L-Gate™

CEA-709/BACnet Gateway

User Manual

LOYTEC electronics GmbH

Contact

LOYTEC
Blumengasse 35
A-1170 Vienna
AUSTRIA/EUROPE
support@loytec.com
http://www.loytec.com

Version 3.2

Document 88072407

LOYTEC MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND
LOYTEC SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS PRODUCT IS NOT DESIGNED OR INTENDED FOR USE IN EQUIPMENT INTENDED FOR SURGICAL IMPLANT INTO THE BODY OR OTHER APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH IN THE FAILURE OF SUCH PRODUCT COULD CREATE A SITUATION IN WHICH PERSONAL INJURY OR DEATH MAY OCCUR.

Contents

Abbreviations

100BaseT	100 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several CEA-709 packets into a single CEA-852 packet
AST	Alarming, Scheduling, Trending
BACnet	Building Automation and Control Network
CC	Configuration Client, also known as CN/IP Device
CEA-709	Protocol standard for LONWORKS networks
CEA-852	Protocol standard for tunneling CEA-709 packets over IP channels
CN	Control Network
CN/IP	Control Network over IP
CN/IP Channel	logical IP channels that tunnels CEA-709 packets according CEA-852
CN/IP packet	IP packet that tunnels one or multiple CEA-709 packet(s)
COV	change-of-value
CR	Channel Routing
CS	Configuration Server that manages CEA-852 IP devices
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DNS	Domain Name Server, RFC 1034
DST	Daylight Saving Time
GMT	Greenwich Mean Time
IP	Internet Protocol
LSD Tool	LOYTEC System Diagnostics Tool
MAC	Media Access Control
MD5	Message Digest 5, a secure hash function, see Internet RFC 1321
MS/TP	Master/Slave Token Passing (this is a BACnet data link layer)
NAT	Network Address Translation, see Internet RFC 1631
NV	Network Variable
RTT	Round-Trip Time
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SNVT	Standard Network Variable Type
SSL	Secure Socket Layer
TLS	Transport Layer Security
UI	User Interface
UNVT	User-Defined Network Variable Type
UTC	Universal Time Coordinated
XML	eXtensible Markup Language

1 Introduction

1.1 Overview

The L-Gate is a high performance, reliable and secure network infrastructure component that provides data access to a defined set of data points, which are mapped from one control network technology to another control network technology. In particular, the CEA-709/BACnet Gateway (LGATE-900) implements mappings between a set of CEA-709 network variables (NVs) and a set of standard BACnet server objects. Which NVs are mapped to BACnet objects can be configured by an LNS plug-in or stand-alone configuration software. Easy to understand diagnostic LEDs allow installers and system integrators to install and troubleshoot this device without expert knowledge and dedicated troubleshooting tools. The LGATE-900 is equipped with a 100-BaseT Ethernet port (IP), an FT-10 port (CEA-709), and an RS-485 port (MS/TP). The device is fully compliant with ANSI/CEA-709 and ENV14908, ANSI/ASHRAE-135-2004 and ISO 16484.

On the CEA-709 side of the L-Gate, there can be up to 1000 NVs. The NVs can be bound in the CEA-709 network or operated as “external NVs”. External NVs are polled or explicitly written to without allocating static or dynamic NVs on the L-Gate. In this case, address information is supplied by the configuration software by importing e.g. a CSV file. As communications media on the CEA-709 side, the L-Gate supports either the FT-10 channel or an CEA-852 channel (IP channel over the Inranet/Internet). Which of the two interfaces is used is configurable. The CEA-852 interface can be used behind NAT routers and firewalls, which allows seamless integration in already existing Intranet networks. It supports DHCP even with changing IP addresses in an Intranet environment.

The BACnet objects on the L-Gate can be of the type analog input/output, binary input/output, and multistate input/output. There can be up to 750 of such objects. They are mapped to NVs as configuraed by the Gateway configuration software. This software is able to automatically create BACnet object as counterparts to NVs. In particular, BACnet properties such as Object_Name, Description, Units, Max_Pres_Value, Min_Pres_Value, Resolution, Number_Of_States, and State_Text are derived from the Standard Network Variable Types (SNVTs)[1]. Further, the automatically assigned default values can be edited in the configuration software. BACnet properties updated during run-time by the gateway are Present_Value, Status_Flags, Reliability, Out_Of_Service. Structured NVs are mapped to one BACnet object per structure member. The BACnet server objects are accessible from the BACnet network. In addition, the L-Ggate also includes BACnet client functionality. For each server object a “client mapping” can be defined. These mappings specify other BACnet objects on the network where the L-Gate can read values from (poll or COV subscribe) or write updates to.

[1] This is based on the recommendation in CEN/TS 15231:2006.

The built-in Web server allows convenient device configuration through a standard Web browser such as the Internet Explorer or Firefox. The Web interface also provides statistics information for system installation and network troubleshooting.

In firmware 1.2 and up, the L-Gate supports user-defined network variable types (UNVTs) as dynamic or external NVs, and can access configuration properties (CPs) on other devices through file transfer. To transfer CPs it supports both the LonMark file transfer and the read memory access method. For CPs, the standard (SCPTs) and user-defined (UCPTs) are supported. All of those new CEA-709 data points can be mapped automatically to BACnet objects.

In firmware versions from 3.0 and up, the L-Gate also supports Trendlog, Schedule and Notification Class objects. These objects can be used to operate on any of the basic BACnet objects, which are mapped to CEA-709 NVs. This allows the L-Gate to provide trend data of one or more NVs, schedule NVs and BACnet objects, and report alarms based on NV conditions directly in BACnet. There can be up to 100 scheduler and calendar objects, up to 32 notification class objects, and up to 100 trend log objects with an aggregated total log buffer size of 2MB.

Furthermore, the L-Gate provides LonMark scheduler/calendar objects, which can directly schedule NVs or be translated to BACnet schedules/calendars. For alarm conditions, the L-Gate can be configured to send E-Mails to pre-defined addresses.

The L-Gate is used for:

- connecting BACnet and CEA-709 networks,
- communicating on BACnet with either BACnet/IP or BACnet/MSTP,
- communicating on CEA-709 with either FT-10 or CEA-852 (IP channel on the Intranet/Internet),
- accessing ANSI/CEA-709 network variables (NVs) and configuration properties (CPs) in BACnet,
- supporting standard (SNVT, SCPT) and user-defined (UNVT, UCPT) types,
- accessing BACnet objects in ANSI/CEA-709 networks,
- scheduling BACnet objects and ANSI/CEA-709 network variables,
- translating BACnet schedules/calendars to LonMark schedules/calendars,
- trending BACnet objects,
- generating alarms using intrinsic reporting on BACnet objects,
- sending E-Mails on alarms or scheduled events.

1.2 Scope

This document covers L-Gate devices with firmware version 3.2 and the L-Gate Configurator Software version 3.2. See Chapter 12 for differences between the different L-Gate firmware versions.

2 Quick-Start Guide

This Chapter shows step-by-step instructions on how to configure the L-Gate for a simple network architecture, mapping CEA-709 network variables to BACnet server objects.

2.1 Hardware installation

Connect power (12-35 VDC or 12-24 VAC), the CEA-709 network, and the Ethernet cable as shown in Figure 1. More detailed instructions are shown in Chapter 3.

Important: ***Do not connect terminal 17 to earth ground!***

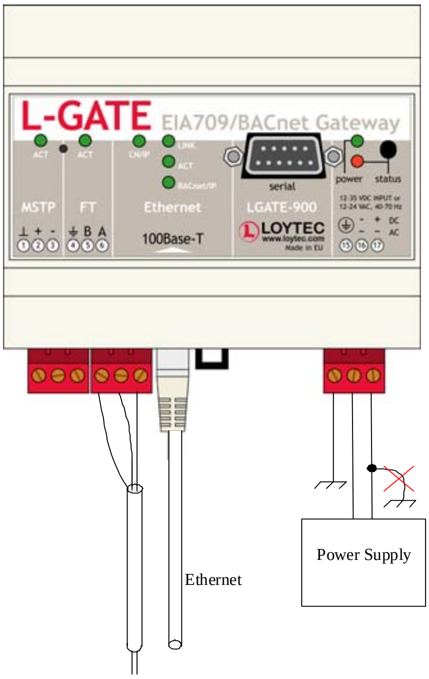


Figure 1: Basic Hardware Installation

If the L-Gate is connected to a BACnet MS/TP network, the MS/TP network segment must be properly terminated with an LT-04 network terminator connected at each of the two ends of the segment media.

2.2 Configuration of the L-Gate

The L-Gate can be configured via a console interface or via the Web interface. To configure the L-Gate, the following steps have to be performed:

1. Setup IP configuration (see Sections 2.2.1 and 2.2.2).

2. Setup BACnet configuration (see Section 2.2.3).

3. Setup gateway configuration (see Section 2.3).

Note: *This setup procedure assumes the use of the IP interface.*

2.2.1 IP Configuration on the Console

Use a PC terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake. To connect COM1 of the PC to the Console on the device, use a standard null-modem cable with full handshaking. Power up the device or press **Return** if the device is already running. The following menu should appear on the terminal:

```
Device Main Menu
================

[1]  Show device information
[2]  Serial firmware upgrade
[3]  System configuration
[4]  CEA-709 configuration
[5]  IP configuration
[6]  CEA-852 device configuration
[7]  BACnet configuration
[8]  Reset configuration (factory defaults)
[9]  Device statistics

[a]  Data Points

[0]  Reset device

Please choose:
```

Figure 2: Device Main Menu

Select ‘5’ from the device main menu and enter the IP address, netmask, and gateway address. Note that you must use different IP addresses if you are using multiple IP devices in your setup.

```
IP Configuration Menu
=====================

[1]  DHCP                 : disabled
[2]  IP Address           : 192.168.1.254
[3]  IP Netmask           : 255.255.255.0
[4]  IP Gateway           : 192.168.1.1
[5]  Hostname             : new
[6]  Domainname           : <unset>
[7]  DNS Servers          : <unset>
[9]  MAC Address          : 00:0A:B0:01:0C:9F (factory default)
[0]  NTP Servers          : <unset> (out-of-sync)
[b]  Link Speed & Duplex  : Auto Detect

[q]  Quit without saving
[x]  Exit and save

Please choose:
```

Figure 3: Enter basic IP settings.

Press ‘x’ to save the IP settings and reset the device with the main menu item ‘0’ in order to let the new IP settings take effect.

Important! ***The default IP address 192.168.1.254 is only set for configuration access. It must be changed in order to make the device functional.***

2.2.2 IP Configuration via the Web Interface

Optionally to using the console interface one can also use the Web interface to configure the client device. In a Web browser enter the default IP address 192.168.1.254 of the L-Gate. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx please open a command tool and enter the following route command to add a route to the L-Gate.

To Add a Route to the Device

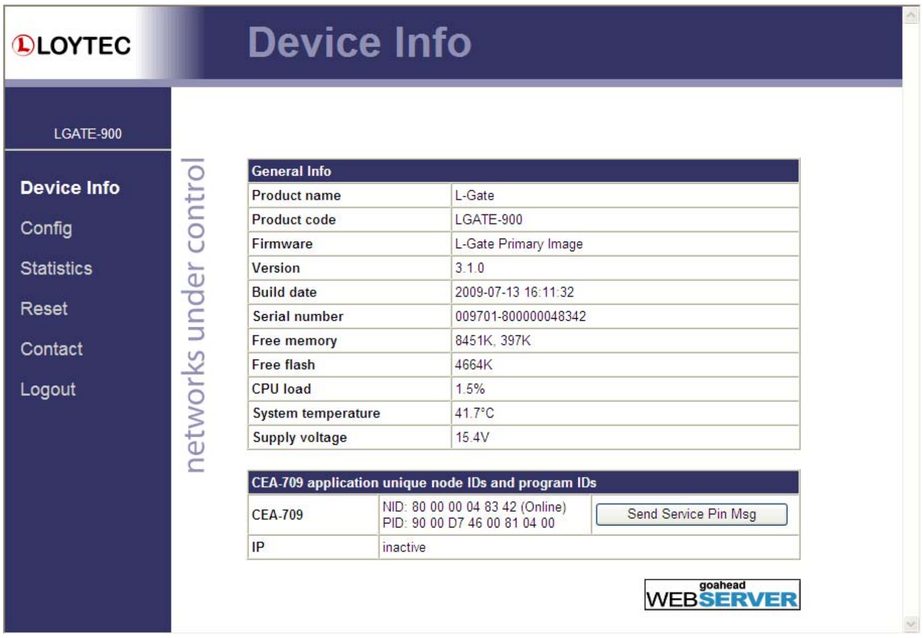
1. Windows **START → Run**

2. Enter ‘cmd’ an click **OK**.

3. In the command window enter the command line

```
route add 192.168.1.254 %COMPUTERNAME%
```

4. Then open your Web browser and type in the default IP address 192.168.1.254.

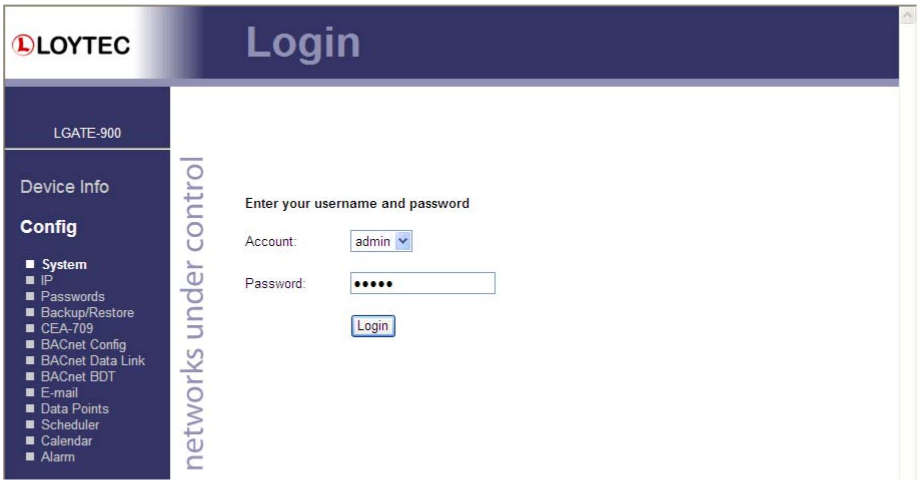


General Info	
Product name	L-Gate
Product code	LGATE-900
Firmware	L-Gate Primary Image
Version	3.1.0
Build date	2009-07-13 16:11:32
Serial number	009701-800000048342
Free memory	8451K, 397K
Free flash	4664K
CPU load	1.5%
System temperature	41.7°C
Supply voltage	15.4V

