming and trigger threshold values can be configured on these monitored properties. As a result, it is easier to detect trends in the network behaviour when monitoring/troubleshooting the network and act accordingly. Find more information on this add-on in manual Ref.[26] in Table 1.

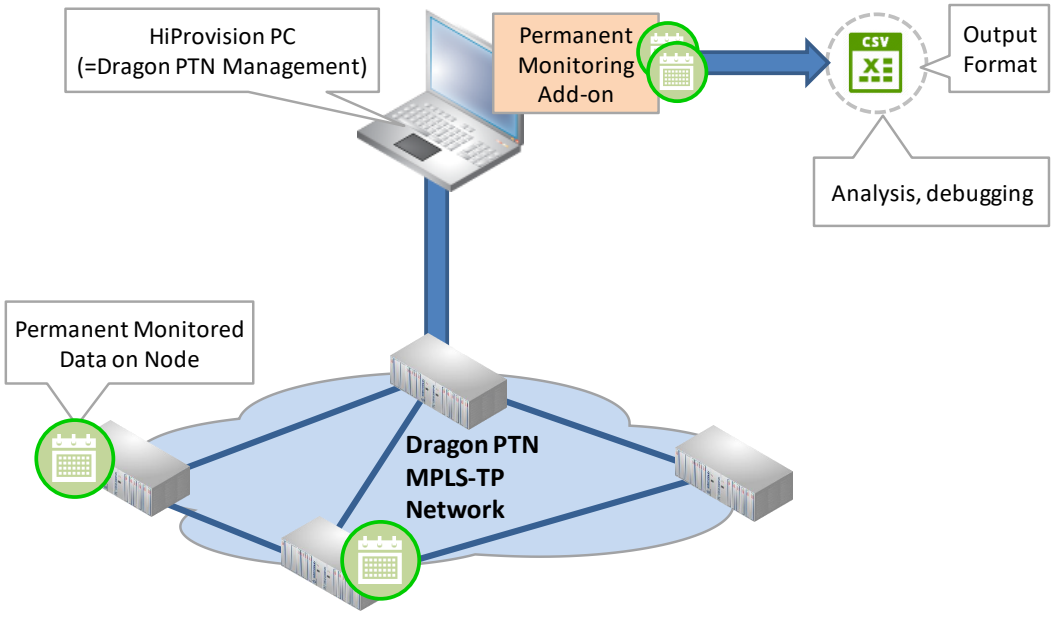


Figure 161 Permanent Monitoring Example

18. EXTERNAL DEVICES

18.1 General

It is possible in HiProvision to create new External Device Types in order to monitor third party devices. Also the links from Dragon PTN to these devices and the links between them will be monitored.

1. Create/Generate External Devices types: Dashboard → External Devices tile;
   - General flow: see §18.2;
     - Generate **Default** External Device Types delivered by Hirschmann Automation and Control GmbH (§18.3);
     - Create/Generate new **Custom** External Device Types (§18.4);
2. Create new devices based on this new type: Dashboard → Network Hardware tile → Devices, see §18.5;
3. Create Monitored Links via Dashboard → Network Hardware tile → Links, see §18.6:
   - between the Dragon PTN network and these devices;
   - between these devices themselves;
4. Configure Monitoring and Alarming of External Devices, see §18.7;
5. Backup & Restore External Devices, see §18.10;

18.2 Flow: Default External Devices/Custom External Devices

Hirschmann Automation and Control GmbH already delivers a default set of external devices types, that are common used, in the Dragon PTN Release package. An external device type is basically defined by a configuration structure (GenericDevices\Config*.xml files) and a picture (GenericDevices\Resources*.*).

See in the Dragon PTN release package → 02. Documentation\GenericDevices\Config which types are delivered by default.

If you still need other external devices types, it is still possible to create your own custom types.

The flow below shows the major steps for both the default and custom types.

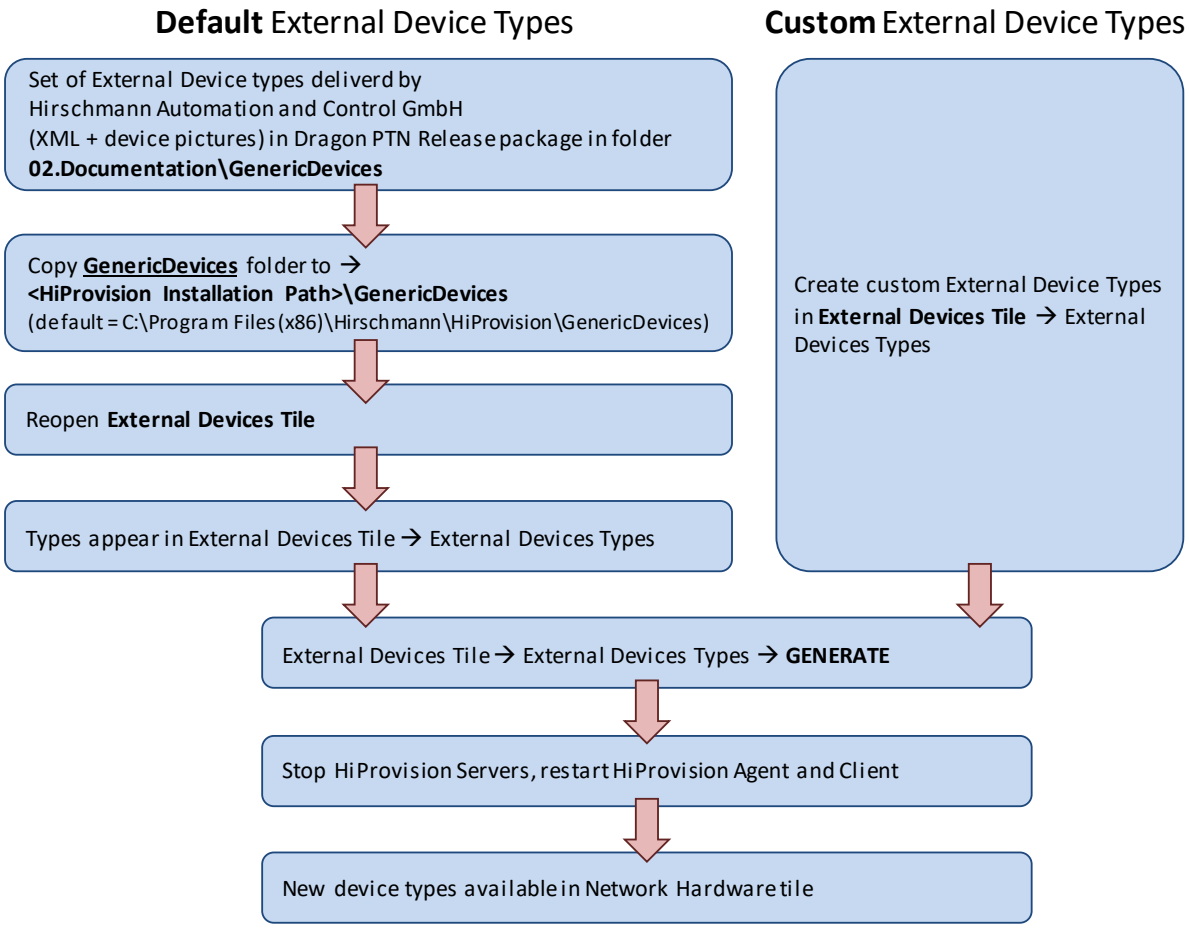


Figure 162 Flow: Default/Custom External Device Types

18.3 Generate Default External Device Types Delivered by Hirschmann Automation and Control GmbH

After copying the GenericDevices folder as described in previous flow, and reopening the External Devices tile, the default set of external device types will be listed. Existing custom made types are listed too. Only click the Generate button, stop the servers and restart the Agent/Client to make these types available in the network hardware tile. See also §18.5.

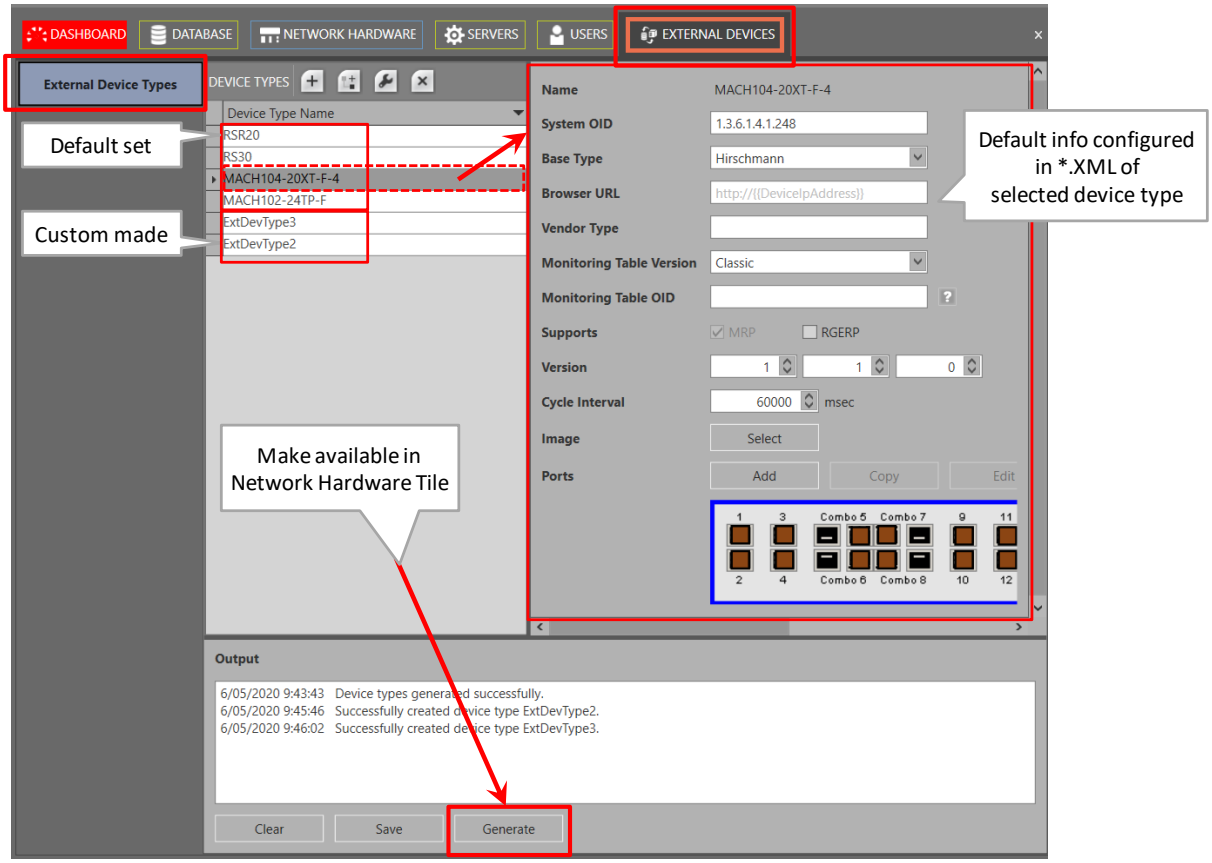


Figure 163 Generate Default External Device Types

18.4 Create/Generate New Custom External Device Type

1. Go to Dashboard → (Tools) External Devices → External Devices Types;

Figure 164 External Devices Types

Table 21 External Device Types: Menu Buttons

Button	Short Description
	Adds a new External Device Type.
	Copies the selected Device Type.
	Rename the existing Device Type. CAUTION: Renaming the device type automatically deletes all existing devices in HiProvision with the original Device Type Name.

	Deletes the selected Device Type. CAUTION: it also deletes all the configured devices of this type.

2. Click Devices Types → to add a device type. Fill out the device type in the figure below, e.g. ExtDevType4 and click OK;

CAUTION: Use correct spelling! Renaming afterwards automatically deletes all existing devices in HiProvision of the original Device Type Name.

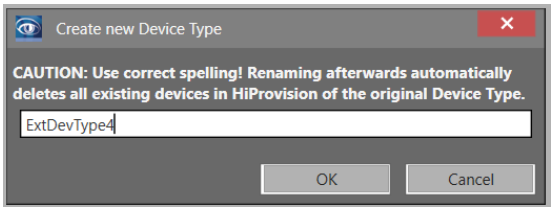


Figure 165 Create External Device Type

3. The window below is shown.

NOTE: More info on the fields below can be found in Table 22.