CEA-709 application unique node IDs and program IDs		
CEA-709	NID: 80 00 00 04 83 42 (Online) PID: 90 00 D7 46 00 81 04 00	Send Service Pin Msg
IP	inactive	

Figure 4: Example Start Screen

5. Click on **Config** in the left menu. You will be asked to enter the administrator password in order to change the IP settings. Enter ‘admin’ and select **Login**.



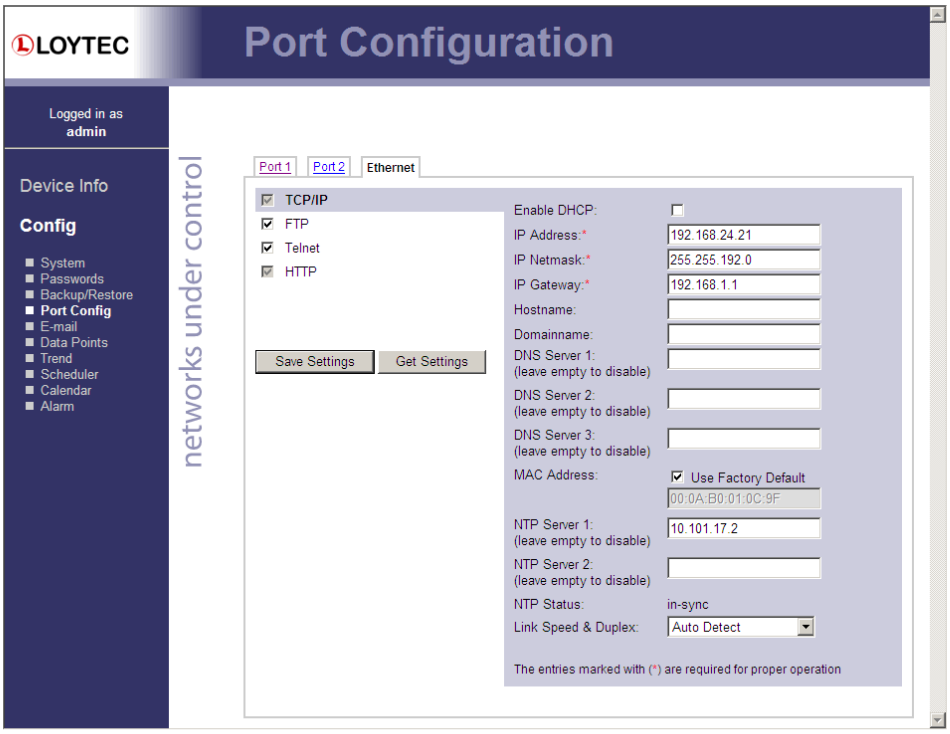
Enter your username and password

Account: admin

Password: •••••

Figure 5: Enter admin as the default administrator password.

6. The Config menu opens. Click on **Port Config** and change to the tab Ethernet. The TCP/IP settings are selected as shown in Figure 6. Enter the IP address, the IP netmask, and IP gateway for this device.



☑ TCP/IP
☑ FTP
☑ Telnet
☑ HTTP

Enable DHCP: □
IP Address:* 192.168.24.21
IP Netmask:* 255.255.192.0
IP Gateway:* 192.168.1.1
Hostname:
Domainname:
DNS Server 1: (leave empty to disable)
DNS Server 2: (leave empty to disable)
DNS Server 3: (leave empty to disable)
MAC Address: ☑ Use Factory Default 00:0A:B0:01:0C:9F
NTP Server 1: (leave empty to disable) 10.101.17.2
NTP Server 2: (leave empty to disable)
NTP Status: in-sync
Link Speed & Duplex: Auto Detect

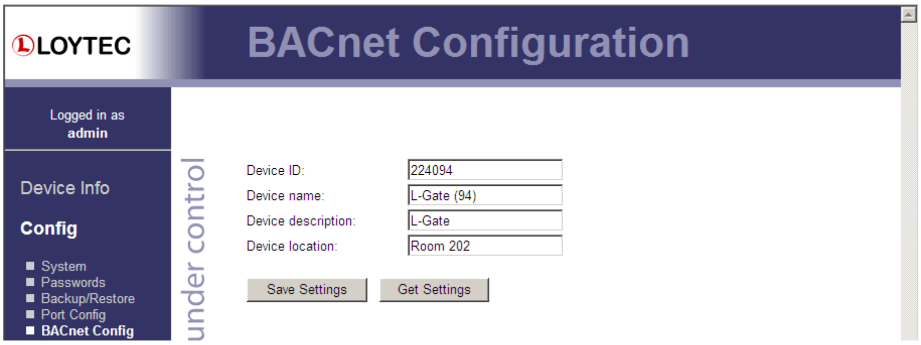
The entries marked with (*) are required for proper operation

Figure 6: Enter IP address and gateway.

7. Press **Save Settings** and then reset the device by selecting **Reset** in the highlighted text. This changes the IP settings of the device.

2.2.3 BACnet Configuration

To configure the BACnet interface, at least the Device ID and the Device Name must be configured (see Figure 7).



Device ID: 224094
Device name: L-Gate (94)
Device description: L-Gate
Device location: Room 202

Figure 7: BACnet Device Configuration

The device ID corresponds to the instance number of the BACnet device object. It must be a unique ID on the BACnet internetwork. Also the Device Name must be a unique name on the BACnet internetwork.

By default the BACnet/IP data link layer is used. If the L-Gate shall be used with the BACnet MS/TP data link layer, please refer to Section 4.2.7 for further information.

2.3 Gateway Configuration with LNS-based Tools

Install the L-Gate Configurator software from the setup.exe. This file can be downloaded from www.loytec.com. In your LNS-based tool register the L-Gate Configurator as an LNS plug-in.

The detailed guide to configuring the L-Gate and downloading the configuration can be found in section 6.4.2 (Configure with LNS).

3 Hardware Installation

3.1 Enclosure

3.1.1 LGATE-900

The L-Gate enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 8).

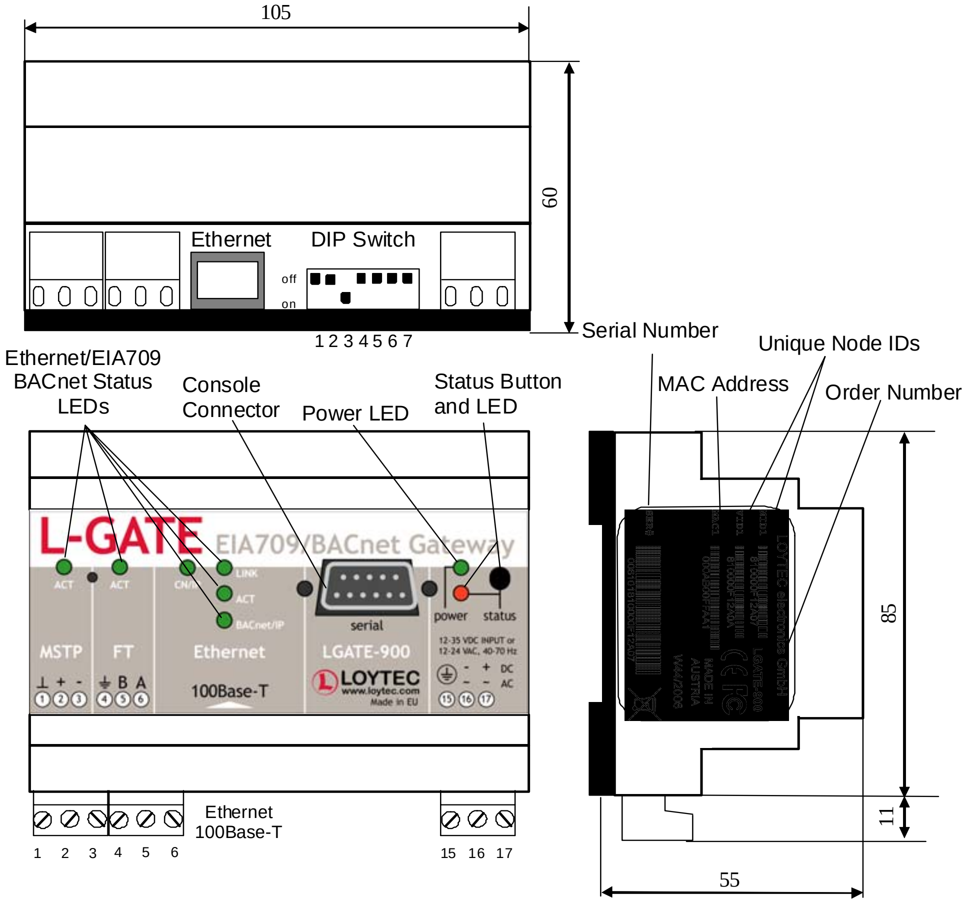


Figure 8: L-Gate Enclosure (dimensions in mm)

3.2 Product Label

The product label on the side of the L-Gate contains the following information (see Figure 8):

- L-Gate order number with bar-code (e.g., LGATE-900),
- serial number with bar-code (Ser#),
- unique node ID and virtual ID of each port (NID1, VID1) with bar-code,
- Ethernet MAC ID with bar-code (MAC1).

Unless stated otherwise, all bar codes are encoded using “Code 128”. An additional label is also supplied with the L-Gate for documentation purposes. A virtual ID (VID) is a Node ID on the IP channel.

3.3 Mounting

The device comes prepared for mounting on DIN rails following DIN EN 50 022. The device can be mounted in any position. However, an installation place with proper airflow must be selected to ensure that the L-Gate’s temperature does not exceed the specified range (see Chapter 13).

3.4 LED signals

3.4.1 Power LED

The L-Gate power LED lights up green when power is supplied to terminals 15, 16, and 17.

3.4.2 Status LED

The L-Gate is equipped with a red status LED (see Figure 8). This LED is normally off. During boot-up the status LED is used to signal error conditions (red). If the fall-back image is executed the status LED flashes red once every second.

3.4.3 MSTP Activity LED

The MS/TP port has a three-color MSTP Activity LED (see Figure 8). Table 2 shows the different LED patterns of the port and their meaning. A permanent color reflects a state. Flicker is for 25 ms when there is activity on the MS/TP data link layer.

Behavior	Description	Comment
GREEN permanently, flicker off	Multi-Master, token ok, flicker when traffic	Normal condition on a multi-master MS/TP network
ORANGE flicker	Sole master, flicker when traffic	Normal condition on a single-master MS/TP network
RED permanent, flicker GREEN	Token lost state, flicker when transmit attempt	Cable might be broken.
RED flash fast	Transmission or receive errors.	This hints at bad cabling.

Table 1: MS/TP Activity LED Patterns

3.4.4 FT Activity LED

The FT port on the L-Gate has a three-color LED (green, red, and orange, see Figure 8). Table 2 shows different LED patterns of the port and their meaning.

Behavior	Description	Comment
GREEN flashing fast	Traffic	
GREEN flashing at 1Hz	L-Gate is unconfigured	
RED permanent	Port damaged	
RED flashing fast	Traffic with high amount of errors	
RED flashing at 1 Hz (all ports)	Firmware image corrupt	Please upload new firmware.
ORANGE permanent	Port disabled	e.g. using LSD Tool
ORANGE flashing fast	Traffic on port configured as management port	e.g. using LSD Tool

Table 2: CEA-709 Activity LED Patterns

3.4.5 Ethernet Link LED

The Ethernet Link LED lights up green whenever an Ethernet cable is plugged-in and a physical connection with a switch, hub, or PC can be established.

3.4.6 Ethernet Activity LED

The Ethernet Activity LED lights up green for 6 ms whenever a packet is transmitted or received or when a collision is detected on the network cable.

3.4.7 CN/IP LED

The CNIP LED is a three color LED that indicates different operating states of the L-Gate’s CEA-852 device.

Green: The CEA-852 device is fully functional and all CEA-852 configuration data (channel routing info, channel membership list, send list) are up-to-date.

Green flicker: If a valid CEA-709 packet is received or transmitted over the IP channel, the CNIP LED turns off for 50 ms. Only valid CEA-709 IP packets sent to the IP address of the L-Gate can be seen. Stale packets or packets not addressed to the L-Gate are not seen.

Yellow: The CEA-852 device is functional but some configuration data is not up-to-date (device cannot contact configuration server but has configuration data saved in Flash memory)

Red: The CEA-852 device is non-functional because it was rejected from the CEA-852 IP channel or shut-down itself due to an internal error condition.

Off: The CEA-852 device is non-functional because it has not been started. This can be the case if the L-Gate uses DHCP and it has not received a valid IP configuration (address) from the DHCP server.

Flashing Red at 1 Hz: The CEA-852 device is non-functional because it is started but has not been configured. Please add the device to a CEA-852 IP channel (register in configuration server).

Flashing green or orange at 1 Hz: The L-Gate’s CEA-709 side of the gateway has not been commissioned yet. The color indicates the CEA-852 IP channel status as described above.

3.4.8 BACnet/IP LED

The BACnet/IP LED flashes green for 25 ms when BACnet packets are transmitted or received over the BACnet/IP interface.

3.4.9 Wink Action

If the L-Gate receives a wink command on any of its network ports, it shows a blink pattern on the CNIP and the CEA-709 activity LEDs. The CEA-709 activity and the CNIP LED turn green/orange/red (each 0.15 s). This pattern is repeated six times. After that, the CNIP LED flashes orange six times if the wink command was received on the IP channel or the CEA-709 activity LED flashes orange six times if the wink command was received on the CEA-709 channel. After that the L-Gate LEDs resume their normal behavior.

3.4.10 Network Diagnostics

The L-Gate provides simple network diagnostics via its CEA-709 activity LED:

If the LED does not light up at all, this port is not connected to any network segment or the connected network segment currently shows no traffic.

If the LED is flashing green, the network segment connected to this port is ok.

If the LED is flashing red, a potential problem exists on the network segment connected to this port. This state is referred to as overload condition.

A port overload condition occurs if

- the average bandwidth utilization of this port was higher than 70% or
- the collision rate was higher than 5% or
- more than 15% CRC errors have occurred on a port with a power-line transceiver or more than 5% on a port with a transceiver other than power-line or
- the L-Gate was not able to process all available messages.

For a deeper analysis of the reason for the overload condition, it is recommended to use a protocol analyzer (e.g. LOYTEC’s LPA) or a similar tool. The exact reason of the overload condition can also be determined with the LSD Tool.

3.5 Status Button

The L-Gate is equipped with a status button (see Figure 8). When pressing the status button shortly during normal operation of the L-Gate, it sends a “Service Pin Message” on the active CEA-709 network port (FT-10 or CEA-852). It also sends a BACnet “I-Am” message on all active BACnet data link layers. As an alternative to pressing the status button, a service pin message can be sent via the Web interface (see Section 4.1).

The status button can also be used to switch the device back to factory default state. Press the service button and power-cycle the device. Keep the button pressed until the port LEDs illuminate orange permanently. Release the button within five seconds from that time on to reset the device to factory defaults. Alternatively, the device can be switched back to factory defaults over the console UI (see Section 10.2.2).

3.6 DIP Switch Settings

The DIP switch assignment for the L-Gate is shown in Table 3. Please leave all switches at default state.

DIP Switch #	Function	Factory Default
1	Must be OFF	OFF
2	Must be OFF	OFF
3	Must be ON	ON
4	Must be OFF	OFF
5	Must be OFF	OFF
6	Must be OFF	OFF
7	Must be OFF	OFF

Table 3: DIP Switch Settings for L-Gate

3.7 Terminal Layout and Power Supply

The L-Gate provides screw terminals to connect to the network as well as to the power supply. The screw terminals can be used for wires of a maximum thickness of 1.5 mm^2/AWG12. The device can either be DC or AC powered.

Terminal	Function
1	BACnet MS/TP Ground
2	BACnet MS/TP Non-Inverting Input
3	BACnet MS/TP Inverting Input
4	Earth Ground
5, 6	CEA-709 A, B of FT-10 Channel Port
8	Ethernet 100BaseT
15	Earth Ground
16, 17	Power Supply 12-35 VDC or 12-24 VAC ± 10% **Do not connect terminal 17 to earth ground!**

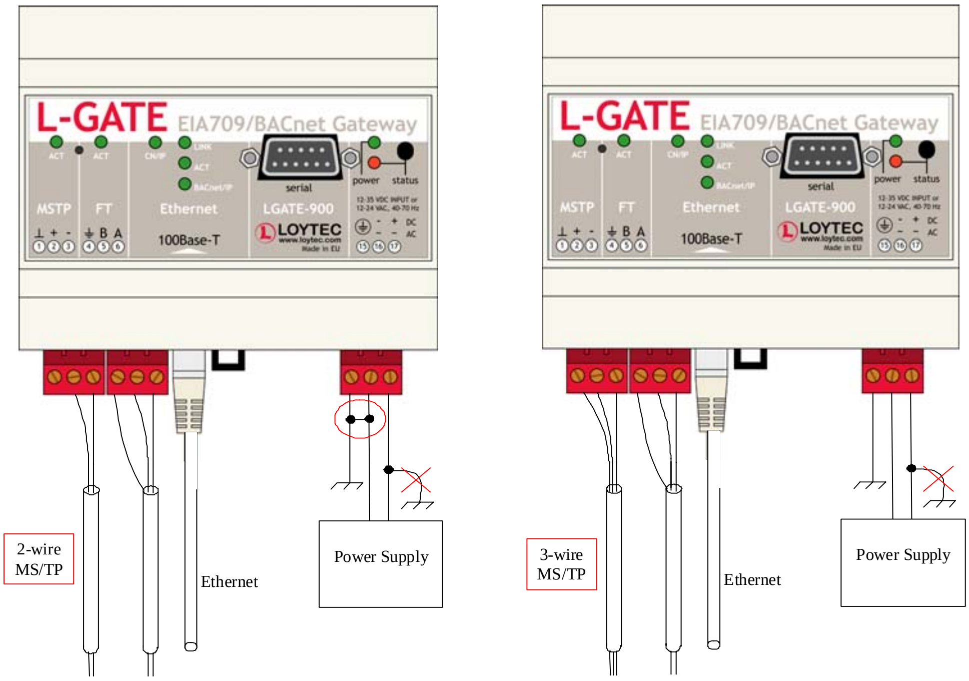
Table 4: L-Gate Terminals LGATE-900.

3.8 Wiring

The CEA-709 network segment connected to the L-Gate needs to be terminated according to the rules found in the specification of the transceiver (see Section 8.1). If BACnet is configured to run over MS/TP, the MS/TP network segment must be properly terminated with an LT-04 network terminator connected at each of the two ends of the segment media.

Important: ***When using shielded network cables, only one side of the cable should be connected to earth ground. Thus, the shield must be connected to earth ground either at the L-Gate terminals or somewhere else in the network.***

Important: ***When using 2-wire MS/TP, earth ground must be connected to both terminal 15 and 16 (see Figure 9a). Never connect terminal 17 to earth ground!***



(a) (b)

Figure 9: Connecting the L-Gate: (a) 2-wire MS/TP, (b) 3-wire MS/TP

4 Web Interface

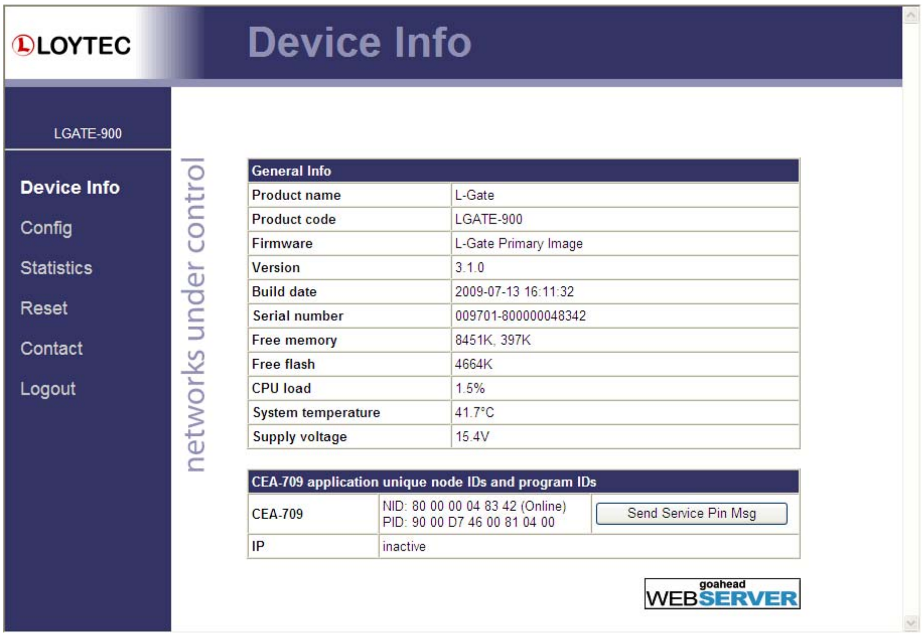
The L-Gate comes with a built-in Web server and a Web interface to configure the L-Gate and extract statistics information. The Web interface allows configuring the IP settings, CEA-852 and CEA-709 settings, and the BACnet settings. This interface is very simple to use and has an intuitive, self-explanatory user interface.

4.1 Device Information and Account Management

In a Web browser enter the default IP address 192.168.1.254 of the device. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx you must open a command tool and enter the following route command to add a route to the device:

To Add a Route to the Device

1. Windows START → Run
2. Enter ‘cmd’ an click **Ok**.
3. In the command window enter the command line
   ```
   route add 192.168.1.254 %COMPUTERNAME%
   ```
4. Then open your Web browser and type in the default IP address 192.168.1.254.
5. The device information page should appear as shown in Figure 10.



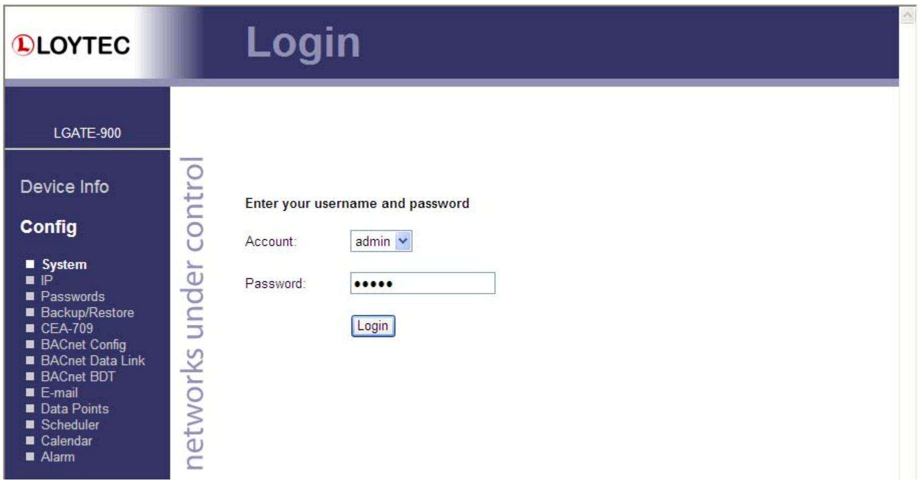
General Info	
Product name	L-Gate
Product code	LGATE-900
Firmware	L-Gate Primary Image
Version	3.1.0
Build date	2009-07-13 16:11:32
Serial number	009701-800000048342
Free memory	8451K, 397K
Free flash	4664K
CPU load	1.5%
System temperature	41.7°C
Supply voltage	15.4V

CEA-709 application unique node IDs and program IDs		
CEA-709	NID: 80 00 00 04 83 42 (Online) PID: 90 00 D7 46 00 81 04 00	Send Service Pin Msg
IP	inactive	

Figure 10: Device Information Page

The device information page shows information about the L-Gate and the current firmware version. It includes the unique node IDs (“Neuron IDs”) of the CEA-709 network interfaces. This page can also be used to send the CEA-709 service pin messages. This is a useful feature when commissioning the L-Gate, since it is not necessary to be on-site to press the device’s status button.