4. System OID: For custom alarming/monitoring: Fill out the System OID from the MIB file of the external device type, e.g. 1.2.3.4.5.6.7. More info on the System OID in §18.7.4 and Table 22.
5. Base Type: Assign the correct Base Type to the created device type.
   - Hirschmann: Select this for Hirschmann devices;
   - MiB2: Select this if your device is not a Hirschmann device, but supports MiB2;
   - Generic: Select this for any other device type;
   - In this example, select Generic.
6. Browser URL: Indicates the URL that HiProvision has to use to open the device. See Table 22.
7. Vendor Type: Fill out the vendor type (casesensitive!), which can be found in the Description field in the MIB of the device, e.g. Hirschmann Rail Switch Power Smart. See Table 22.
8. Monitoring Table Version (only visible for Hirschmann devices): see HirschmannMonitoringFamily in Table 22.
9. Monitoring Table OID (only visible for Hirschmann devices): See Table 22.
10. Supports (Optional): Check the protocol that your external device supports: MRP and/or RGERP. If MRP is checked, external devices connected to Dragon PTN will be detected for participating in the MRP protocol in Ref. [2Eth] in Table 1. If RGERP is checked, external devices connected to Dragon PTN will be detected for participating in the RGERP protocol in Ref. [2Eth] in Table 1.
11. Version (Optional): This can be used by the user for versioning, but it's not used by the Generic Device framework.
12. Cycle Interval (default = 60000 ms): indicates the interval in which HiProvision polls (via SNMP poll) and measures the external devices of this device type, See Table 22.
13. Click the Image Select button to assign an image to the device type;

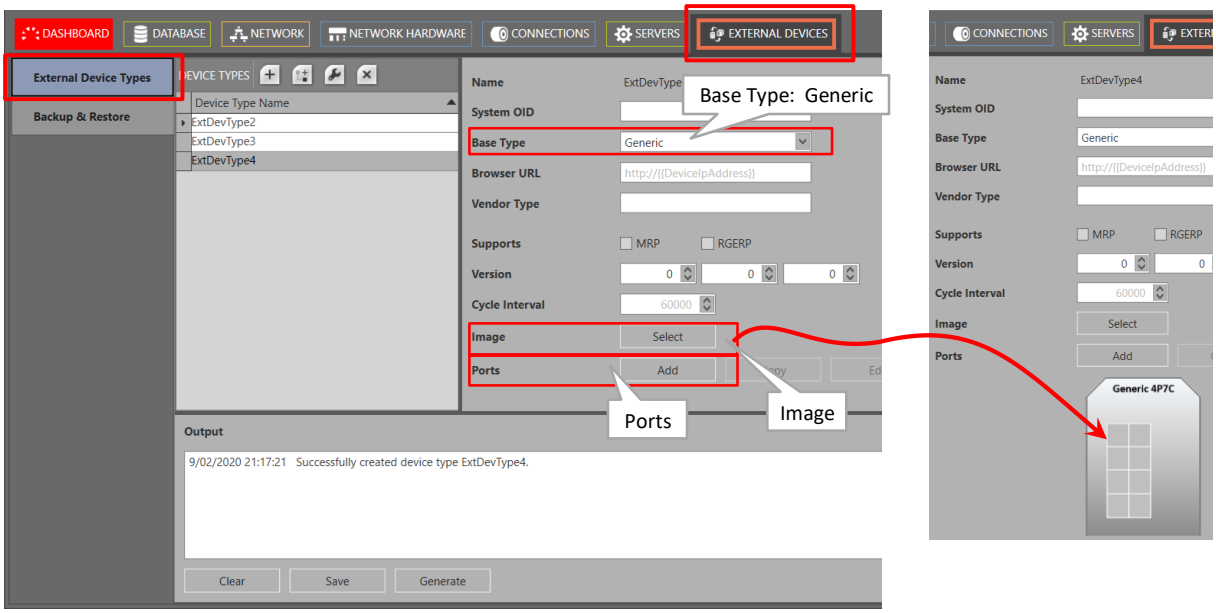


Figure 166 External Device Type: Base Type and Image

14. Click the Ports Add button to add a port. The window below pops up. The name is by default 'Port<n>'. <n> is a number that automatically increases with every port that you add. If desired, change and customize the Name and click Close.

    NOTE: Ports can be copied, edited and deleted via the Copy/Edit/Delete buttons.

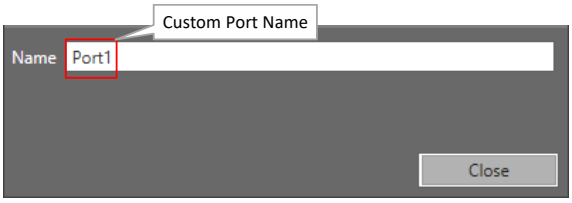


Figure 167 External Device Type: Add Port

15. A red border port icon will be placed somewhere onto the device type picture. Drag and drop the port icon into the right place on the corresponding port slot. Repeat these two steps until all ports are added and positioned in the correct port slot.

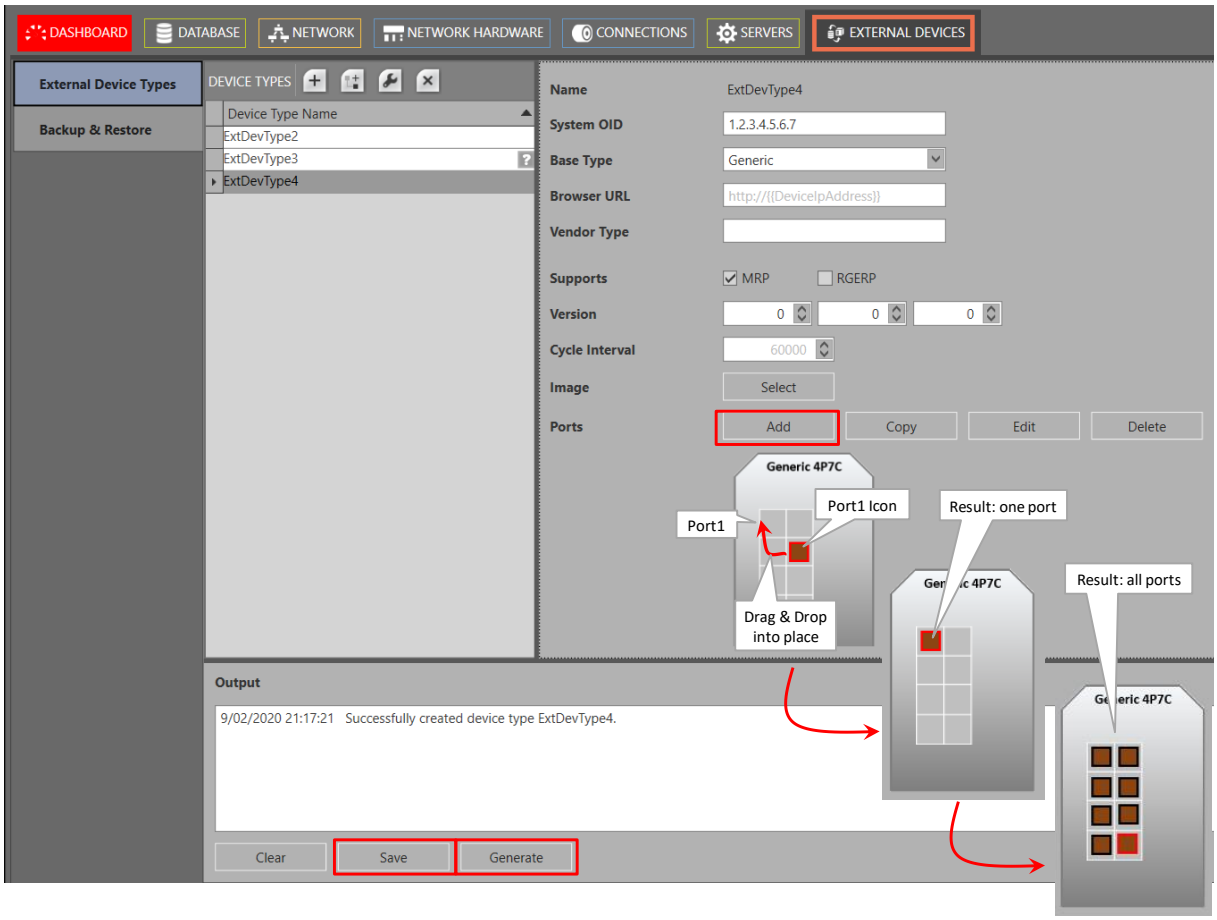


Figure 168 External Device Type: Drag & Drop Ports Into Place

16. Click the Save button to save your configuration and generate an XML file which might be needed later on to customize monitoring and alarming of properties;
17. Click the Generate button to make these new device types available later on in the Device Type list in the Network Hardware Tile;
18. To update the devices types list in the Network Hardware Tile: stop the Servers (Servers Tile → stop button) first, then shut down and restart both the HiProvision Client and Agent. The HiProvision Agent could be installed as program or service. See §3 to start/stop the HiProvision Agent;
19. Login in HiProvision and start the Servers via the Servers Tile → play button;
20. From now, this new type can be selected to create devices, see the following paragraph;

18.5 Create New External Device

1. Go to Network Hardware Tile → Devices →  ;
2. The newly created external device type shows up in the Device Type list and can be selected to create a new device for your network drawings. Fill out the Name, Type and ID and click the Create button.

Figure 169 External Device: New Device Type in Device List

3. Fill out the connection parameters below, allowing HiProvision to monitor this device.
   - Mgt. IP Address: the IP address of the external device;
   - SNMP V2:
     - checked (=default): use SNMP V2;
     - unchecked: use SNMP V3;
   - Community:
     - private (=default): indicates read-write access to the external devices, write access is required to set trap registrations on the external devices;
     - public: indicates read access only.

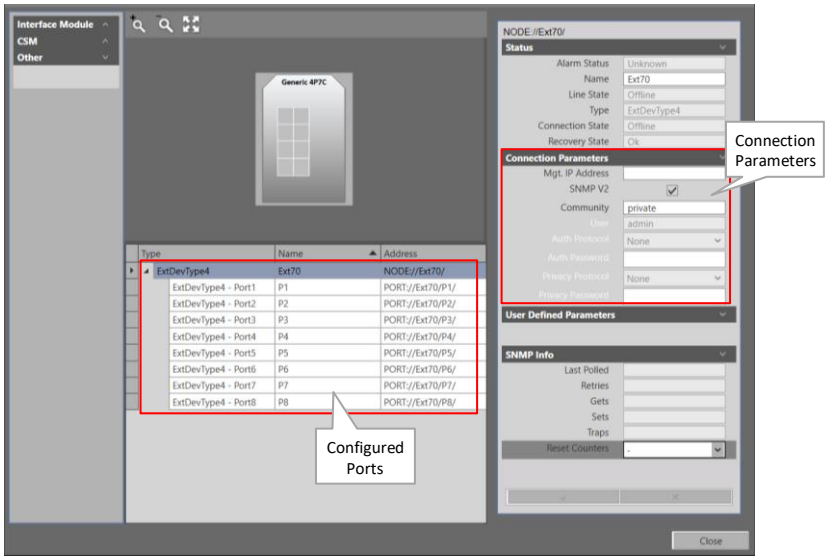


Figure 170 External Device: Connection Parameters

4. Click the Close button. The created external device appears in the Devices list.

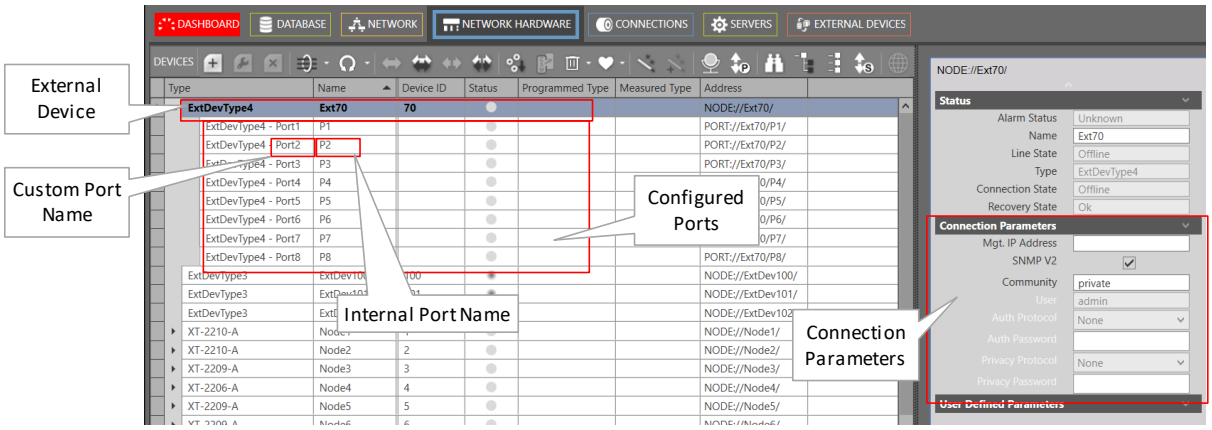


Figure 171 External Device: Created External Device

18.6 Linking External Devices to Dragon PTN

Prerequisite: make sure that the correct vouchers are purchased and the corresponding license pack has been installed. Note: for external device type ‘MIB2’, the ‘Generic Device’ voucher (prefix ‘S1’) is required. See also §4.2.

Once the External Devices have been created, they still have to be connected to the Dragon PTN network.

1. Make a physical connection between the External Devices and Dragon PTN via connecting the device to an Ethernet LAN port on an Ethernet IFM (4-GC-LW...) or an L2/L3 IFM in Dragon PTN;
2. Make sure that all the external devices are reachable via the filled out connection parameters §18.5. HiProvision cannot discover the external devices via the normal DCN path. Therefore, an extra physical path between a second NIC in the HiProvision PC and the external devices must be created, e.g. via an external network or via a configured Ethernet service over Dragon PTN, either routed or not.
3. Connect via clicking the buttons or in the network hardware tile;
4. Create a 'Monitored Link' between all the external devices and the Ethernet ports in Dragon PTN via Network Hardware Tile → Links → → Monitored Link
5. If the External Devices can be connected via HiProvision, the External Devices (=rounded icons) including the Monitored Links should turn green, indicating that all is OK (=no alarms). Any other color than green indicates some kind of alarm.