Click through the menus on the left hand side to become familiar with the different screens. If you click on **Config** in the left menu you will be asked to enter the administrator password in order to make changes to the settings as shown in Figure 11. Enter the default administrator password ‘admin’ and select **Login**.



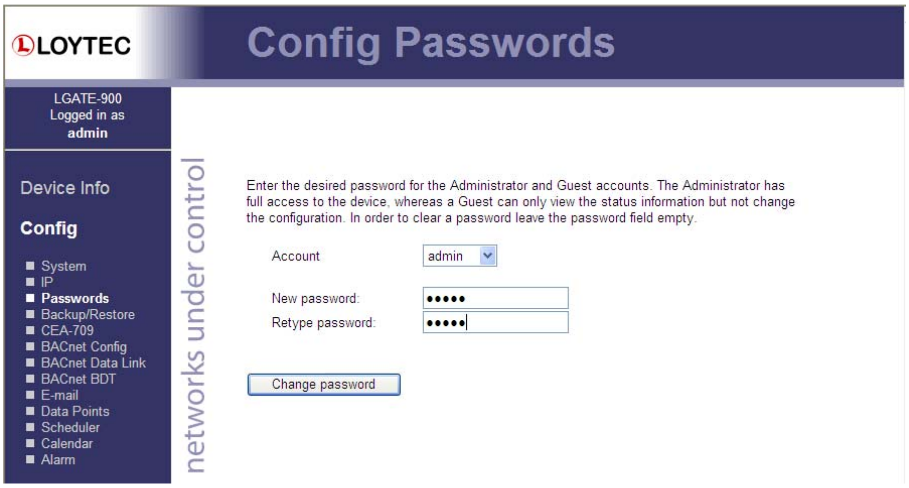
Enter your username and password

Account: admin

Password: •••••

Figure 11: Enter admin as the default administrator password.

The Config menu opens. Click on **Passwords** in the Config menu, which opens the password configuration page as shown in Figure 12. The L-Gate has three user accounts: (1) **guest** allows the user to view certain information only, e.g., the device info page. By default the guest user has no password. (2) **operator** is able to read more sensible information such as calendar data. (3) **admin** has full access to the L-Gate and can make changes to its configuration. Note that the user accounts are also used to log on to the FTP and Telnet server.



Enter the desired password for the Administrator and Guest accounts. The Administrator has full access to the device, whereas a Guest can only view the status information but not change the configuration. In order to clear a password leave the password field empty.

Account: admin

New password: •••••

Retype password: •••••

Figure 12: Password Configuration Screen

Please change the administrator password in order to protect yourself from unwanted configuration changes by anyone else. To do so, select the **admin** account in the drop-down box and enter the new password. If the administrator password is left empty, password protection is turned off and everyone can access the L-Gate without entering a password. Click on **Change password** to activate the change.

4.2 Device Configuration

The device configuration pages allow viewing and changing the device settings of the L-Gate. Here are some general rules for setting IP addresses, port numbers, and time values:

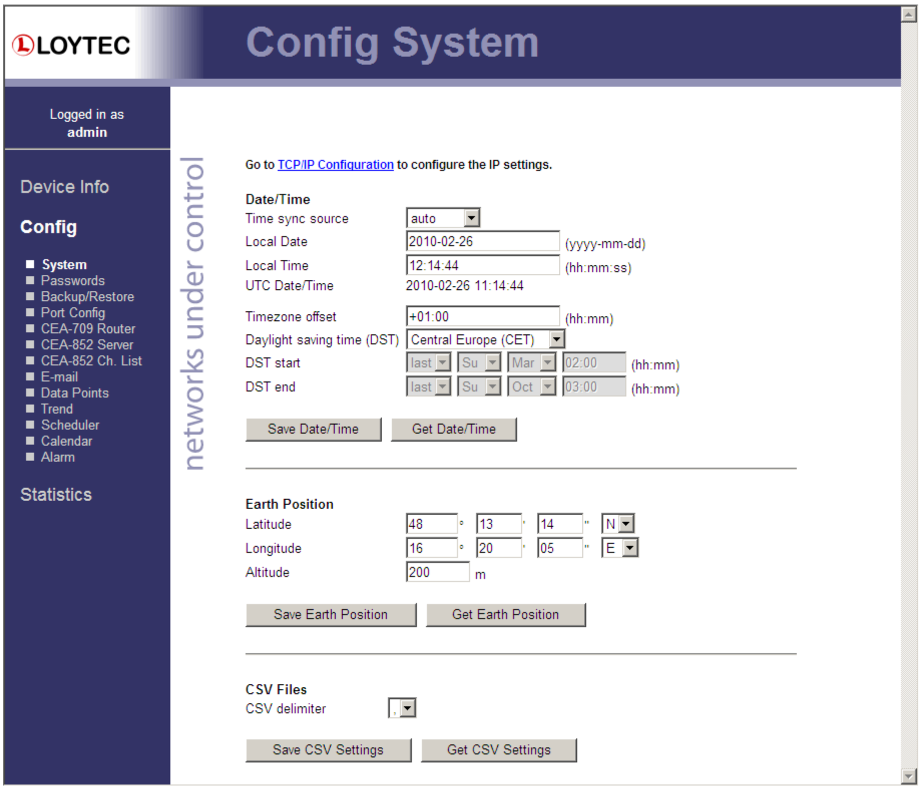
- An empty IP address field disables the entry.
- An empty port number field sets the default port number.
- An empty time value field disables the time setting.

4.2.1 System Configuration

The system configuration page is shown in Figure 13. This page allows configuring the device's system time and other system settings. The **TCP/IP Configuration** link is a shortcut to the Ethernet port configuration. Follow that link to change the IP settings of the device

The time sync source can be set to **auto**, **manual**, **NTP**, **BACnet**, or **LonMark**. In the **auto** mode, the device switches to the first external time source that is discovered. Possible external time sources are NTP, BACnet. The option **manual** allows setting the time manually in the fields **Local Time** and **Local Date**. In **manual** mode, the device does not switch to an external time source. Note, that if **NTP** is selected, the NTP servers have to be configured on the IP Configuration page (see Section 4.2.4).

The time zone offset must be defined independently of the time source. It is specified as the offset to GMT in hours and minutes (e.g., Vienna/Austria is +01:00, New York/U.S.A. is -06:00). For setting the daylight saving time (DST) pre-defined choices are offered for Europe and U.S.A./Canada. DST can be switched off completely by choosing **none** or set manually for other regions. In that case, start and end date of DST must be entered in the fields below.



Go to TCP/IP Configuration to configure the IP settings.

Date/Time

Time sync source: auto

Local Date: 2010-02-26 (yyyy-mm-dd)

Local Time: 12:14:44 (hh:mm:ss)

UTC Date/Time: 2010-02-26 11:14:44

Timezone offset: +01:00 (hh:mm)

Daylight saving time (DST): Central Europe (CET)

DST start: last Su Mar 02:00 (hh:mm)

DST end: last Su Oct 03:00 (hh:mm)

Earth Position

Latitude: 48 ° 13 ' 14 " N

Longitude: 16 ° 20 ' 05 " E

Altitude: 200 m

CSV Files

CSV delimiter: ,

Figure 13: System Configuration Page

The next section on the page allows configuring the L-Gate's earth position. This setting defines the longitude, latitude and elevation of the device. The latitude and longitude are entered as degrees, minutes, and seconds. The altitude (or elevation) is entered in meters from sea level. This setting is used for an astronomical clock. For fixed locations such as a building, the position can be entered on this page. For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 7.2.3).

For generating CSV files for trend logs, alarm logs, etc. the delimiter for those CSV files can be configured. This setting can be changes between a comma ',' and a semi-colon ';'. The change takes effect immediately for all files generated by the device.

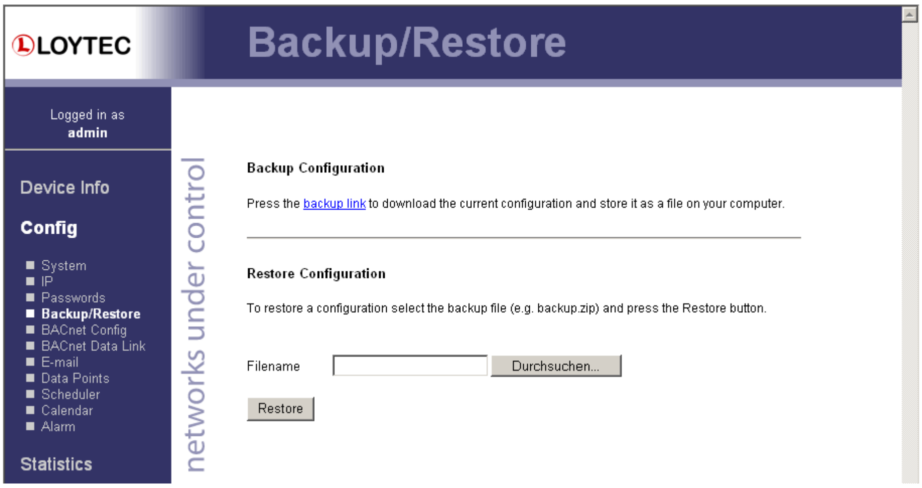
4.2.2 Backup and Restore

A configuration backup of the L-Gate device can be downloaded via the Web interface. Press the **Backup/Restore** link as shown in Figure 14 to start the download. The L-Gate device assembles a single file including all required files. A file requestor dialog allows specifying the location where the backup file shall be stored.

To restore the device settings, simply select a previously generated backup file in the **Restore Configuration** section of the page by clicking the button next to the **Filename** field. Then press the **Restore** button.

The backed up configuration data consists of:

- Device settings (Passwords, IP settings, e-mail config, etc.),
- Data point configuration,
- CEA-709 binding information,
- BACnet server objects and client mappings,
- AST settings.



LOYTEC

Backup/Restore

Logged in as
admin

Backup Configuration

Press the backup link to download the current configuration and store it as a file on your computer.

Restore Configuration

To restore a configuration select the backup file (e.g. backup.zip) and press the Restore button.

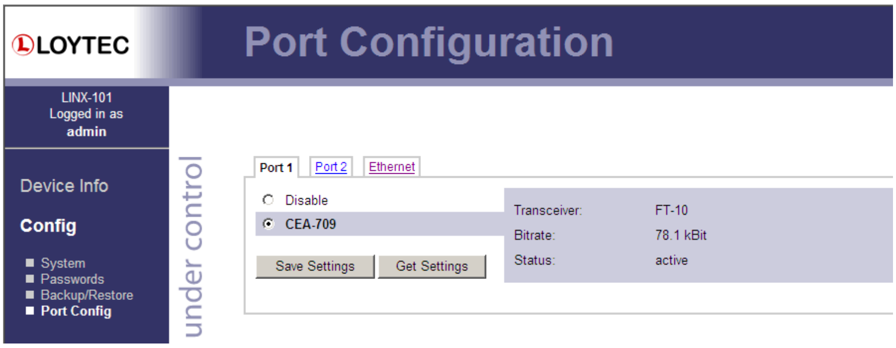
Filename [ ] Durchsuchen...

Restore

Figure 14: Backup/Restore page.

4.2.3 Port Configuration

This menu allows configuring the device’s communications ports. For each communication port, which is available on the device and shown on the label (e.g., Port 1, Port 2, Ethernet), a corresponding configuration tab is provided by the Web UI. An example is shown in Figure 15. Each port tab contains a selection of available communication protocols. By selecting a checkbox or radio button the various protocols can be enabled or disabled on the communication port. Some ports allow exclusive protocol activation only, other ports (e.g., the Ethernet port) allow multiple protocols bound to that port.



LOYTEC

Port Configuration

LINX-101
Logged in as
admin

○ Disable
● CEA-709

Save Settings Get Settings

Transceiver: FT-10
Bitrate: 78.1 kBit
Status: active

Figure 15: Port Configuration Page.

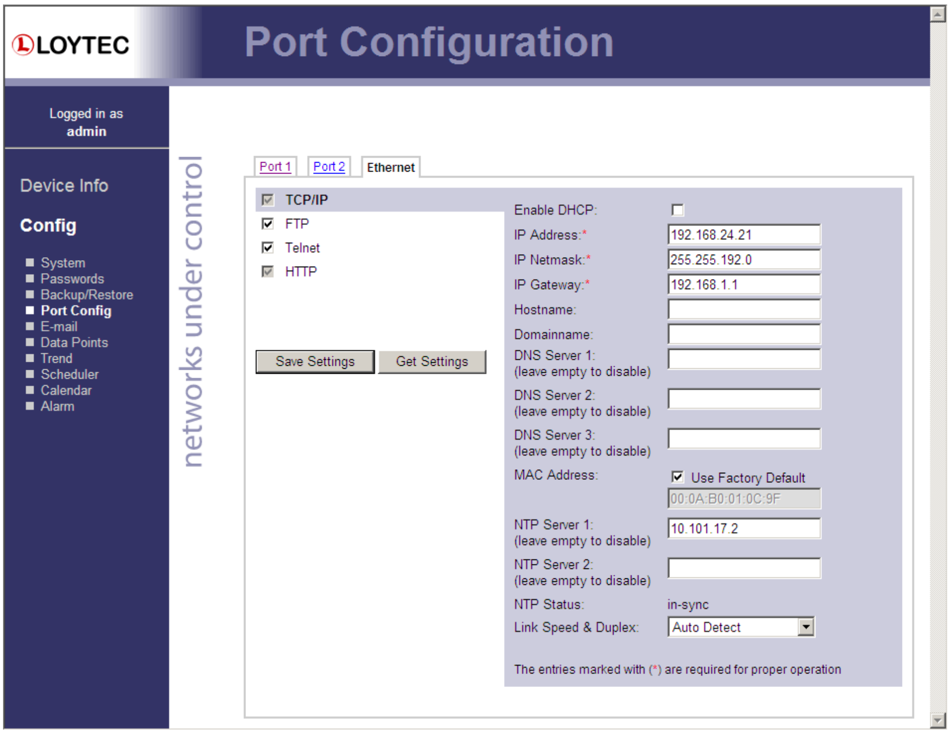
When selecting a protocol on a communication port, the protocol’s communication parameters are displayed in a box on the right-hand side. To save the settings of the currently opened protocol, click the **Save Settings** button. Pressing **Get Settings** retrieves the current settings from the device.

4.2.4 IP Configuration

The TCP/IP configuration is done under the Ethernet port tab as shown in Figure 16. The mandatory IP settings, which are needed to operate the device, are marked with a red asterisk (IP address, netmask, gateway). The **Enable DHCP** checkbox switches between manual entry of the IP address, netmask, and gateway address, and automatic configuration from a DHCP server.

Important! ***The default IP address 192.168.1.254 is only set for configuration access. It must be changed in order to make the device functional.***

Hostname and **Domainname** are optional entries and can be left empty. For some DHCP configurations it may be necessary to enter a hostname. Please contact your system administrator on how to configure DHCP to acquire an IP address. Further, you can configure up to 3 Domain Name Servers.



☑ TCP/IP
☑ FTP
☑ Telnet
☑ HTTP

Enable DHCP: □
IP Address:* 192.168.24.21
IP Netmask:* 255.255.192.0
IP Gateway:* 192.168.1.1
Hostname:
Domainname:
DNS Server 1: (leave empty to disable)
DNS Server 2: (leave empty to disable)
DNS Server 3: (leave empty to disable)
MAC Address: ☑ Use Factory Default
00:0A:B0:01:0C:9F
NTP Server 1: (leave empty to disable) 10.101.17.2
NTP Server 2: (leave empty to disable)
NTP Status: in-sync
Link Speed & Duplex: Auto Detect

The entries marked with (*) are required for proper operation

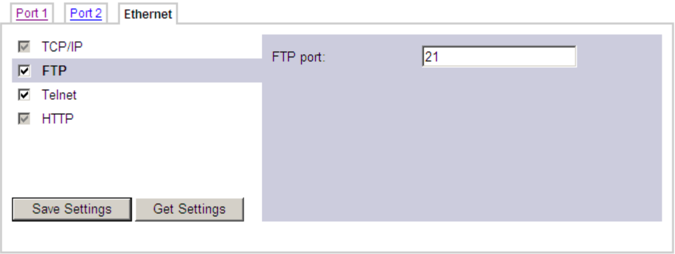
Figure 16: IP Configuration Page with DHCP disabled

The device comes configured with a unique MAC address. This address can be changed in order to clone the MAC address of another device. Please contact your system administrator to avoid MAC address conflicts.

The device can be configured to synchronize its clock with NTP time. Enter the IP address of a primary and, optionally, a secondary NTP server. The L-Gate will use NTP as a time source if the time sync source in the system configuration page is set to **NTP** (see Section 4.2.1). The field **NTP status** below the NTP server settings displays the current NTP synchronization status (**out-of-sync**, or **in-sync**).

If the L-Gate is operated with a 10Mbit/s-only hub, the link speed should be switched from **Auto Detect** to **10Mbps/Half-Duplex**. With modern 100/10Mbit/s switches this setting can be left at its default.

Other standard protocols that are bound to the Ethernet interface are FTP, Telnet, and HTTP (Web server). By deselecting the checkbox, those protocols can be individually disabled. The standard UDP/TCP ports can be changed in the respective protocol settings. An example for the FTP server is shown for FTP in Figure 17. The FTP server is used for instance to update the firmware (see Section 9.1) or to upload a new data point configuration. Note that HTTP for the Web server can only be disabled on the console interface or by using the device configuration of the Configurator.



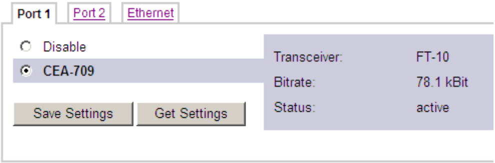
☑ TCP/IP
☑ FTP
☑ Telnet
☑ HTTP

FTP port: 21

Figure 17: FTP server configuration on the Ethernet port.

4.2.5 CEA-709 Configuration

The CEA-709 protocol can be enabled on the device’s ports Port1, Port2, etc. if available. To enable it, click the **CEA-709** radio button as shown in Figure 18. Note, that depending on the device model, other protocols on the same port will be disabled in this case. The protocol settings box on the right-hand side displays the current transceiver settings.



○ Disable
● CEA-709

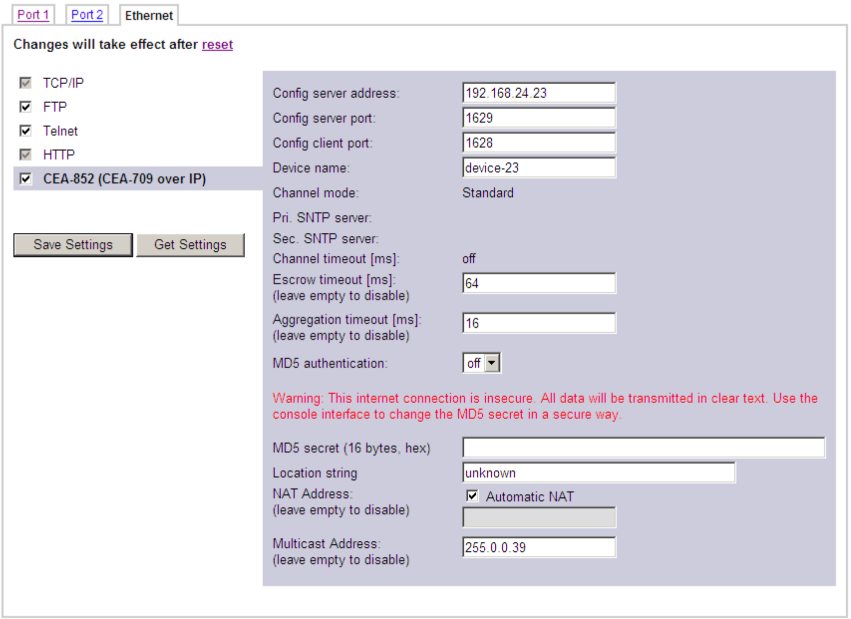
Transceiver: FT-10
Bitrate: 78.1 kBit
Status: active

Figure 18: CEA-709 Configuration Page.

4.2.6 CEA-852 Device Configuration

The CEA-852 protocol is only available on the Ethernet port. To enable CEA-852 on the device, select the **CEA-852 (CEA-709 over IP)** checkbox on the **Ethernet** tab of the port configuration page. Please note that on device models without a router or a proxy, the CEA-709 protocol on other ports will be disabled (e.g., LINX-100, L-Gate).

The CEA-852 protocol settings are displayed in the settings box on the right-hand side as shown in Figure 19. Typically, the device is added to an IP channel by entering the relevant information on a configuration server. The configuration server then contacts the CEA-852 device of the L-Gate and sends its configuration.



Changes will take effect after reset

☑ TCP/IP
☑ FTP
☑ Telnet
☑ HTTP
☑ CEA-852 (CEA-709 over IP)

Config server address:	192.168.24.23
Config server port:	1629
Config client port:	1628
Device name:	device-23
Channel mode:	Standard
Pri. SNTP server:	
Sec. SNTP server:	
Channel timeout [ms]:	off
Escrow timeout [ms]: (leave empty to disable)	64
Aggregation timeout [ms]: (leave empty to disable)	16
MD5 authentication:	off

Warning: This internet connection is insecure. All data will be transmitted in clear text. Use the console interface to change the MD5 secret in a secure way.

MD5 secret (16 bytes, hex)	
Location string	unknown
NAT Address: (leave empty to disable)	☑ Automatic NAT
Multicast Address: (leave empty to disable)	255.0.0.39

Figure 19: CEA-852 Device Configuration Page

The field **Config server address** and **Config server port** display the IP address and port of the configuration server, which manages the L-Gate and the IP channel. The field **Config client port** represents the IP port of the L-Gate's CEA-852 device. This setting should be left at its default (1628) unless there are more than one CEA-852 devices operating behind a single NAT router. Please refer to the L-IP User Manual [1] to learn more about NAT configuration.

In the field **Device name** the user can enter a descriptive name for the L-Gate, which will appear in the IP channel to identify this device. You can enter a device name with up to 15 characters. It is recommended to use unique device names throughout the IP channel.

The **Channel mode** field reflects the current channel mode of the CEA-852 device. It is configured by the configuration server. If there are any two devices in the channel which use the same IP address but different ports (e.g., multiple L-Gate behind one NAT router) the channel switches to **Extended NAT mode**. Please refer to the L-IP User Manual [1] to learn more about configuring the Extended NAT mode in the configuration server.

The configuration server sets the **SNTP server** addresses and the **Channel timeout**.

The filed **Escrow timeout** defines how long the CEA-852 device on the L-Gate waits for out-of-sequence CEA-852 data packets before they are discarded. Please enter the time in ms or '0' to disable escrowing. The maximum time is 255 ms.

The field **Aggregation timeout** defines the time interval in which multiple CEA-709 packets are combined into a single CEA-852 data packet. Please enter the time in ms or '0' to disable aggregation. The maximum time is 255 ms. Note that disabling aggregation will negatively affect the performance of the CEA-852 device of the L-Gate.

The field **MD5 authentication** enables or disables MD5 authentication. Note that MD5 authentication cannot be used together with the Echelon's *i*.LON 1000 since the *i*.LON 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i*.LON 600. In the following field **MD5 secret** enter the 16-byte MD5 secret. Note that for security purposes the active MD5 secret is not displayed. You may enter the 16 bytes as one string or with spaces between each byte, e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

Also note that entering the MD5 secret on the Web interface may pose a security risk. Since the information is transmitted over the network it can be subject for eavesdroppers on the line. It is recommended to either use a cross-over cable.

In the field **Location string** the user can enter a descriptive test which identifies the physical location of the L-Gate. A location string can have a maximum length of 255 characters. This is optional and for informational purposes only.

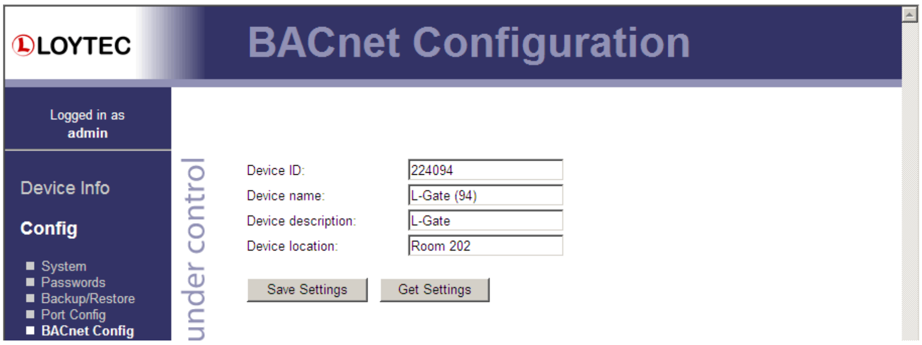
If the CEA-852 device on the L-Gate is used behind a NAT router, the public IP address of the NAT router or firewall must be known. To automatically detect the NAT address leave the **Auto-NAT** checkmark enabled.

The **Multicast Address** field allows the user to add the CEA-852 device of the L-Gate into a multi-cast group for the CEA-852 IP channel. Enter the channel's IP multi-cast address here. Please contact your system administrator on how to obtain a valid multi-cast address. To learn when it is beneficial to use multi-cast addresses in your channel please refer to the L-IP User Manual [1].