   NOTE: If there are problems with a link not coming up, verify the IfTableIndex of all the <port> tags in the XML file (see §18.7.4f). The IfTableIndex value of each <port> tag must match with its value in the MIB file of the external device. If the IfTableIndex is missing in the <port> tag, add it with the correct value from the MIB;

   NOTE: Performance between the HiProvision server and the external devices can be improved, see §21.9.

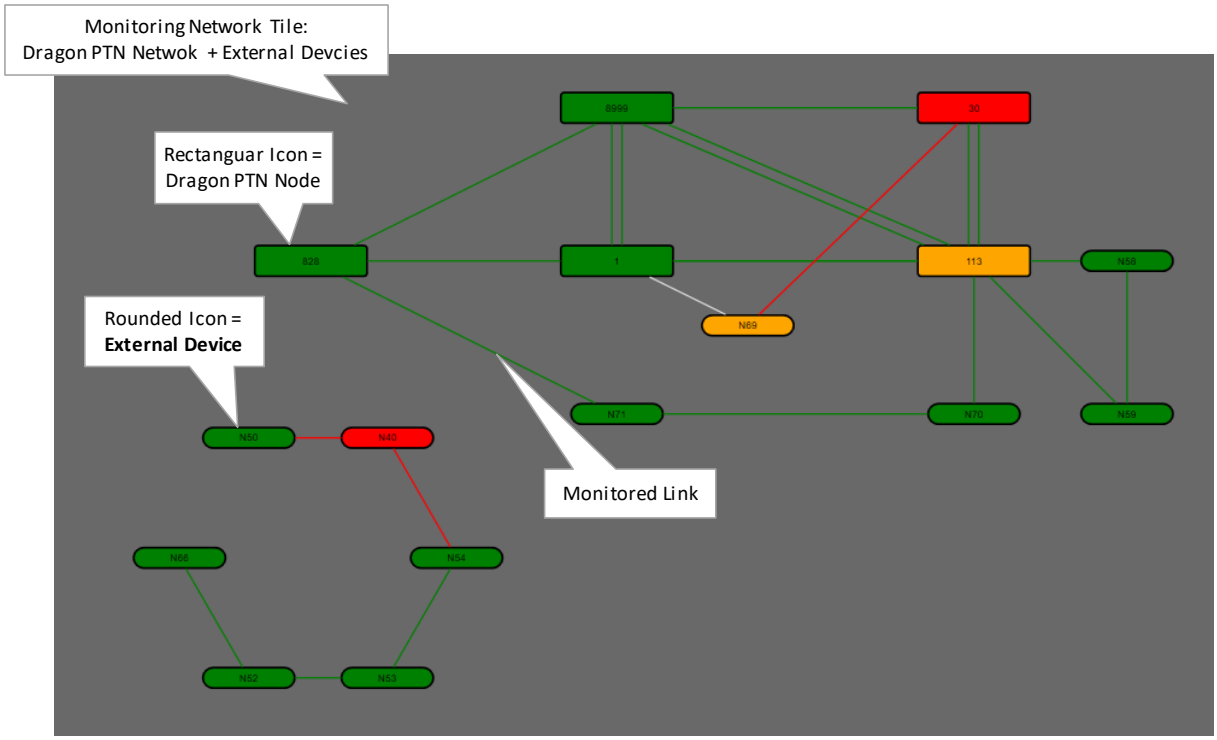


Figure 172 Dragon PTN Network + External Devices

NOTE: The Discovery function (see §2.5) is not relevant for External Devices.

18.7 Monitoring and Alarming of External Devices

18.7.1 Prerequisites

Make sure that HiProvision can connect to the external devices as described in previous paragraph.

18.7.2 General

The external device and port properties in the Network Hardware tile in the figure below are monitored in HiProvision via SNMP Poll and Trap (→SNMP Poll and Trap, see §18.7.3).

The default properties are always available in HiProvision. Custom properties in the 'User Defined Parameters' section can be added via customizing an XML file per external device type, not per device.

The MIB file of the external device type must be used as a source or reference to customize the XML file syntactically correct (→ XML file customization, see §18.7.4).

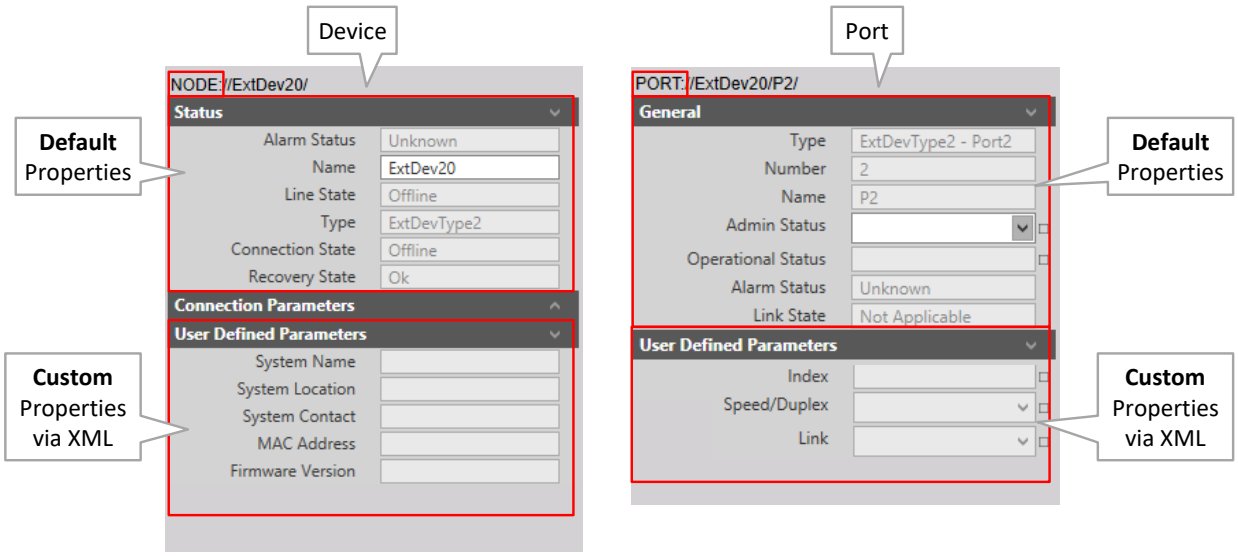


Figure 173 Default and Custom Properties

18.7.3 SNMP Poll and Trap

HiProvision combines the SNMP Poll and Trap techniques to monitor (=measure) the External Devices.

- SNMP Poll:
  - HiProvision starts the communication;
  - Periodic: HiProvision periodically requests, by default every 60 seconds, information from all the configured External Devices. This polling interval can be overruled by setting the 'CycleIntervalOverride' property of the root element in the XML (see Table 22) or by filling it out in §18.2;
  - Trap-based: HiProvision also re-polls the External Device that sends an SNMP trap to HiProvision. This extra poll will request all the parameter info from the device and not only the parameter that trapped;
  - Updates (the measured values off) the default and custom properties in HiProvision;
  - Polling cannot be disabled.

- SNMP Trap:
  - The external device starts the communication;
  - A message that External Devices immediately send to notify HiProvision when something occurs in the External Devices, e.g. port down, temperature too high, PoE disabled....;
  - Trap generation can be enabled/disabled per property (see §18.7.4j);
  - Does not influence a HiProvision device/port property directly, it triggers HiProvision to start a new poll cycle.

18.7.4 XML File Customization for Custom Properties

a. General

CAUTION: Do not forget to copy manually the External Device configuration files after a first HiProvision installation from the newly installed folder E.g.
C:\Program Files (x86)\Hirschmann\HiProvision\HiProvision V<version>\Documentation\GenericDevices
to the folder
C:\Program Files (x86)\Hirschmann\HiProvision\GenericDevices.

All External Device configuration files are placed in <HiProvision Installation path>\GenericDevices. This allows multiple HiProvision installations to reuse the same configuration files. These files are insensitive to HiProvision upgrades. The GenericDevices folder contains two subfolders:

- Config folder: contains all the XML configuration files, one XML file per device type. E.g. ExtDevType2.xml;
- Resources folder: contains the images for the External Device Types;

b. Step Overview

Follow the steps below to add custom properties for monitoring. All these steps are explained in more detail in the paragraphs below.

1. Open the MIB file (e.g. via a MIB browser) of your external device;
2. Decide which device and port properties you want to monitor;
3. Search these properties in the MIB file of the external device type;
4. Open the XML file in a text editor, e.g. Notepad;
5. Add the desired device properties in the XML file with respect to the syntax and case-sensitivity used in the MIB file;
   - Name;
6. Repeat the same for all the desired port properties. Note that you have multiple ports using the same properties. Use the IfTableIndex and RowIndex attribute to differentiate between ports;
   - Name, IfTableIndex, RowIndex, ;
7. Add a PropertyDefinition for each unique device and port property in the XML file;
   - Name, Oid, PropertyType, SnmpType, Alarm (optional);
8. Add an AlarmDefinition in the XML file for each unique PropertyDefinition that has PropertyType ="Reading";
   - Name, Severity, Message, Text, Help;
9. Add a TrapRegistration for each desired property that must send traps to HiProvision:
   - Oid, Value, RowIndex, SnmpType, Comment;
10. Save and Close the XML file;
11. Apply XML changes in HiProvision and the live Dragon PTN network, see §18.7.4k;

c. XML Structure Overview

CAUTION: XML file content is case-sensitive! XML tags must have the exact same case as used in the examples below. Properties, attributes, values must have the exact same case as used in the MIB files of the device type!

A basic XML file structure has following major parts (=root element + root child elements). The parts are still empty, but are explained further on;

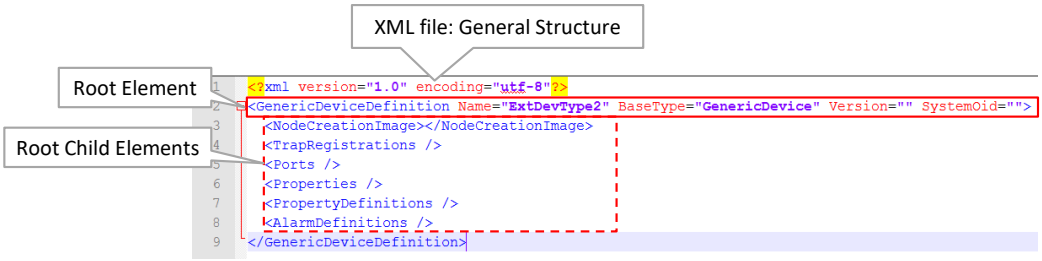


Figure 174 XML File: General Structure

- GenericDeviceDefinition: the root element of the External Device, having its own properties e.g. Name, BaseType... all its properties are listed in the table below;

Table 22 XML File: Root Element Properties

Root Element Property	Short Description
Name	The name of the device type.
BaseType	Must be one of the following values: Generic, Hirschmann.
Version (optional)	This can be used by the user for versioning, but it's not used by the Generic Device framework. Can be filled out as well via §18.2.
SystemOid	The root OID of the system in the external device MIB. This makes it easier to change it later in one place instead of numerous places in the XML. It's also used by the properties. For example, let's say that all external devices have a system name property with OID '{{SystemOid}}.1.1'. The first bit of the OID is usually the same and the second part differs per external device type. This way the property can be defined in a generic way. The {{SystemOid}} pattern is replaced at runtime by the actual SystemOid of the device. Can be filled out as well via §18.2.
HirschmannMonitoringFamily	Only visible for Hirschmann devices: - Classic (=default): uses OID 1.3.6.1.4.1.248.14.5.3 as reference monitoring OID - HiOS: uses OID 1.3.6.1.4.1.248.11.40.1.1.1 as reference monitoring OID Can be filled out as well via §18.2.
MonitoringTableOid	For Hirschmann devices: OID required to fill out the Hirschmann MRP Monitoring tables (see Ref. [2Eth] in Table 1) in HiProvision. Only use this field if the OID is different from the Classic or HiOS OID defined via the HirschmannMonitoringFamily parameter. Can be filled out as well via §18.2.
CycleIntervalOverride (optional)	Generic devices have a slow polling interval combined with updates when traps are received (trap-based polling). By default the cycle interval is 60000 ms (=60 seconds). Use this property to override this interval. The value must be in milliseconds. Can be filled out as well via §18.2.

Root Element Property	Short Description
TrapReceivePortOverride (optional)	Traps are received on port 6021 and 6022 by default. Some Generic Devices send traps to other ports (162 by default). Use this attribute to make HiProvision listen on extra ports.
SupportsMrp (optional)	If the value=True, then external devices of this device type support MRP. Can be filled out as well via §18.2.
SupportsRgerp (optional)	If the value=True, then external devices of this device type support RGERP. Can be filled out as well via §18.2.
BrowserUrl (for all device types) (optional)	Indicates the URL that HiProvision has to use to open the device. By default, this is `http://{{DeviceIpAddress}}`, this is already OK if Mgt. IP Address has been filled out in Network Hardware Tile → Select External Device → Connection Parameters → Mgt. IP Address. If this field is not filled out, you can still fill out an IP address in the XML file in this field. See also §18.9.
VendorType (optional)	This field is used to verify if the external device type in the live network matches the device type configured in HiProvision. Fill out the vendor type (casesensitive!) which can be found in the Description field in the MIB of the device, e.g. Hirschmann Rail Switch Power Smart. The vendor type filled out or configured in HiProvision must be the same as the vendor type of this device in the live network. If this is different, an alarm will be raised in HiProvision.