4.2.7 BACnet Configuration

Figure 20 shows the BACnet device configuration page. This configuration page allows setting the **Device ID**, which is the instance part of the Object_Identifier property of the BACnet Device object. The field **Device name** holds the name of the BACnet device object (property Object_Name).

Important: ***The device ID and device name must be unique within the BACnet internetwork.***



Device ID: 224094
Device name: L-Gate (94)
Device description: L-Gate
Device location: Room 202

Figure 20: BACnet Device Configuration.

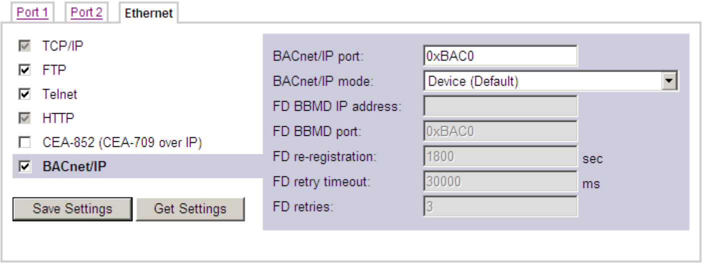
Further, the description and location can be configured. These configuration items correspond to the properties Description, and Location respectively of the BACnet Device object.

On the settings for BACnet/IP refer to Section 4.2.8. For configuring the MS/TP data link refer to Section 4.2.9.

4.2.8 BACnet/IP Configuration

The BACnet/IP protocol is available on the Ethernet port. To enable BACnet/IP on the device, select the **BACnet/IP** checkbox on the Ethernet tab of the port configuration page. Please note that on device models without a router, the BACnet MS/TP protocol on other ports will be disabled (e.g., LINX-200, L-Gate).

The BACnet/IP protocol settings are displayed in the settings box on the right-hand side as shown in Figure 21. If the BACnet/IP network uses a non-default UDP port number other than 47808/0xBAC0, enter this port in the **BACnet/IP** port field. Enter '0' in this field for switching back to the default setting.



☑ TCP/IP
☑ FTP
☑ Telnet
☑ HTTP
□ CEA-852 (CEA-709 over IP)
☑ BACnet/IP

BACnet/IP port:	0xBAC0	
BACnet/IP mode:	Device (Default)	
FD BBMD IP address:		
FD BBMD port:	0xBAC0	
FD re-registration:	1800	sec
FD retry timeout:	30000	ms
FD retries:	3	

Figure 21: BACnet/IP Configuration.

In the field **BACnet/IP mode** the operation mode of the device is selected:

- **Device** (Default): In this mode the device operates as a regular BACnet/IP device on the local network without other advanced features.

- **Foreign Device** (FD): In this mode, the device registers at an existing BBMD in the BACnet/IP network as a foreign device. It is used, if the device is located as a single BACnet/IP device on a remote IP subnet or behind a NAT router. If operated as a foreign device behind a NAT router, port forwarding to the BACnet/IP port (UDP, default port 0xBAC0) and optionally to the Web server and FTP server port (TCP, default port 80 and 21) must be setup in the NAT router. If foreign device is selected, the following, additional settings must be made:

    - **FD BBMD IP address** and **FD BBMD port**: IP address and port of the remote BBMD the device registers at as a foreign device.

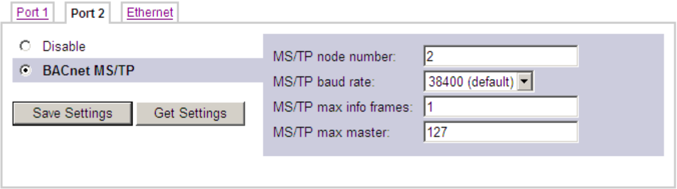
    - **FD re-registration**: A foreign device must periodically re-register at a BBMD. Here you can setup the corresponding interval. The default is 1800 seconds.

    - **FD retry timeout** and **FD retries**: Here you can specify the behavior, if registration does not work instantly. These values should be left at default: 30000ms / 3 retries.

- **Broadcast Management Device** (BBMD): This option is available on the L-Gate. It is the same as **Device** but the BBMD function is enabled (see Section 4.2.10).

4.2.9 MS/TP Configuration

The BACnet MS/TP protocol can be enabled on the device's port Port2 if available. To enable it, click the **BACnet MS/TP** radio button as shown in Figure 22. Note, that depending on the device model, other protocols on the same port will be disabled in this case. On the L-Gate the MS/TP port is not enabled by default.



○ Disable
● BACnet MS/TP

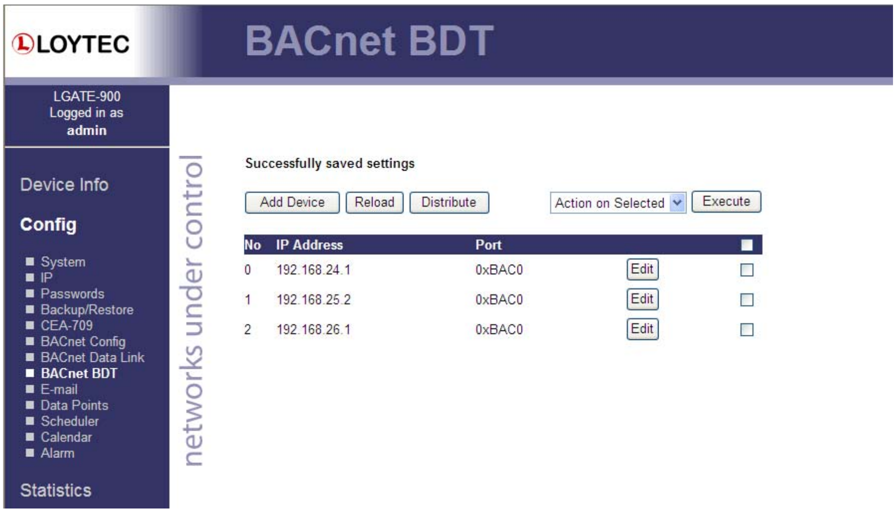
MS/TP node number:	2
MS/TP baud rate:	38400 (default)
MS/TP max info frames:	1
MS/TP max master:	127

Figure 22: MS/TP Configuration.

The MS/TP protocol settings are displayed in the settings box on the right-hand side as shown in Figure 22. Mandatory settings that have to be made are the **MS/TP node number** and the **MS/TP baud rate.** The MS/TP node number determines the physical address of the device on the MS/TP channel and must be in the range from '0' to the number configured with the **MS/TP max master** configuration option. It must be unique within the MS/TP channel. The baud rate on the MS/TP channel can be set to 9600, 19200, 38400, and 76800 baud. It is strongly recommended to leave the **MS/TP max info frames** and the **MS/TP max master** configuration options at their default settings.

4.2.10 BACnet BDT (Broadcast Distribution Table)

The BBMD function is only available on the L-Gate. The BBMD function is needed when a BACnet/IP network spans over several IP subnets separated by IP routers. If the device is configured as a BBMD (see Section 4.2.7), the BDT (Broadcast Distribution Table) specifies all other BBMDs of the BACnet/IP network. The BDT is shown in Figure 23.



Successfully saved settings

No	IP Address	Port		□
0	192.168.24.1	0xBAC0	Edit	□
1	192.168.25.2	0xBAC0	Edit	□
2	192.168.26.1	0xBAC0	Edit	□

Figure 23: BACnet Broadcast Distribution Table.

By clicking **Add Device** new BBMDs (IP address and port) can be added. With **Action on Selected** and selecting existing entries, certain BBMDs can be deleted again from the table. To commit the finished table, device must be rebooted (see Section 4.4).

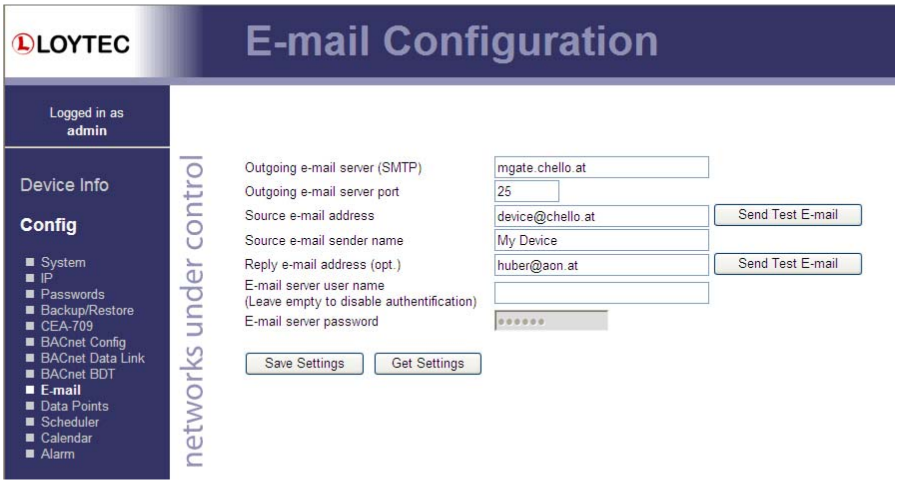
4.2.11 E-Mail Configuration

The Web interface provides the e-mail configuration page to set up an e-mail account, which is used to send e-mails. The content and time when E-mails are sent is configured through the Configurator software (see Section 6.11). The E-Mail configuration page is shown in Figure 24.

In the field for the outgoing e-mail server, enter the SMTP server of your Internet provider. Typically, the SMTP server port can be left at 25. In the field **Source E-mail Address**, enter the e-mail address of the device’s e-mail account. In the field **Source E-mail Sender Name** enter a name that the e-mail will display as the source name. Note, that only ASCII characters are allowed in the name. If replies shall be sent to another e-mail address, specify this in the **Reply E-mail Address**.

If the provider’s SMTP server requires authentication, enter the required user name and password. Note, that only username/password is supported. SSL/TLS authentication is not supported by the L-Gate (e.g., Hotmail, gmail cannot be used).

To verify the E-Mail configuration, reboot the device to let the changes take effect and return to the E-Mail configuration page. Then press one of the **Send Test E-Mail** buttons. Note, that a DNS server must be configured in the IP settings (see Section 4.2.4) to resolve the E-Mail server host name. The Web UI displays a warning message at the top of the page, if the DNS configuration is missing. Results of sending the test E-Mail are logged in the system log for further analysis of an existing problem (see Section 4.3.1).



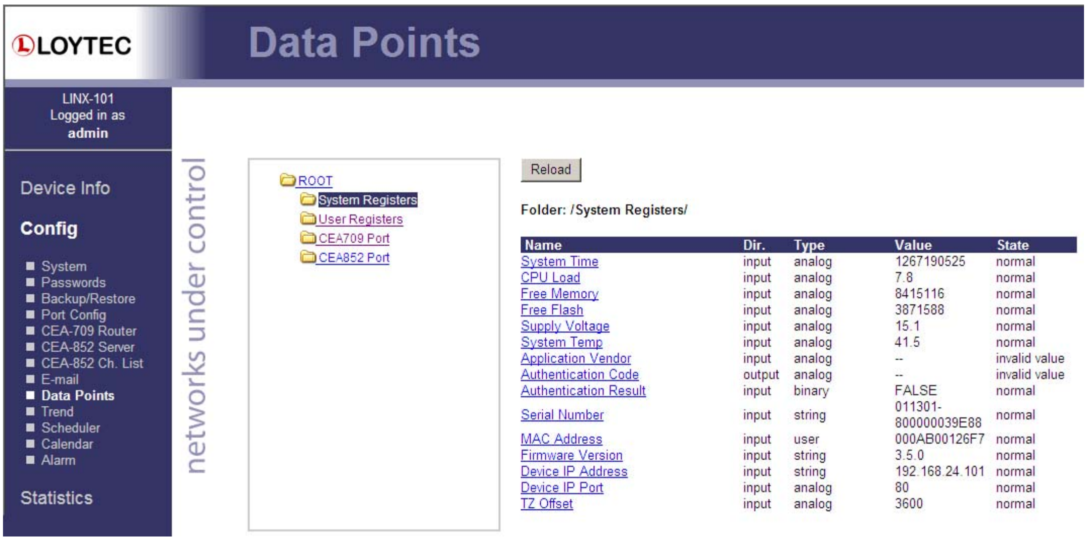
Outgoing e-mail server (SMTP)	mgate.chello.at
Outgoing e-mail server port	25
Source e-mail address	device@chello.at
Source e-mail sender name	My Device
Reply e-mail address (opt.)	huber@aon.at
E-mail server user name (Leave empty to disable authentification)	
E-mail server password	••••••

Figure 24: E-Mail Configuration Page

4.2.12 Data Points

The device’s Web interface provides a data point page, which lists all configured data points on the L-Gate. An example is shown in Figure 25. The data point page contains a tree view. Clicking on a particular tree item fills the right part of the page with a data point list of that tree level and all levels below. Thus, one can get an easy overview of all data points.