All the child elements of the root element are described in the table below.

Table 23 XML File: Root Child Elements

Root Child Element	Short Description
NodeCreationImage	The file name (without extension) of the image for this device type. The image will be used in different HiProvision screens. Do not change manually, only change images via the wizard!
TrapRegistrations (optional)	If you want to receive traps from a device of this type, certain OIDs have to be set on the device (such as the IP address of HiProvision). The trap registrations are a list of all OIDs that have to be set to certain values for a device of this type to enable the traps that you're interested in.
PropertyDefinitions	Definitions of all the properties that you want to monitor on this device and its ports. The definitions include things such as OID, SNMP type, display name, possible min and max value, enum values, translations, ... Adding a property here, does not automatically add it to the device type. You still have to reference it in the Properties section of the device or the ports. - IntPropertyDefinition: the property is numeric, e.g. portStatusIndex; - StringPropertyDefinition: the property is not numeric but a string, IpAddress, MacAddress, ..., e.g. systemName; - EnumPropertyDefinition: the property has a set of values e.g. portStatusLink (value1 = up; value2 = down);
AlarmDefinitions	The alarm definitions for the properties defined in the PropertyDefinitions section that can raise alarms. An alarm definition includes things such as the severity, the message or help texts and possible translations.
Properties	The properties that you want to monitor on the device level (=not port level). Each of these properties has its own PropertyDefinition.
Ports	The list of port definitions for this device type. Every port has a name, a location (=XY coordinates) and a list of properties that you want to monitor. Each of these properties has its own PropertyDefinition.

d. XML: Device Picture

- NodeCreationImage: the filename of the device image (in the Resources folder) after generating the External Device in via the Generate button. Do not change manually in the XML, only change images via the wizard!

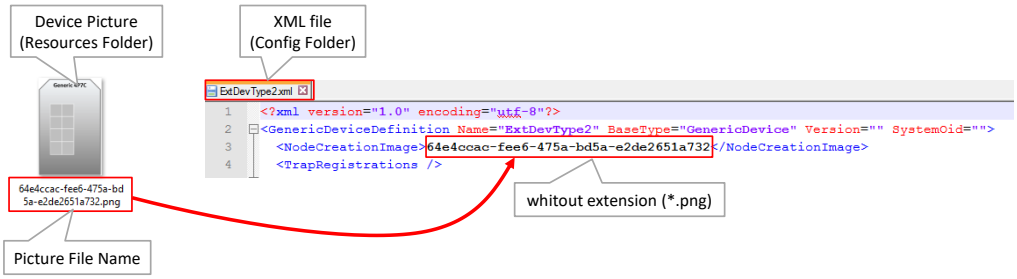


Figure 175 External Device Picture In XML File

e. XML: Device Properties

A device has multiple properties and each unique property in the XML file must have a Property Definition, referred by Name. If the property must be able to raise alarms, set the PropertyType ="Reading" in the Property Definition and add an Alarm Definition, see further. If no alarms are needed, set PropertyType ="Indication".

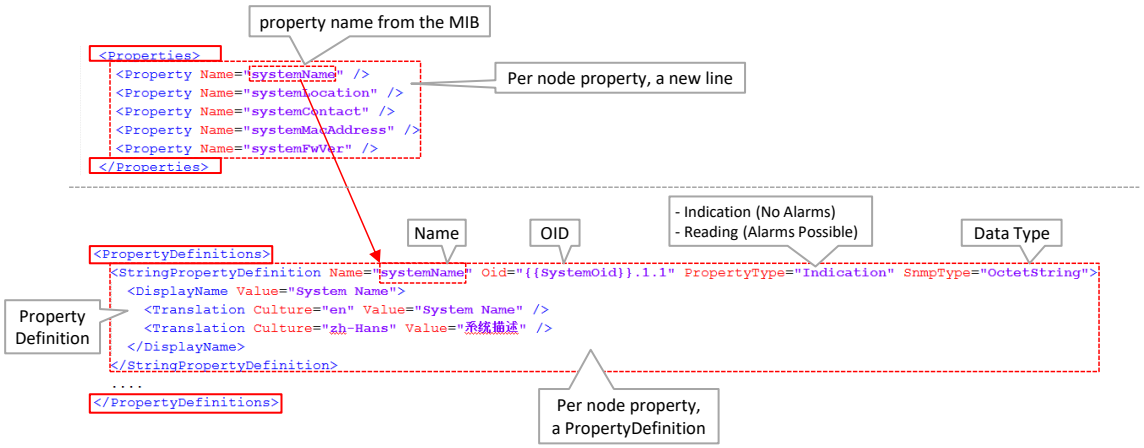


Figure 176 XML: Device Properties/Property Definition

f. XML: Port Properties

A port has multiple properties. Each unique port is identified by the value of the IfTableIndex attribute in the <port> tag. Each unique property in the XML file must have a Property Definition as well. If the property must be able to raise alarms, set the PropertyType ="Reading" in the Property Definition and add an Alarm Definition, see further. If no alarms are needed, set PropertyType ="Indication".

A port contains the following attributes:

- Name: the name of the port;

- RelativeLocation: the XY location of the port icon on the device Image, the port icon is used to create links in the link wizard. Valid values range from -0.5 to 0.5 in both x and y direction. (0, 0) would be the center of the image, while (0.5, -0.5) would be the upper right image corner;
- IfTableIndex: the index in the IF table in the MIB. This value identifies the correct port. This value is used as RowIndex value in the <property> tag. Make sure this value is filled out for each port.

A port has the following child elements:

- Properties: a list of properties to monitor on this port. Every property refers to a property definition by name. Every property must have a RowIndex to differentiate between ports with the same properties. The RowIndex can contain the {{IfTableIndex}} pattern, in which case it is replaced by the value of the IfTableIndex property on the port definition.

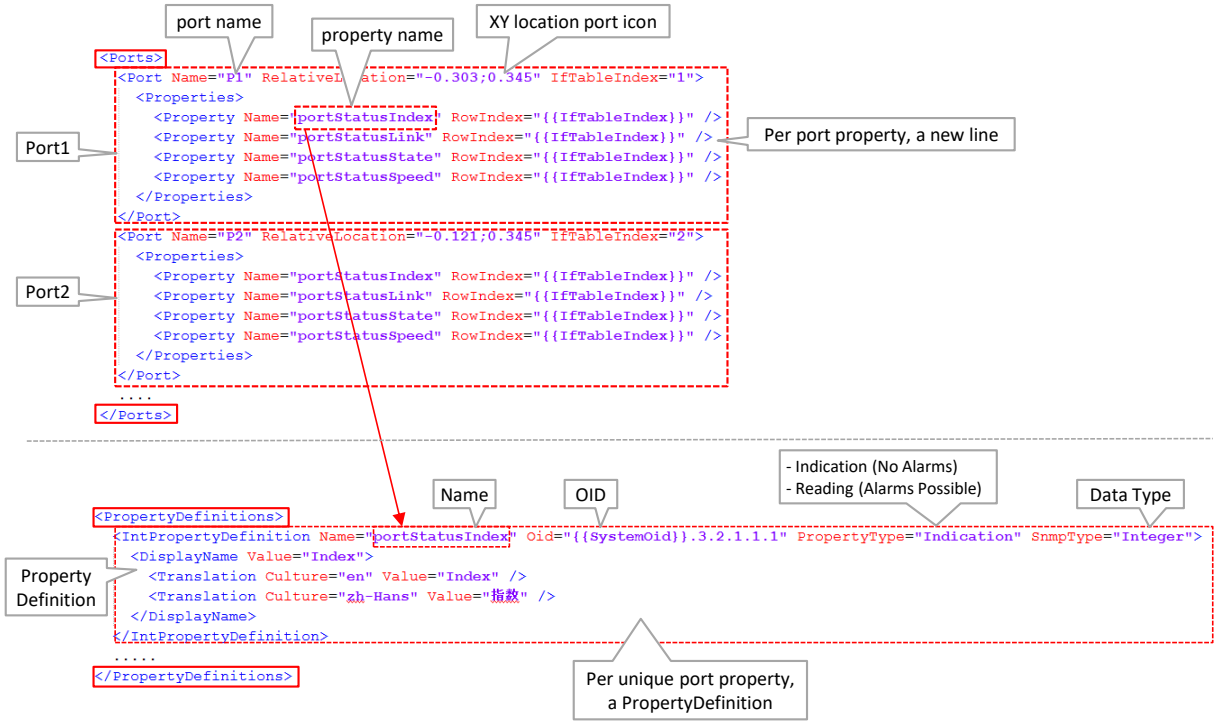


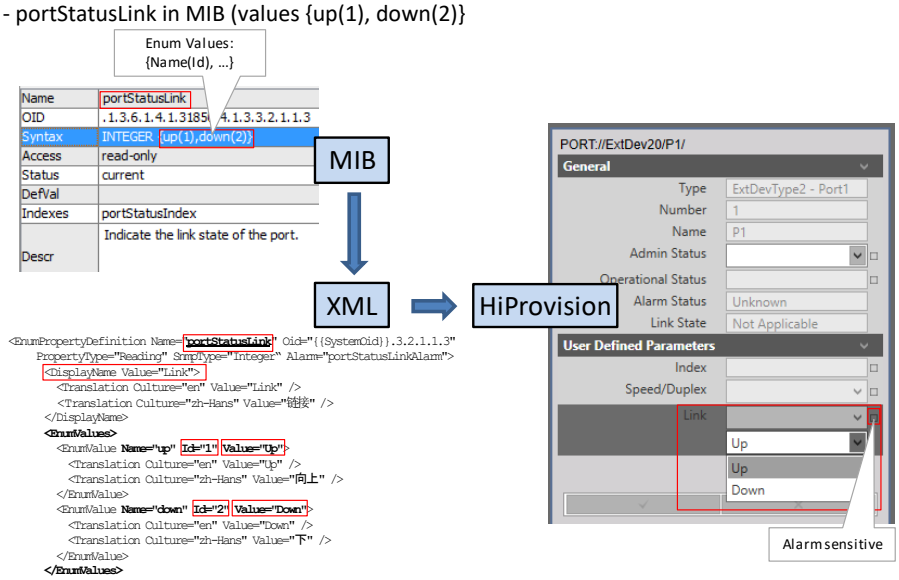
Figure 177 XML: Port Properties/Property Definition

g. XML: Property Definitions

There are 3 types of property definitions:

- IntPropertyDefinition: the property is numeric, e.g. portStatusIndex;
- StringPropertyDefinition: the property is not numeric but a string, IpAddress, MacAddress, ..., e.g. systemName;
- EnumPropertyDefinition: the property has a set of values e.g. portStatusLink (value1 = up; value2 = down);

Table 24 XML File: PropertyDefinition Attributes

Attribute	Short Description
Required	
Name	The name of the property in the MIB. This is used to refer to it, in the Properties section of the device type or the Properties sections of the ports (see below).
Oid	The full OID in the MIB. It is advised to replace the root OID part with the {{SystemOid}} variable for a better overview and more consistency in your XML file. Example: You can use: <GenericDeviceDefinition Name="ExtDevType2" BaseType="GenericDevice" **SystemOid="1.2.3.4.5"**> <IntPropertyDefinition Name="portStatusIndex" Oid="**1.2.3.4.5**.**1.2**" PropertyType="Indication" SnmpType="Integer"> or (better, advised): <GenericDeviceDefinition Name="ExtDevType2" BaseType="GenericDevice" **SystemOid="1.2.3.4.5"**> <IntPropertyDefinition Name="portStatusIndex" Oid="**{{SystemOid}}**.**1.2**" PropertyType="Indication" SnmpType="Integer">
PropertyType	- Indication: does not raise alarms - Reading: can raise alarms
SnmpType	The data type definition, it has to match a value in 'XML SnmpType' column in Table 25.
Alarm (required for 'Reading' properties)	A reference to the alarm definition in 'AlarmDefinitions' that has to be used when this property raises an alarm.
Optional	
DefaultValue	The default value used by 'Reading' properties to check if an alarm has to be raised. A string for string properties, an integer for integer and enum properties.
MinimumValue (only for integer properties)	The minimum value used by 'Reading' properties to check if an alarm has to be raised.
MaximumValue (only for integer properties)	The maximum value used by 'Reading' properties to check if an alarm has to be raised.
EnumValues (only for enum properties)	A set of values (=EnumValues). Every enum value has a name, an id, a value and optional translations. The **Name** and **Id** have to match the value list in the MIB description. How the value is displayed in HiProvision can be tuned via the **Value** attribute and/or Translation lines. Example: The port status can be up or down: - portStatusLink in MIB (values {up(1), down(2)} 

h. Mapping: MIB Syntax / XML SnmpType

Table 25 Properties: Mapping: MIB Syntax / XML SnmpType

MIB Syntax	XML SnmpType	Short Description
OCTET STRING, DISPLAYSTRING	BitString	String that has only 0 and 1, that represents binary data
OCTET STRING, DISPLAYSTRING	BitStringToInteger	String containing a bit-representation of an integer value (ex: "10111101001")
Counter32	Counter32	Unsigned 32-bit counter.
Counter64	Counter64	Unsigned 64-bit counter
Gauge32	Gauge	SNMP gauge
OCTET STRING	HexOctetStringInteger	A hex octet string (in SNMP) representing a specific elapsed time in milliseconds
OCTET STRING, DISPLAYSTRING	HexString	String containing a hexadecimal value (ex: "f044d2")
INTEGER	Integer	SNMP integer
IPADDRESS	IpAddress	SNMP ipaddress
MACADDRESS	MacAddress	SNMP macaddress
Link to other table	ObjectIdentifier	Value containing an oid (ex: 1.2.3.4.5.6)
OCTET STRING	OctetString	SNMP normal string
OCTET STRING	OctetStringDateTime	An octet string (in SNMP) representing a DateTime (formatted as YYYYMMDDHHMMSS)
OCTET STRING	OctetStringIpAddress	An octet string (in SNMP) representing an IP address (formatted as xx.xx.xx.xx)
OCTET STRING	OctetStringToVersion	Provides a conversion from OctetString to version
TimeTicks	TimeTicks	SNMP time
TruthValue	TruthValue	SNMP boolean
Unsigned32	Uinteger	SNMP unsigned integer.
Unsigned32	UintEnum	Provides a conversion from Uint for enums

i. XML: Alarm Definitions

An alarm definition must be added or created per PropertyDefinition that must be able to raise alarms (PropertyType = "Reading"). The alarm definitions below define how the alarm looks when it appears in the Alarms tile in HiProvision. See §18.7.5 to find out when an alarm is really raised.

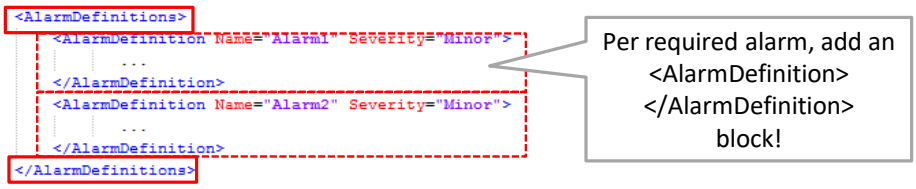


Figure 178 XML: AlarmDefinition Block per Alarm

The Alarm attribute in the PropertyDefinition must refer to the name in the AlarmDefinition, see an example below. Also add a severity.

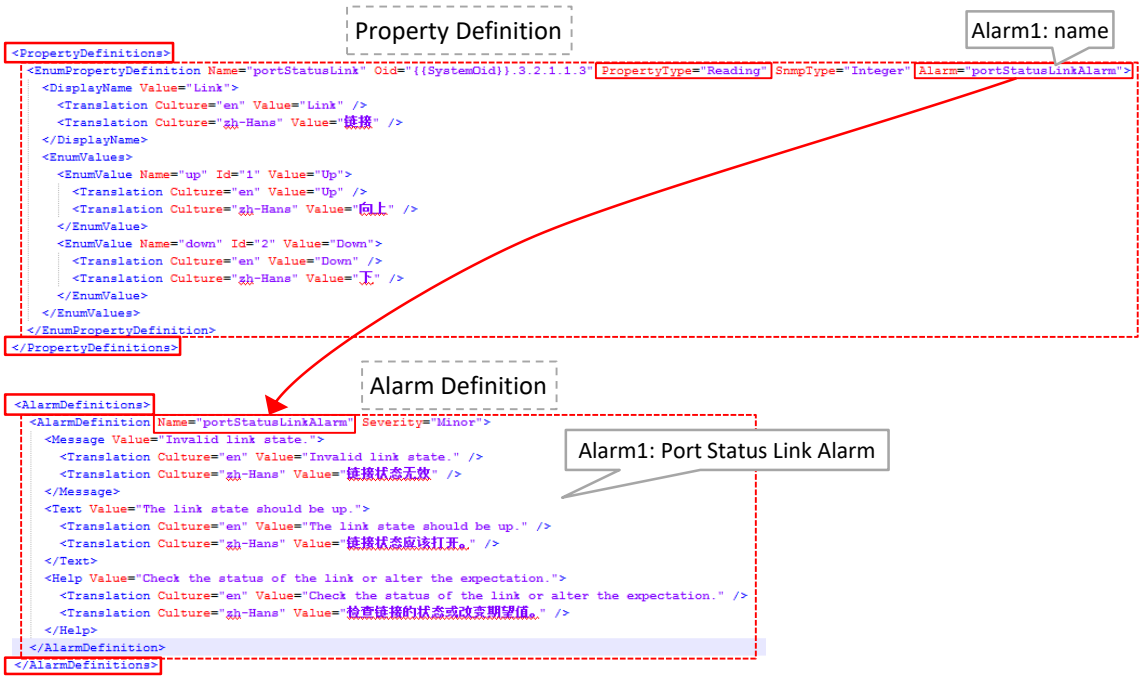


Figure 179 Alarm Definitions Example

An alarm definition contains the following attributes:

- Name: the name of the alarm definition. This is used to refer to it by the property that uses this alarm data. See the alarm attribute on a property definition;
- Severity (optional) (default = Minor, values [Warning, Minor, Major, Critical]: the alarm severity.

An alarm definition has the following child elements:

- Message: the alarm message or title in the Alarms tile in HiProvision. Translations can also be provided. Culture indicates the language code: en = English, zh-Hans = Chinese; es = Spanish, de = German, pl =Polish;
- Text: the alarm text or body in the Alarms tile in HiProvision. Translations can also be provided.
- Help: the help text in the Alarms tile in HiProvision. Translations can also be provided.

j. XML Trap Registrations

HiProvision can receive traps from external devices. A received trap does not influence directly a property in HiProvision, but it triggers HiProvision to poll the external device again (=trap-based poll). These poll results can influence the properties in HiProvision.

So if you configure for example a trap for disabling PoE on a port, make sure that you also configure a PoE property and PropertyDefinition in the XML for polling purposes. Not doing so, and receiving a trap for a PoE disabled port, will initiating a new poll and not influencing any custom property/alarms in HiProvision.

To make HiProvision receive traps from a device of this device type, the actions below must be performed on the external device itself.

CAUTION: Setting trap registrations (=write action) on the external device itself can be done via the XML file. It impacts ALL the external devices of this device type at once. If you don't want this (e.g. you only want to impact some devices and not all), do not use the XML for trap registrations. Instead, configure each external device individually e.g. via a local configuration tool or web interface on the external device.

- Disable trap server;
- Initialize trap operations:
  - traps have to be enabled;
  - set up the trap agent:
    - the HiProvision server IP address has to be filled out in the value field of the IpAddress trap registration;
    - the community and version has to be set;
- Configure the trap events via the OID in which you are interested. There is no strict mapping in the XML file required between a registered trapped property and a PropertyDefinition.
- Enable trap server;

NOTE: These steps are device type specific and could differ for other device types;

NOTE: HiProvision receives traps by default on port 6021 and 6022. An extra port to which HiProvision must listen can be added via the 'TrapReceivePortOverride' attribute in the root element, see Table 22.

Find an XML example below with trap registrations.

Figure 180 XML: Trap Registrations

A trap registration contains the following attributes:

- Oid: the full OID in the Mib. It is advised to use the {{SystemOid}} pattern in combination with the SystemOid attribute on the root element;

- Value:
  - 1 = enabled, up or... depending on the property, see MIB;
  - 2 = disabled, down or... depending on the property, see MIB;
  - 3 = both '1' and '2'. Example: if value="3" is set for the Link Status property, then HiProvision will receive a trap when the link goes up on that specific port and another trap when the link goes down;
  - RowIndex: the row index is required when the OID of the trap refers to a table in the MIB. Use the row index to select the desired row from the table. If the OID does not refer to a table, the RowIndex attribute must be empty or omitted;
  - SnmpType: the SNMP Type or data type, has to match a value in the XML SnmpType column in Table 25;
- Comment (optional): not used by the Generic Device framework but it's handy for the user to comment and remember what each setting does.

k. Apply XML File Changes to Live Network

Once you have changed, optimized and saved your XML file, follow the steps below to apply these changes on the external devices in the live network:

1. (Skip this step when HiProvision is already running) Start HiProvision Agent (see §3) + HiProvision Client;
2. (Skip this step when the External Devices tile is already closed) Close the External Devices tile;
3. Open the External Devices tile;
4. Press the Generate button to configure the XML file input of ALL external device types, into HiProvision;
5. In the Servers tile, stop Servers (not just close HiProvision);
6. Close HiProvision Client and HiProvision Agent (see §3);
7. Restart HiProvision Agent (see §3) and HiProvision Client;
8. The XML changes that should cause changes in the external devices in the HiProvision GUI (e.g. new properties on port or node level, etc...) should be visible now in the Network Hardware Tile via node properties, port properties etc...
9. Make a Connect in HiProvision. Trap registration in the external devices will be done just after the connect;
10. As of now, everything should be up and running. Properties should be monitored according to the configured poll/trap settings, and alarms should be raised when properly configured.

18.7.5 Raising Alarms

Alarms are raised when HiProvision monitors and detects mismatches on alarm sensitive properties. Alarm sensitive properties have a little square box, see §9.3.

Custom properties, created via XML, must have a PropertyDefinition with the attribute PropertyType ="Reading" to be alarm sensitive.

18.8 Usage of External Devices in HiProvision

External Devices appear in HiProvision on the following places:

- Dashboard → Tools → External Devices Tile;
- Dashboard → Configuration → Network Hardware Tile: Devices + Monitored Links;
- Dashboard → Configuration → Protocols → MRP;
- Dashboard → Monitoring → Network Tile;
- Dashboard → Monitoring → Alarms Tile;
- Dashboard → Administration → Licenses Tile;

Not Relevant for External Devices:

- Discovery, Tunnels, Services (Wizards), Performance counters, Protocols;

18.9 Open External Device in Web Browser via HiProvision

Go to on the locations below:

- Dashboard → Network Hardware
- Dashboard → Network → Devices Tab
- Dashboard → LNM → Devices

And select your external device in the Devices list → Click the  button to open the web browser of the external device.

The filled out IP address in the Mgt. IP Address field will be used to open the web browser of the external device. Via the web browser, it is possible to configure your external device.

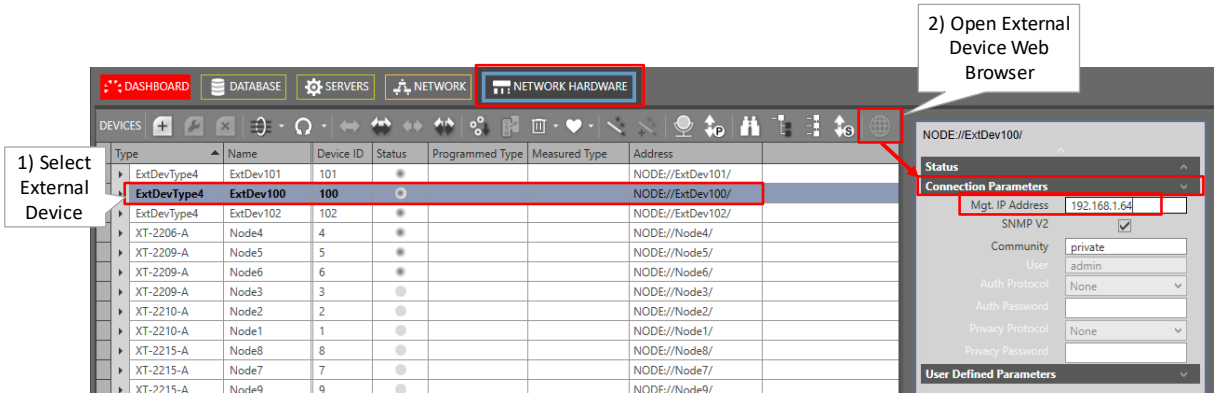


Figure 181 External Device in Web Browser

18.10 Backup & Restore (currently not supported)

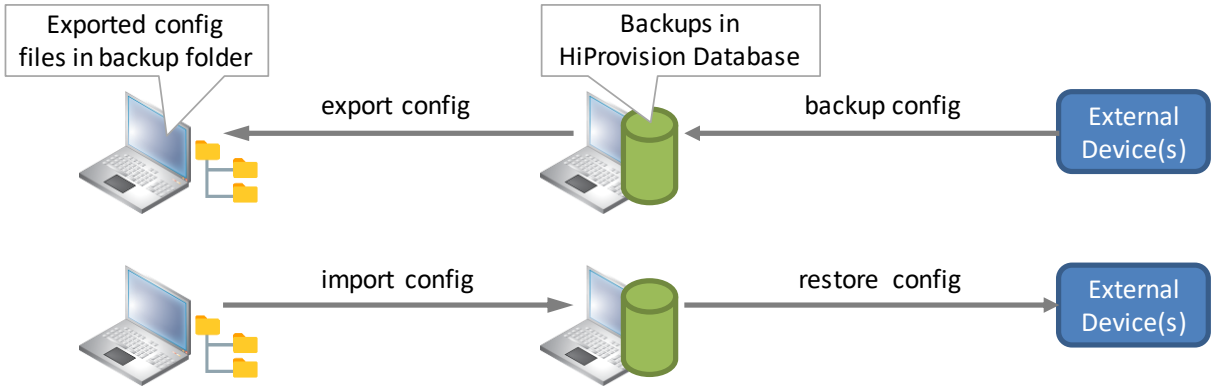


Figure 182 Backup & Restore Flows

19. SCRIPTING

19.1 General

Via scripting, it is possible to do bulk operations (e.g. change 100 port settings at once) into the database which will save you some time on configuration.