The data point list displays the data point name, direction, type, current value, and data point state. Inactive points are displayed in gray. If the data point list does not fit on one page, there are page enumerator links at the bottom. Important data point states and their implications are listed in Table 5.



Folder: /System Registers/

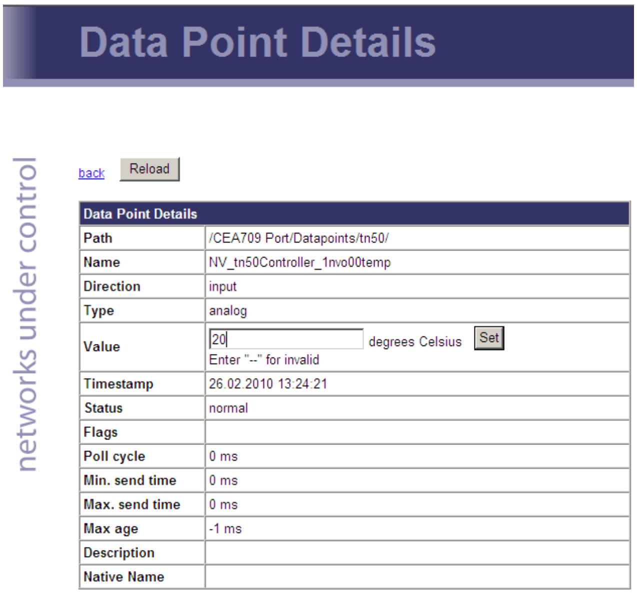
Name	Dir.	Type	Value	State
System Time	input	analog	1267190525	normal
CPU Load	input	analog	7.8	normal
Free Memory	input	analog	8415116	normal
Free Flash	input	analog	3871588	normal
Supply Voltage	input	analog	15.1	normal
System Temp	input	analog	41.5	normal
Application Vendor	input	analog	--	invalid value
Authentication Code	output	analog	--	invalid value
Authentication Result	input	binary	FALSE	normal
Serial Number	input	string	011301-800000039E88	normal
MAC Address	input	user	000AB00126F7	normal
Firmware Version	input	string	3.5.0	normal
Device IP Address	input	string	192.168.24.101	normal
Device IP Port	input	analog	80	normal
TZ Offset	input	analog	3600	normal

Figure 25: Data point page

Data Point Status	Description
normal	The data point is in normal operation state and possesses a value.
invalid value	The data point has no valid value.
offline (config)	The data point has a value but it is not reflected on the network due to a configuration error (not commissioned, no binding, no client mapping, etc.)
offline	The data point has a value but it is not reflected on the network due to a communication error (e.g., the peer node is not online).
unreliable (offline)	The data point has a value but it is considered unreliable because it was derived from a source, which was offline (e.g., the value was fed from a connection, where the source is offline).
unreliable (range)	The data point has a value but it is considered unreliable because the value source specified an out-of-range value. The value is limited to the supported range.
unreliable	The data point has a value but it is considered unreliable for an unspecified reason.
not configured	The data point is mapped to a port, which is not configured (e.g., the port is disabled).
Line grayed-out	The data point is inactive. Values can be written but no network communication is triggered. This can be the case, if a data point is not used in the configuration or it is connected to a BACnet server object, which is not present on the device.

Table 5: Data Point States.

The data point names are links. Clicking on such a link opens a detailed page on that data point. If the data point supports it, the user can also enter a new data point value as depicted in Figure 26. The **Status** field is discussed in Table 5. The **Flags**, **Poll cycle**, **Min/Max send time** and **Max age** fields are the common timing parameters for the data point. See Section 5.2.2 for a closer discussion on timing parameters.



Data Point Details	
Path	/CEA709 Port/Datapoints/tn50/
Name	NV_tn50Controller_1nvo00temp
Direction	input
Type	analog
Value	20 degrees Celsius Enter "--" for invalid
Timestamp	26.02.2010 13:24:21
Status	normal
Flags	
Poll cycle	0 ms
Min. send time	0 ms
Max. send time	0 ms
Max age	-1 ms
Description	
Native Name	

Figure 26: Data point details page

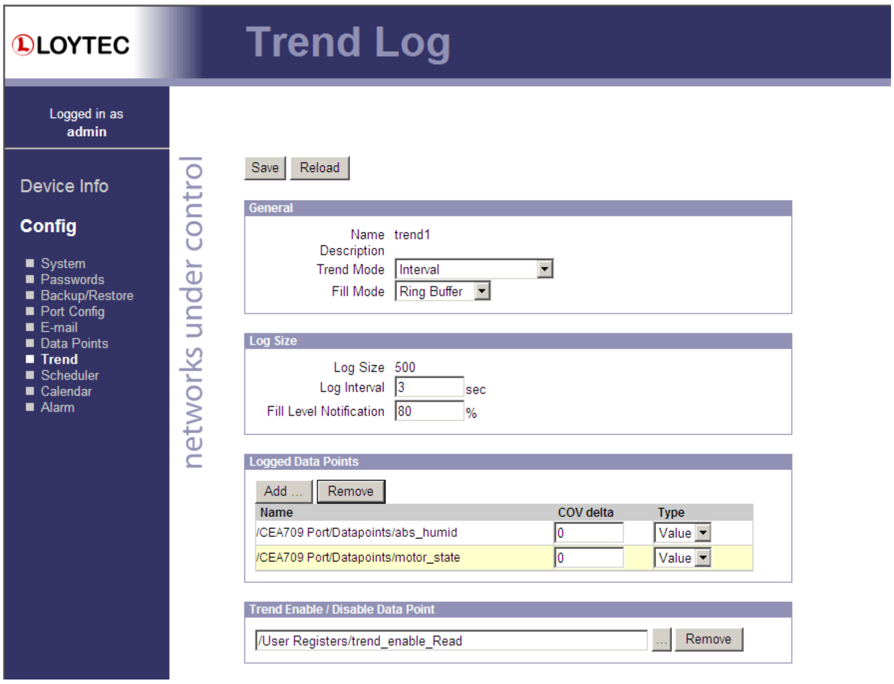
Clicking on the **Set** button writes the new value to the device’s data server. When setting a value, the Web page displays the status of the action:

- **Successfully set value**: The new value has been successfully set in the data point and the update has been sent on the network, if it is a network data point.

- **Could not send value update**: The new value has been set but it has not been sent out on the network. The reason can be that the peer node is currently offline or there is a configuration error. The data point status reflects this error.
- **Could not set value (error code)**: The new value has not been set because of an internal error. Please contact LOYTEC with the error code.

4.2.13 Trend

The Web interface provides a configuration page to re-configure trend logs at run-time. The changes made to the trend logs take effect immediately without the needs for a reboot of the device. Allocating new trend logs can only be done in the configuration software (see Section 6.14.1). The trend log main page displays all available trend logs. Click on the trend log to be edited. This opens the trend log configuration page. An example is shown in Figure 27.



General
Name trend1
Description
Trend Mode Interval
Fill Mode Ring Buffer

Log Size
Log Size 500
Log Interval 3 sec
Fill Level Notification 80 %

Logged Data Points

Name	COV delta	Type
/CEA709 Port/Datapoints/abs_humid	0	Value
/CEA709 Port/Datapoints/motor_state	0	Value

Trend Enable / Disable Data Point
/User Registers/trend_enable_Read

Figure 27: Trend log configuration page.

The user can change the **Trend Mode**, the **Fill Mode**, the **Log Interval** and the **Fill Level Notification**. Furthermore, data points can be added to the trend log by clicking the **Add…** button. A data point selector dialog opens. Click on a data point for adding it. For removing a data point from the trend log, click on it in the **Logged Data Points** list and hit the **Remove** button. Save the changes made by clicking the **Save** button. For more information on how a trend log can be configured please refer to the Configurator Section 6.14.

Note: *This firmware version does not allow configuring trended data points on local BACnet trend logs. The feature is currently limited to CEA-709 trend logs.*

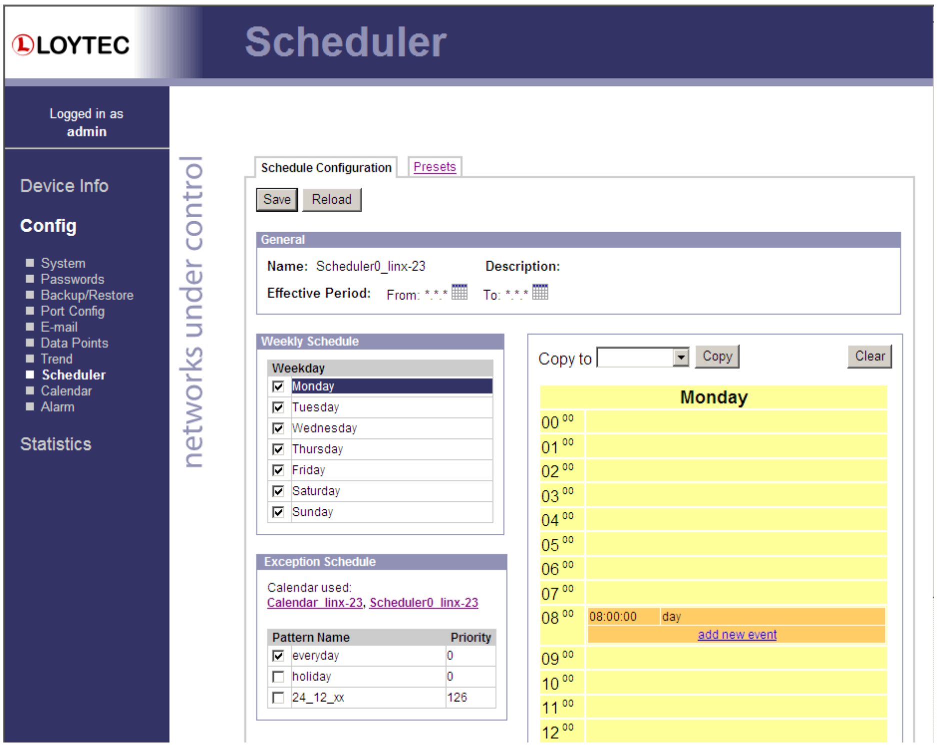
4.2.14 Scheduler

The Web interface provides the scheduler page to edit its schedules at run-time, i.e., change the times and values that shall be scheduled. Allocating new schedules can only be done in the configuration software (see Section 6.12). The scheduler main page displays all available schedules. Click on the schedule to be edited. This opens the scheduler page. An example is shown in Figure 28.

The **effective period** defines when this schedule shall be in effect. Leave **From** and **To** at '*.*.*' to make this schedule always in-effect. Otherwise enter dates, such as '30.1.2000'. To entirely disable a scheduler de-select the **Enable Schedule** check box.

Schedules are defined per day. On the left-hand side, the weekdays **Monday** through **Sunday** can be selected, or exception days from the calendar, e.g. Holidays. Once a day is selected, the times and values can be defined in the daily planner on the right-hand side. In the example shown in Figure 28, on Monday the value **day** is scheduled at **8:00am**. The same principle applies to **exception days**. **Exception days** override the settings of the normal weekday. Put a check mark on those exception days from the calendar, which shall be used in the schedule. To edit the date ranges of exception days click on the links to the used calendars, e.g., 'calendar' or 'Scheduler_1'. The 'Scheduler_1' is a calendar, which is embedded into the schedule and not accessible by other schedulers. For more information on how to set up schedules and calendars refer to Section 6.12.

To define actual values for the names such as **day** click on the tab **Presets** as shown in Figure 29. To define a new value, click on the button **Add Preset**. This adds a new column. Enter a new preset name (e.g., 'day'). Then enter values for the data points in the **preset** column. The **data point description** column displays the short-hand name defined in the configuration software. This description can also be changed on the Web UI.