It allows to bypass the HiProvision Client to add/modify/delete multiple Dragon PTN network elements, properties, etc… in no time. Scripting can be done via interactive scripting or via script files.

CAUTION:
- It is strongly advised that scripting is only used by advanced and trained Dragon PTN/HiProvision users. Only use it at your own risk!
- All commands influence the offline configuration in HiProvision, only if you use the 'Load' command, changes are pushed into the live network!
- Possible scripting errors will not automatically be handled by scripting itself. You have to monitor scripting errors yourself, and solve them later on accordingly by adapting the failed scripting commands. Possible scripting errors are shown in the Python window. For scripting actions on wizards, possible scripting errors are shown after the Finish() command, for all the other scripting actions, possible errors are shown immediately after the single scripting command.

19.2 Interactive Scripting

Prerequisite: The HiProvision Servers must have been started.

CAUTION:
- All commands are case-sensitive!
- Provide a custom scripting username/password (see Ref. [15] in Table 1).

1. Start Python (=scripting language used by HiProvision) via clicking the file below:
   ▶ `<HiProvision Installation path>\HiProvision_V<version>\scripting\python.cmd`

2. The window below pops up. Fill out following commands and ENTER each command. The last command must result in 'success'.
   - `from HiProvisionScript import *`
   - `Authenticate("<username>::<password>")`

   NOTE: **`scripting`** is the default <username> and <password>. It should be removed and changed by your customized scripting username and password (via User Management, see Ref. [15] in Table 1) for security reasons.

Figure 183 Interactive HiProvision Scripting via Python

3. From now on, it possible to enter scripting commands.
4. Command examples can be found in §19.3.3. A full command list can be found via §19.5.

19.3 Script Files

19.3.1 Writing a Script File

NOTE: The '#' character without the quotes can be used to write comments or comment out a command;

1. Open Notepad (or another text editor).
2. The script file must always start with the commands below:

```
from HiProvisionScript import *     # required to import HiProvision scripting extension into Python
Authenticate("<username>::<password>")  # required to authenticate before scripting can be done
```

   NOTE: **`scripting`** is the default <username> and <password>. It should be removed and changed by your customized scripting username and password (via User Management, see Ref. [15] in Table 1) for security reasons.

3. Next, add your own commands in the script file. Command examples can be found in §19.3.3. A full command list can be found via §19.5.

4. After adding all your commands, save the file as a '*.py' in the folder below:
   `<HiProvision Installation path>\HiProvision_V<version>\scripting\`

5. Execute your scripting file as described in next paragraph.

19.3.2 Executing or Importing a Script File

Prerequisite: The HiProvision Servers must have been started.

CAUTION: All commands are case-sensitive!

1. Start Python (=HiProvision scripting tool) via clicking the file below:
   - `<HiProvision Installation path>\HiProvision_V<version>\scripting\python.cmd`

2. The window below pops up. If your scripting file is named for example `myscripts.py`, fill out following commands and ENTER each command to import the file.
   - `from execfile import *`
   - `execfile("myscripts.py")`

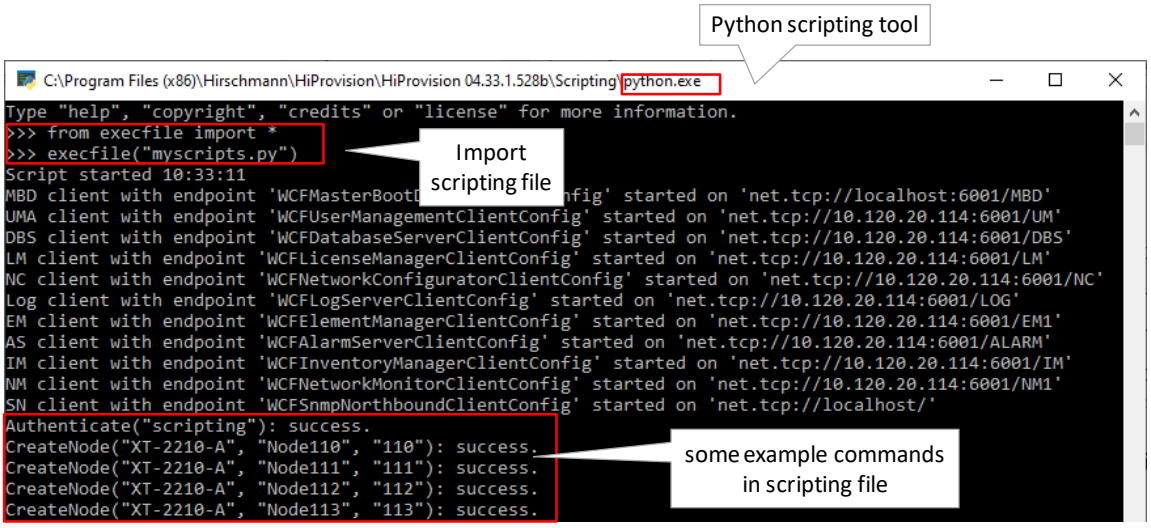


Figure 184 Importing Script File via Python

3. After successful import, can you can see the import results or changes in your HiProvision.

19.3.3 Export HiProvision Database Into Script File

Sometimes it is very useful to export your HiProvision database into a script file. Especially when you are planning to do some bulk-changes into your network (e.g. change a port setting on multiple ports at once). This exported file gives you all the scriptlines that match your database.

Use the listed commands below in Python to export the HiProvision database into `<HiProvision Installation path>\HiProvision_V<version>\scripting\MyExport.py`.

```
from HiProvisionScript import *
Authenticate("<username>::<password>")
ExportNetwork("./MyExport.py")
```

NOTE: **`scripting`** is the default <username> and <password>. It should be removed and changed by your customized scripting username and password (via User Management, see Ref. [15] in Table 1) for security reasons.

You could copy-paste some exported scriptlines from this exported file into a new script file e.g modify_db.py, and for example modify some port settings, save the file and import (§19.3.2) the new modify_db.py file into the live network.

CAUTION: the exported file (via the ExportNetwork command) is not suited to import the entire file again to build up a new database from scratch. It should only be used to extract some example script lines from, for further bulk modifications.

19.4 Command Examples

An example script file, including commands and examples, can be found in:
`<HiProvision Installation path>\HiProvision_V<version>\scripting\Example Scripts\Example script.py`

If you want more examples of your own HiProvision database, just export the HiProvision database into a script file as described in §19.3.3.

Some commands:

```
# Create Nodes
CreateNode("PTN2210", "Node1", "1")
CreateModule("NODE://Node1/", "CSM-1", "CSM310-A")
CreateModule("NODE://Node1/", "IFM-1", "4-GC-LW")
CreateLink("PORT://Node1/IFM-1/P1/", "PORT://Node2/IFM-1/P1/", "", "LANWAN1GLink")
SetProperty("PORT://Node1/IFM-1/P1/ - PORT://Node2/IFM-1/P1/", "LinkVLANIdProperty", "2")
```

19.5 Full Command List/Help

Help on a specific command (e.g. CreateNode) can be shown via e.g.
`help("HiProvisionScript.CreateNode")`

A full command list (command+description) can be displayed via `help("HiProvisionScript")`.

- Pressing the spacebar will navigate through all the listed command screens;
- Pressing the ENTER button navigates line by line;
- Right-clicking the window title-bar and selecting properties will pop-up the screen below. This window and its tabs allow the user to fine-tune the scripting DOS-box for an optimized scripting command listing and view.

20. HELP

Prerequisite: Adobe Acrobat Reader must have been installed on your HiProvision PC. If it is not installed, it can be installed via `<HiProvision installation path>\Tools\AdbeRdr11006_en_US.exe`.

Clicking the Help tile on the dashboard shows an inline help function having listed all the Dragon PTN documentation (manuals, install guides, release note...) for this Dragon PTN release. Click a document in the list to open it. Advanced search functionalities are available via the Adobe Acrobat Reader. The figure below explains how the advanced search works once you have opened a manual.

NOTE: These documents are also located in:
`<HiProvision Installation path>\HiProvision_V<version>\Documentation`.

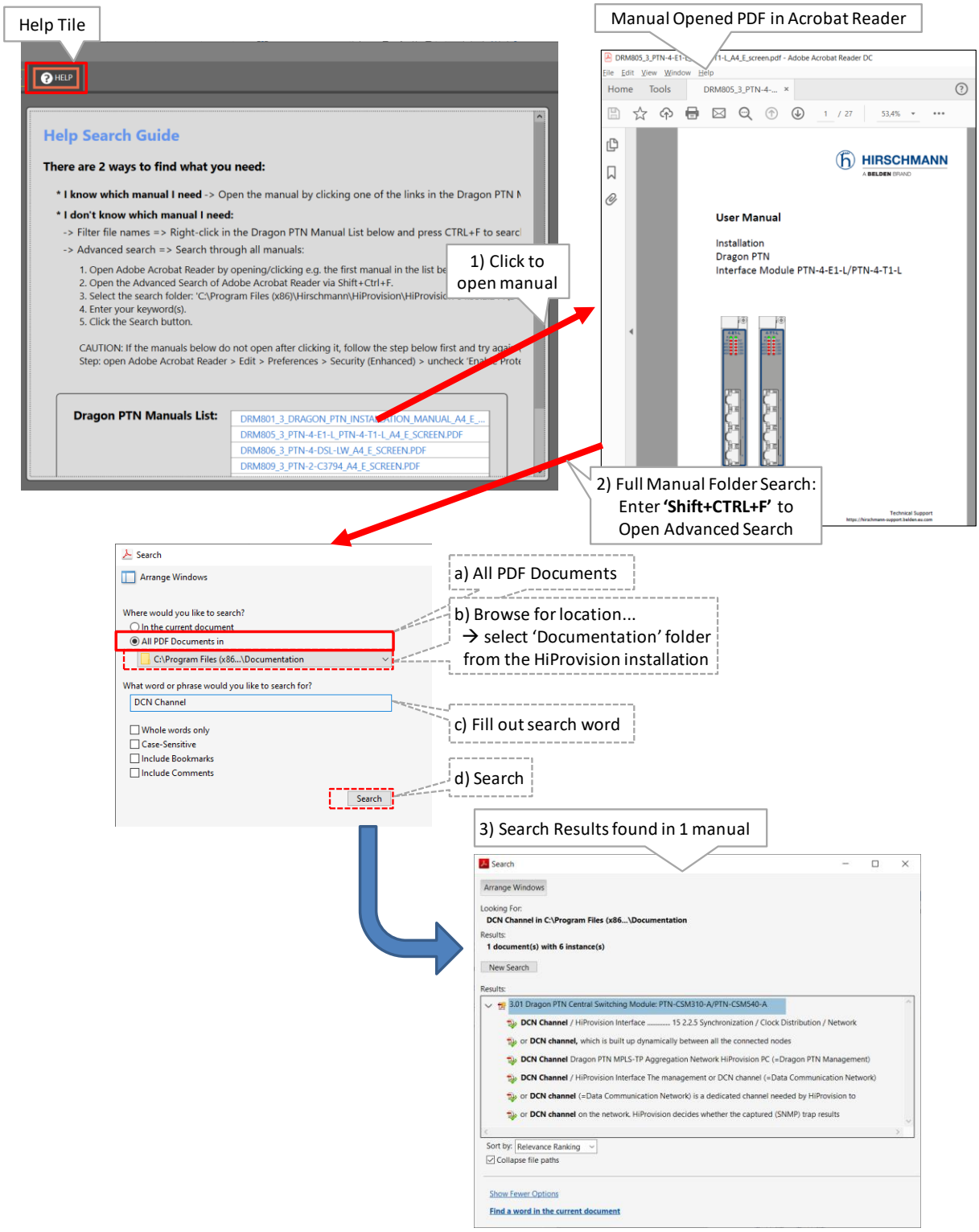


Figure 185 Help Tile: Advanced Search via External Adobe Reader

21. TROUBLESHOOTING

21.1 HiProvision Agent Blocks, Wrong MySQL Installation

- **Problem**: When you start your HiProvision Agent (see §3) and you get the pop-up below, it means that you have installed your MySQL in a wrong way. The HiProvision agent will just block and not go any further. You will not be able to start up HiProvision.

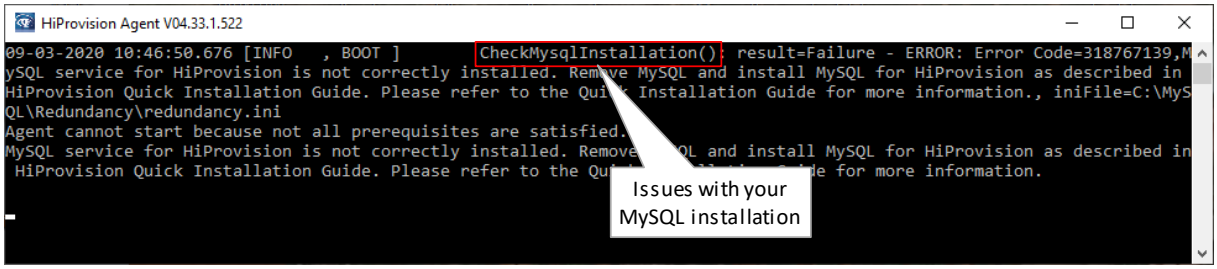


Figure 186 HiProvision Agent Blocks, Wrong MySQL Installation

- **Reason**: The reason why it goes wrong is that your MySQL has been probably installed by just double clicking or executing the <mysql>.msi file, not following the custom install via the Quick Installation Guide. As a result, some important files are missing that HiProvision needs.

- **Solution**:

1. Uninstall MySQL Server via MS Windows Button (Start) → Control Panel → Programs → Uninstall a Program → **MySQL Server** → Uninstall.
2. Existing MySQL databases will not be removed!
3. Install MySQL again by following the Quick Install Guide.
4. Start up the HiProvision agent (see §3). It will not block anymore. Start up the HiProvision Client.

21.2 Database Tile: Authentication Failed

An 'Authentication Failed' error on the database tile means that HiProvision tries to connect to the MySQL server with the wrong authentication credentials. See figure below.

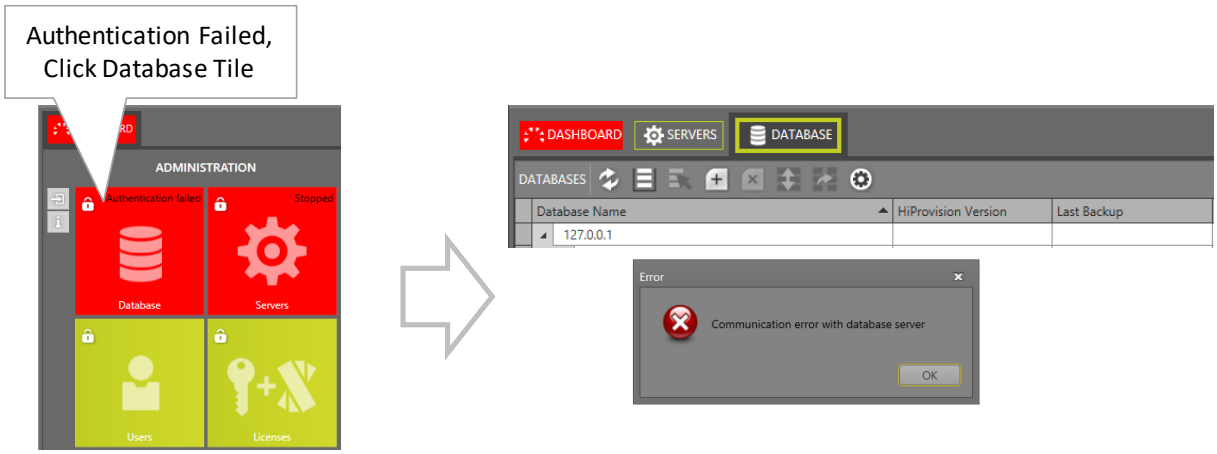


Figure 187 Database Tile: Authentication Failed

Make sure that the configured MySQL database password (default password = **private**) and the password that HiProvision uses to connect is the same. See §8.2.2 how to change passwords and connect with the right credentials.

21.3 View Device Info

The View Device Info tool allows to show more node or L2/L3 IFM information based on a selected CLI command. It can be found via Dashboard → Tools → Advanced → View Device Info;

1. Select the desired node or L2/L3 IFM in the devices list;
2. Select the desired CLI command via the CLI command selector;
3. Click the Execute button;
4. The CLI command output is shown. It can be cleared via the Clear button if desired. If you want to reuse the previous command, select the command from the History dropdown and click Repeat.

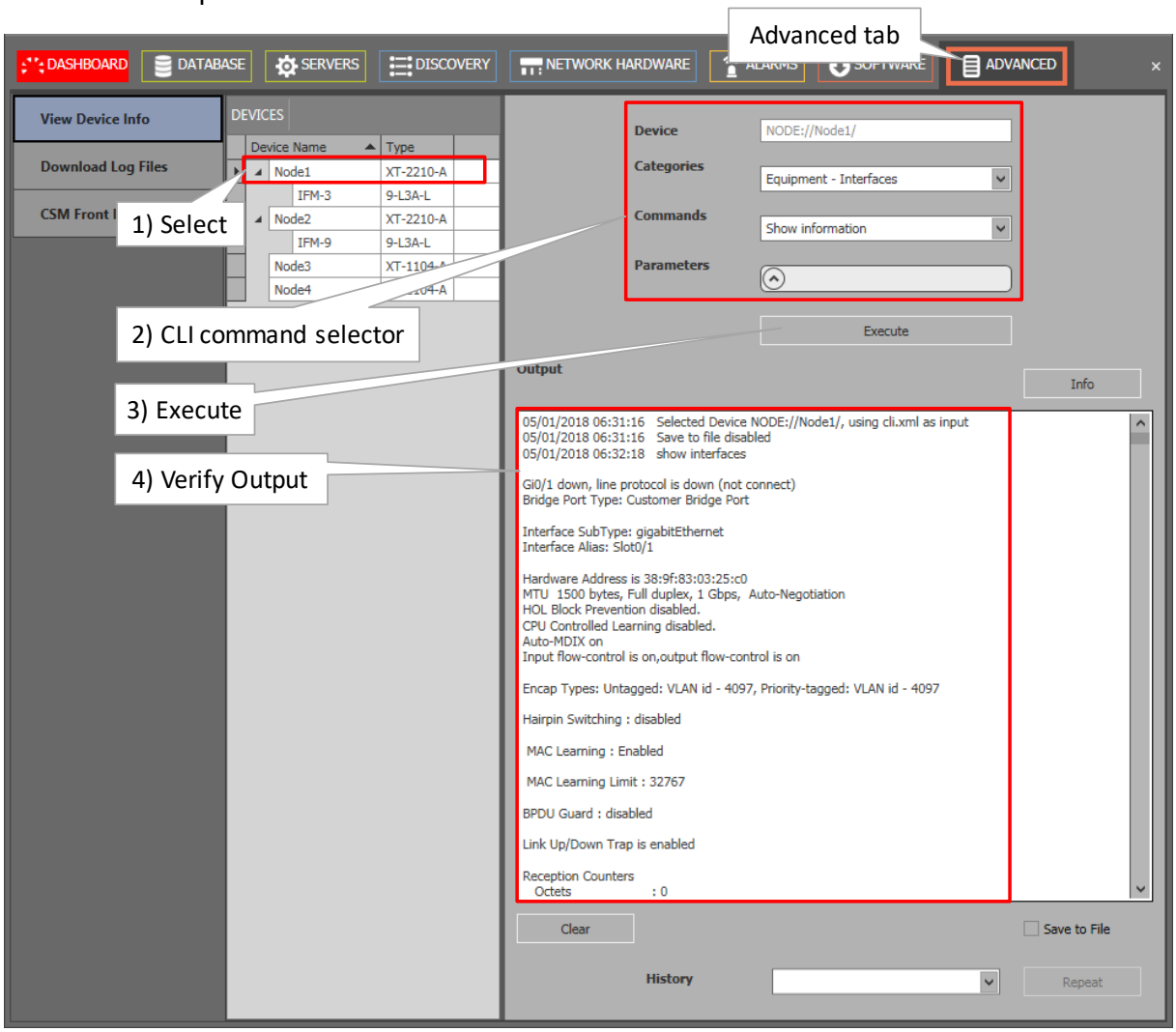


Figure 188 View Device Info: General

5. Port names used in CLI commands are different from the slot/port naming. Therefore, a port mapping table is required to understand which port is meant. This port mapping table can be invoked by clicking the Info button. See figure below.

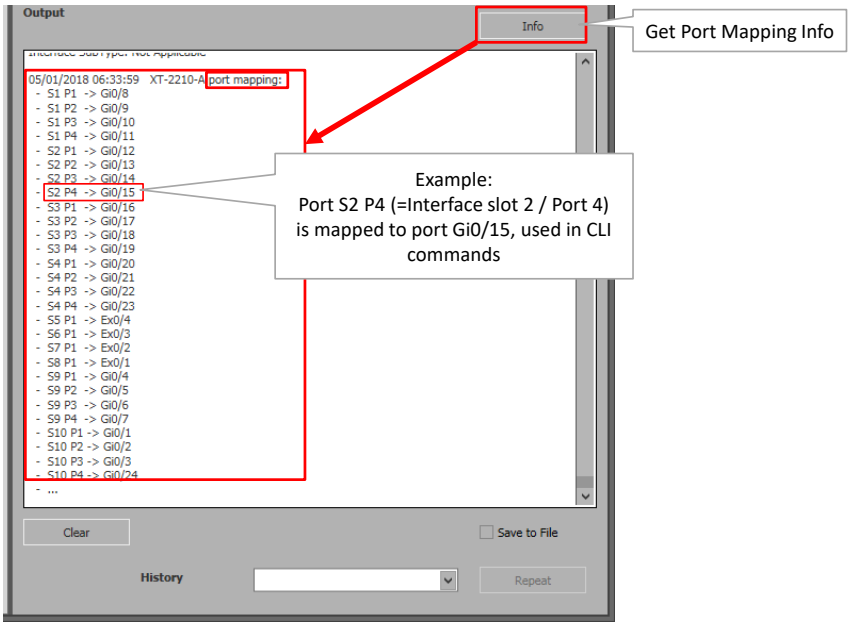


Figure 189 View Device Info: Port Mapping

21.4 Download Log Files from Nodes to HiProvision PC

The 'Download Log Files' tool allows to download log files from your nodes to the HiProvision PC. It can be found via Dashboard → Tools → Advanced → Download Log Files.

1. Select the desired node in the devices list or expand the node and select an IFM only;
2. Click the  button to start the download from the live node to the HiProvision PC;
3. An FTP command has been successfully started, downloading is ongoing into directory C:\FtpRoot\Logs\Node<Node Number>. The 'Download Result' is in the state pending;
4. Click the refresh button  until the 'Download Result' is success;
5. View your downloaded log files in C:\FtpRoot\Logs\Node<Node Number>.

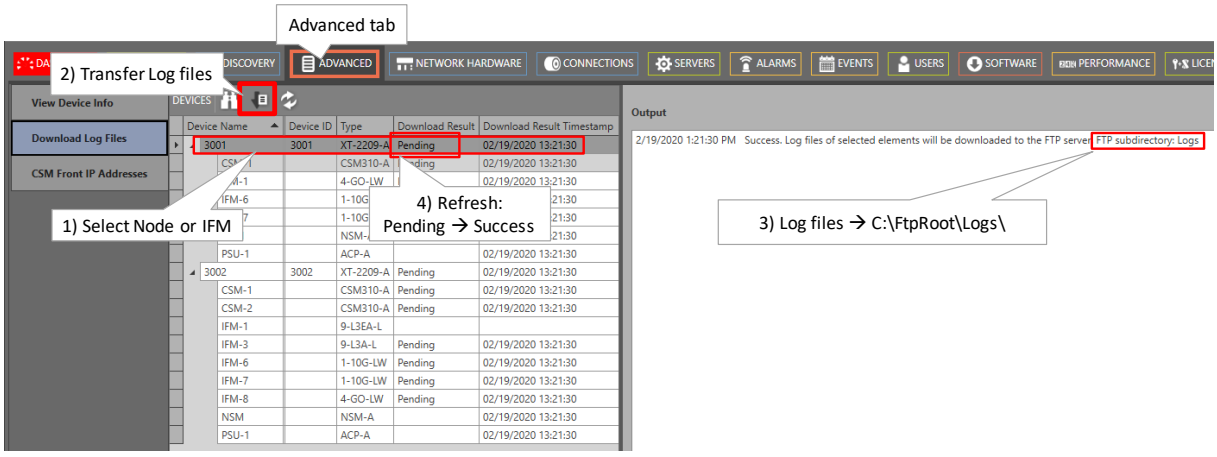


Figure 190 Download Log Files

21.5 Rollback

If something goes wrong and a pop-up in HiProvision asks for a rollback of a node:

1. Go to Dashboard → Network Hardware.
2. Select the node (or all nodes) that must be roll backed and click the rollback button . As a result, the node goes back to a previous restore point (see §7.2) with a working configuration.

21.6 Firewall Ports

If one or the other external LAN connection should not work as expected (e.g. external LAN connections in HiProvision Redundancy, Remote Client, ….), verify your firewall port settings. Make sure that the ports below are not blocked by the firewall:

- TCP 20, 21, 22, 6001, 3306;
- UDP 123, 161, 6020, 6021, 6022, 3306;

NOTE: Remote Client uses TCP 6001;

21.7 Server Does not Start (Server Tile Remains 'Starting')

Verify your FTP server via the Servers tile. If the bullet remains yellow, HiProvision does not succeed in starting the FTP server. As a result the entire HiProvision does not start.

Verify if the HiProvision PC has running another FTP server besides the HiProvision processes. If so, shut down the other third party FTP server and restart the HiProvision Servers.

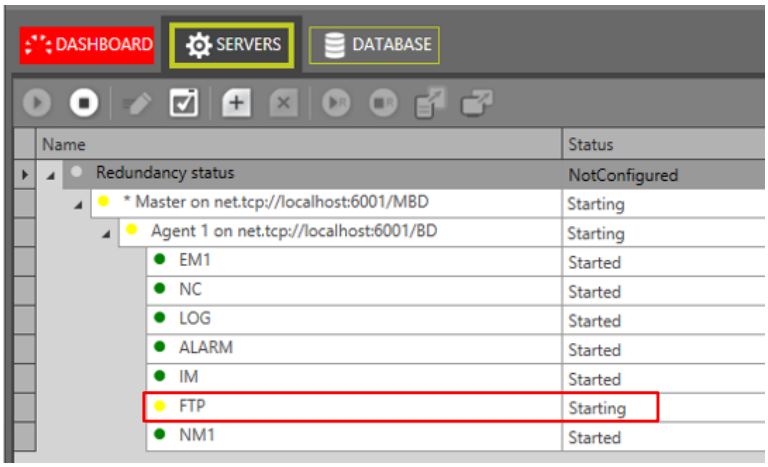


Figure 191 FTP Server Does Not Start

21.8 Lost Tree View Structure Due to Older HiProvision Version

In the special case that a user decides to use an older HiProvision version after using a newer one (=not advised!) it is possible that your tree view structure has been lost in some tables.

To solve this problem, manually clear the user settings via HiProvision User Management, see Ref.[15] in Table 1.

21.9 Improve Performance Between HiProvision Server and External Devices: ARP Reduction

Reduce the number of ARP (=Address Resolution Protocol) messages for better performance between the HiProvision server and the external devices (Hirschmann, …). This can be done by setting following parameters in the 'Hirschmann, …' management NIC in the HiProvision PC:

- the 'Base reachable timer' = 300000 ms (=5min);
- the 'Retransmittime' = in the range of [3000 ms... 10000 ms].

This can be done via opening the command prompt as administrator and enter the command below (fill out the correct <interface>):

- netsh interface ipv4 set interface <interface> basereachable=300000;
- netsh interface ipv4 set interface <interface> retransmittime=<wanted time in ms>.

NOTE: To run as administrator, right-click the CMD(.exe) icon and select 'Run as Administrator'.

21.10 Backup External Device Configuration File Fails – Firewall Problem

When creating backups of external devices fails (dashboard tile → External Devices → Backup and Restore (currently not supported)), the error window below pops up.

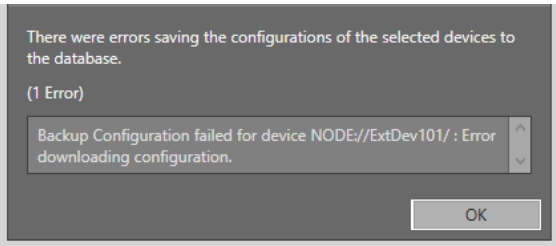


Figure 192 Backup External Device Failed

This backup probably fails due the MS Windows Defender Firewall settings. The firewall is probably turned on and should be turned off.

1. In your MS Windows, go to Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off. See figure below.
2. Turn off the firewall for the Public Network Settings;
3. Click OK;
4. Close Firewall windows;
5. Stop HiProvision Servers;
6. Close HiProvision client and reopen it;
7. Start HiProvision Servers again;
8. Problem should be solved.

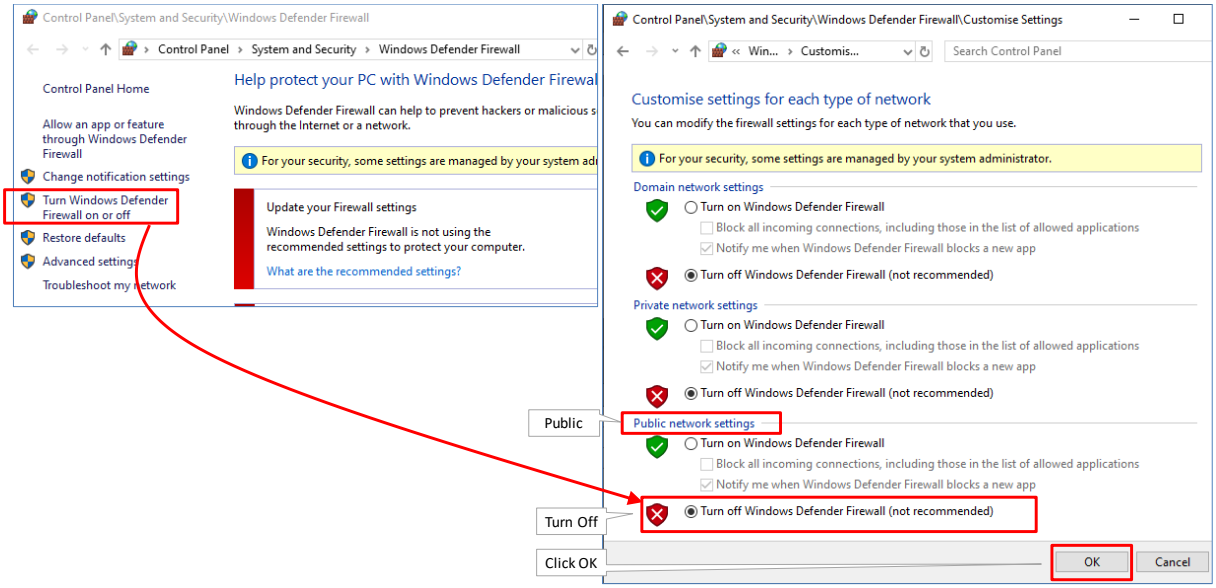


Figure 193 Public: Turn Off Windows Defender Firewall

21.11 Logging/Tracing Folder

Log and tracing results are stored in `<HiProvision Installation Path>\HiProvision_<version>\Logging\System Logging`.

21.12 Automatic Database Backup: Modify Permissions to Access Shared Drive

The Automatic Database Backup feature (§8.4.1b) allows to backup to a shared drive.

It is possible that HiProvision announces that this drive does not exist although this drive does exist and is accessible via Ms Windows Explorer on the HiProvision PC.

HiProvision does probably not have access to this drive. Follow the steps below to grant access:

1. On the HiProvision PC, go to MS Windows start button → Services → HiProvision Agent;
2. Right-click it → select Properties → Log On tab;
3. Select 'This account' and select a network account via the Browse… button to grant permissions to the HiProvision Agent service.

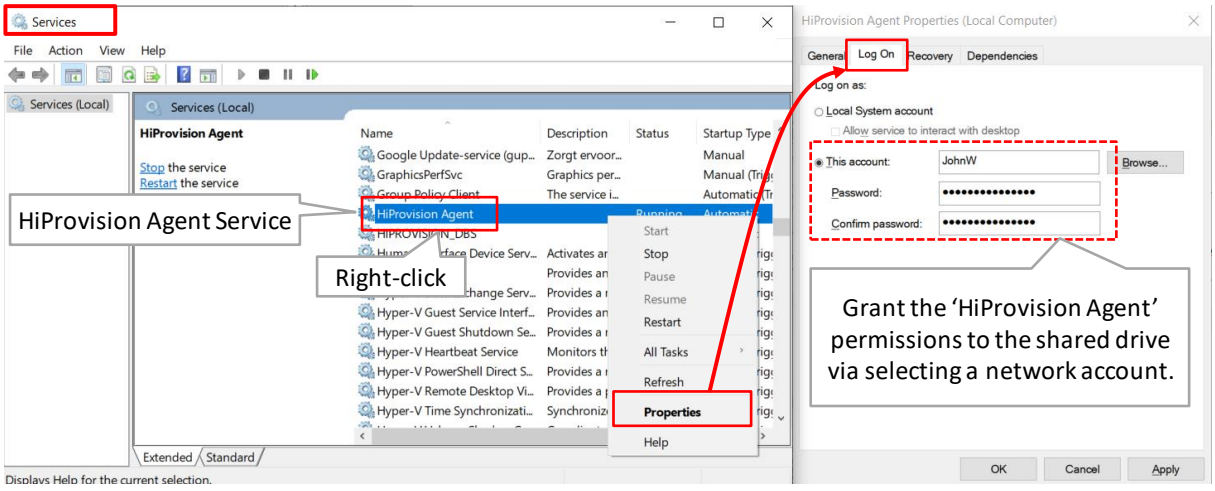


Figure 194 HiProvision Agent: Shared Drive/Network Drive Permissions

22. OPEN SOURCE COMPONENTS

The open source components listed below are used in Dragon PTN.

Table 26 Open Source Components

Component Type	Component	License
LTIB (LINUX)	Apptrk-Base	MIT
LTIB (LINUX)	base_libs	LGPLv2.1
LTIB (LINUX)	bash	GPLv2
LTIB (LINUX)	bridge-utils	GPLv2
LTIB (LINUX)	busybox	GPLv2
LTIB (LINUX)	cramfs	GPLv2
LTIB (LINUX)	curl	Curl License
LTIB (LINUX)	dropbear	MIT Style License
LTIB (LINUX)	e2fsprogs	GPLv2
LTIB (LINUX)	ethtool	GPLv2
LTIB (LINUX)	flex	BSD
LTIB (LINUX)	gdb	GPLv2
LTIB (LINUX)	i2c-tools	GPLv2
LTIB (LINUX)	inet-tools	GPLv2
LTIB (LINUX)	iperf	Ipef License
LTIB (LINUX)	iproute	GPLv2
LTIB (LINUX)	ipsecadm	GPLv2
LTIB (LINUX)	ipsec-tools	BSD
LTIB (LINUX)	iptables	GPLv2
LTIB (LINUX)	iputils	GPLv2
LTIB (LINUX)	kernel	GPLv2
LTIB (LINUX)	libelf	LGPLv2.1
LTIB (LINUX)	libtermcap	LGPLv2.1
LTIB (LINUX)	lzo	GPLv2
LTIB (LINUX)	merge	GPLv2
LTIB (LINUX)	modeps	GPLv2
LTIB (LINUX)	mtd-utils	GPLv2
LTIB (LINUX)	ncurses	MIT
LTIB (LINUX)	netcat	Public Domain
LTIB (LINUX)	net-tools	GPLv2
LTIB (LINUX)	ntpclient	GPLv2
LTIB (LINUX)	openssl	OpenSSL License
LTIB (LINUX)	pciutils	GPLv2

Component Type	Component	License
LTIB (LINUX)	portmap	BSD
LTIB (LINUX)	quotatools	LGPLv2.1
LTIB (LINUX)	screen	GPLv2
LTIB (LINUX)	strace	BSD
LTIB (LINUX)	sysconfig	GPLv2
LTIB (LINUX)	tcp_wrappers	BSD
LTIB (LINUX)	tcpdump	BSD
LTIB (LINUX)	termcap	BSD
LTIB (LINUX)	u-boot	GPLv2
LTIB (LINUX)	vsftpd	GPLv2
LTIB (LINUX)	zlib	Zlib License
CSM	boost	Boost License
CSM	curl	
CSM	DCN	
CSM	emlog	GPLv2
CSM	net-snmp	BSD Like
CSM	olsr	BSD style
ISS	openssh	BSD
ISS	openssl	OpenSSL License
Software	Enterprise Library	Microsoft Public License
Software	GalaSoft.mvvmLight	MIT License
Software	Python	PSF license (GPL compatible)
Software	Quartz scheduling framework for .NET	Apache License 2.0
Software	UDP log	GPLv1 or GPLv2

23. ABBREVIATIONS

ARP Address Resolution Protocol

CAR IP Central Alarm Reporter Internet Protocol

CAS Central Alarm System

CSM Central Switching Module

CSV Comma Separated Values

DCN Data Communication Network

IFM InterFace Module

IP Internet Protocol

L2 Layer2

LAG Link Aggregation Group

LAN	Local Area Network
LER	Label Edge Router
LLDP	Link Layer Discovery Protocol (IEEE)
LNM	Large Network Monitor
LSP	Label Switched Path
LSR	Label Switching Router
LT	Line Termination Character
MAC	Media Access Control
MACsec	Media Access Control Security using 802.1AE IEEE
MPLS-TP	Multiprotocol Label Switching – Transport Profile
MRP	Media Redundancy Protocol
NIC	Network Interface Card
NSM	Node Support Module
NTP	Network Timing Protocol
OSPF	Open Shortest Path First
PSU	Power Supply Unit
PTN	Packet Transport Network
QL	Quality Level
RADIUS	Remote Authentication Dial In User Service
RES	Reserved
RGERP	Redundant Gigabit Ethernet Ring Protocol
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SEC	SDH Equipment Clock
SFP	Small Form Factor Pluggable
TRM	Transmit Receive Module
UDP	Universal Data Protocol
UM	User Management
UTC	Coordinated Universal Time
WAN	Wide Area Network