General

Name: Scheduler0_linx-23 Description:

Effective Period: From: *.*.* To: *.*.*

Weekly Schedule

Weekday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Exception Schedule

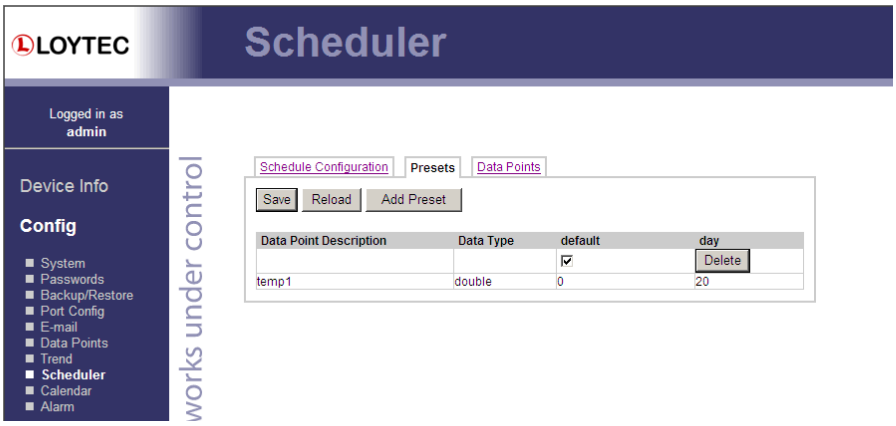
Calendar used:
Calendar_linx-23, Scheduler0_linx-23

Pattern Name	Priority
☑ everyday	0
☐ holiday	0
☐ 24_12_xx	126

Monday

00 00		
01 00		
02 00		
03 00		
04 00		
05 00		
06 00		
07 00		
08 00	08:00:00	day
09 00		
10 00		
11 00		
12 00		

Figure 28: Schedule Configuration Page



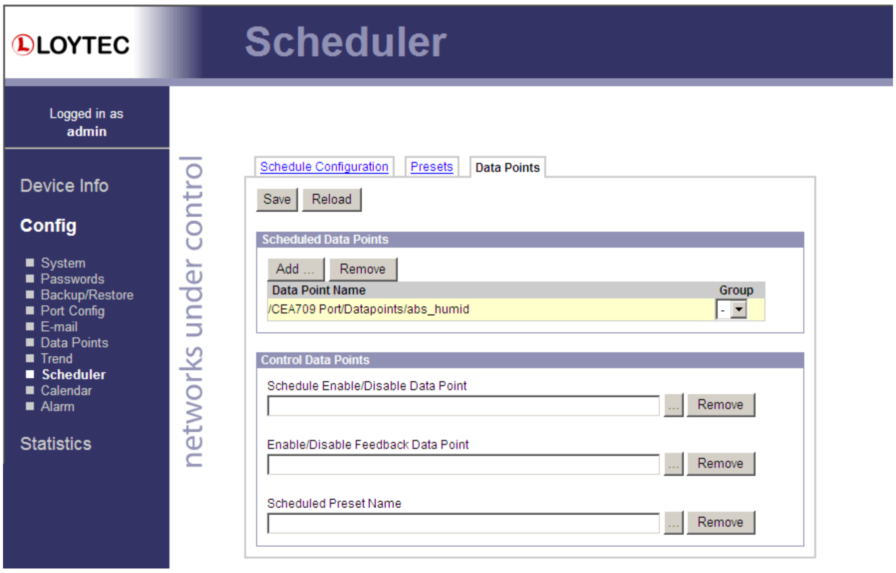
Data Point Description	Data Type	default	day
		☑	Delete
temp1	double	0	20

Figure 29: Scheduled Data Point Value Configuration Page

You can switch back and forth between the two tabs. Once the configuration is complete, click on the **Save** button. This updates the schedule in the device. Any changes made become effective immediately.

On local schedulers the Web UI also allows to reconfigure the scheduled data points. This change takes effect immediately without a reboot of the device. To add and remove data points to the scheduler, go to the **Data Points** tab. The configuration page is depicted in Figure 30. To add a new data point, click the **Add…** button. To remove a data point, select the data point in the list **Scheduled Data Points** by clicking on it and then press the **Remove** button. Finally, store the changes by clicking the **Save** button. After modifying the scheduled data points, go back to the Presets tab and enter descriptive value label names. For more information on how to configure a scheduler please refer to the Configurator Section 6.12.4.

Note: *This firmware version does not allow configuring scheduled data points on local BACnet schedulers. The feature is currently limited to CEA-709 schedulers.*



Scheduled Data Points

Data Point Name	Group
/CEA709 Port/Datapoints/abs_humid	-

Control Data Points

Schedule Enable/Disable Data Point

Enable/Disable Feedback Data Point

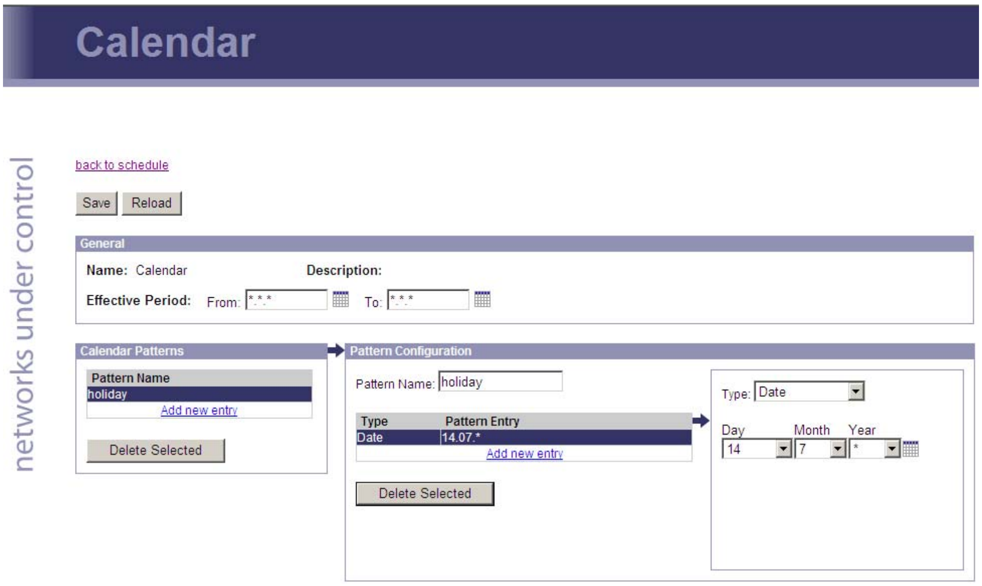
Scheduled Preset Name

Figure 30: Re-configure scheduled data points on the Web UI.

4.2.15 Calendar

The Web interface provides the calendar page to edit its calendars at run-time, i.e., change the exception days. The calendar main page displays all available calendars. Click on the calendar to be edited. This opens the calendar configuration page. An example is shown in Figure 31.

The **effective period** defines when this calendar shall be in effect. Leave **From** and **To** at '*.*.*' to make this calendar always in-effect. Otherwise enter dates, such as '30.1.2000'.



Name: Calendar
Description:
Effective Period: From: *.*.* To: *.*.*

Pattern Name
holiday

Pattern Name: holiday

Type	Pattern Entry
Date	14.07.*

Type: Date

Day	Month	Year
14	7	*

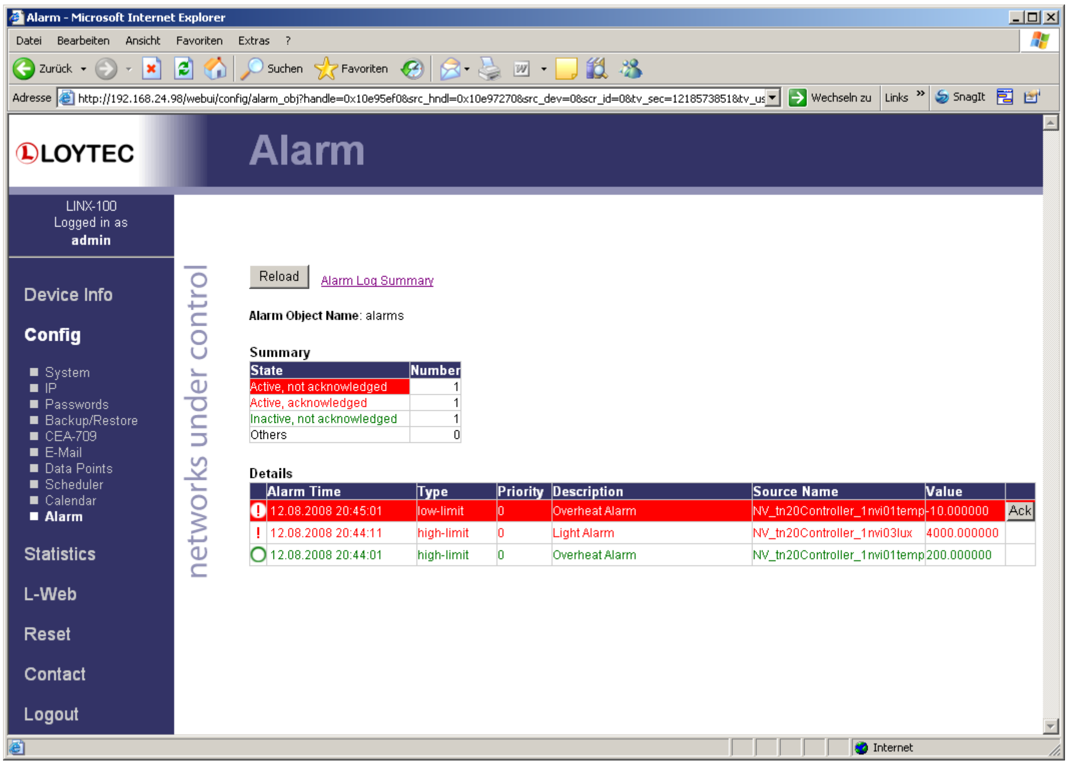
Figure 31: Calendar Configuration Page

On the remainder of this page work from left to right. Click on a calendar pattern or create a new calendar pattern by clicking **Add new entry**. A calendar pattern defines a set of pattern entries, which defines the actual dates or date ranges. In the example in Figure 31 the calendar pattern **Holidays** is selected.

In the **Pattern Configuration** box, the calendar pattern's name can be edited. It also lists the entries. New entries can be added by clicking **Add new entry**. Existing entries can be selected and edited in the box on the right-hand side. In the example in Figure 31 the date **14.7.*** is selected, which means "The 14.7. of every year". Other entry types such as **Date Range** and **Week-and-Day** can be selected. See Section 5.4.3 for more information about defining exception dates.

4.2.16 Alarm

The Web interface provides the alarm page to view the currently pending alarms of its alarm data points. The alarm main page displays all available alarm data points. Alarm objects which have active alarms are displayed in red. Click on the alarm object to be viewed. This opens the alarm summary page. An example is shown in Figure 31.



Reload Alarm Log Summary

Alarm Object Name: alarms

Summary

State	Number
Active, not acknowledged	1
Active, acknowledged	1
Inactive, not acknowledged	1
Others	0

Details

	Alarm Time	Type	Priority	Description	Source Name	Value	
!	12.08.2008 20:45:01	low-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	-10.000000	Ack
!	12.08.2008 20:44:11	high-limit	0	Light Alarm	NV_tn20Controller_1nvi03lux	4000.000000	
○	12.08.2008 20:44:01	high-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	200.000000	

Figure 32: Alarm Summary Page

Active alarms are highlighted red. Inactive alarms which have not been acknowledged are rendered in green. Alarms that can be acknowledged have an **Ack** button. Press on the **Ack** button to acknowledge the alarm. Depending on the technology, this and older alarm records will be acknowledged. Acknowledged, active alarms are rendered in red. Click on **Reload** to refresh your alarm list.

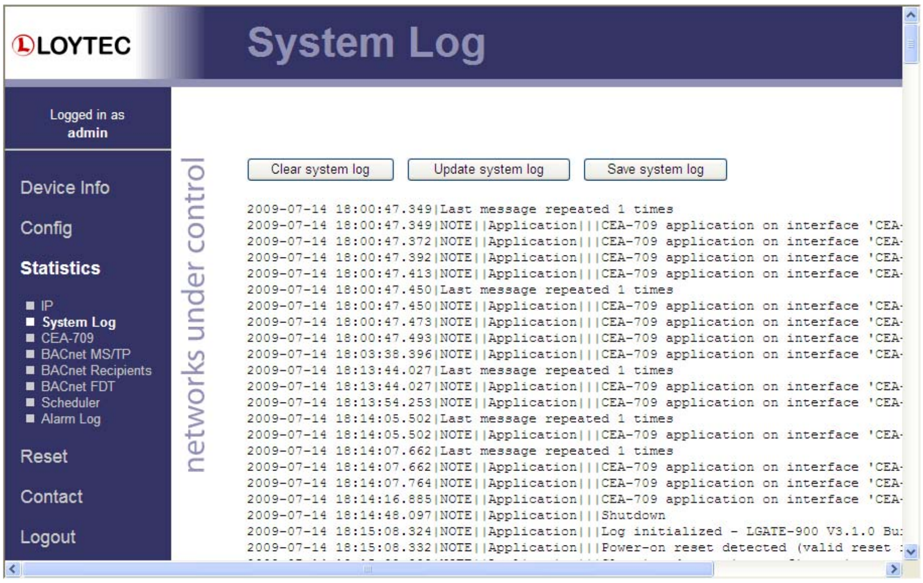
Inactive alarms that have been acknowledged disappear from the list. To record historical information about those alarms, the alarm log must be used. See Section 4.3.8 for the alarm log Web interface.

4.3 Device Statistics

The device statistics pages provide advanced statistics information about the CEA-852 device, BACnet device, and the Ethernet interface.

4.3.1 System Log

The System Log page prints all messages stored in the system log of the device. An example is shown in Figure 38. This log data is important for trouble-shooting. It contains log entries for reboots and abnormal operating conditions. When contacting LOYTEC support, have a copy of this log ready.

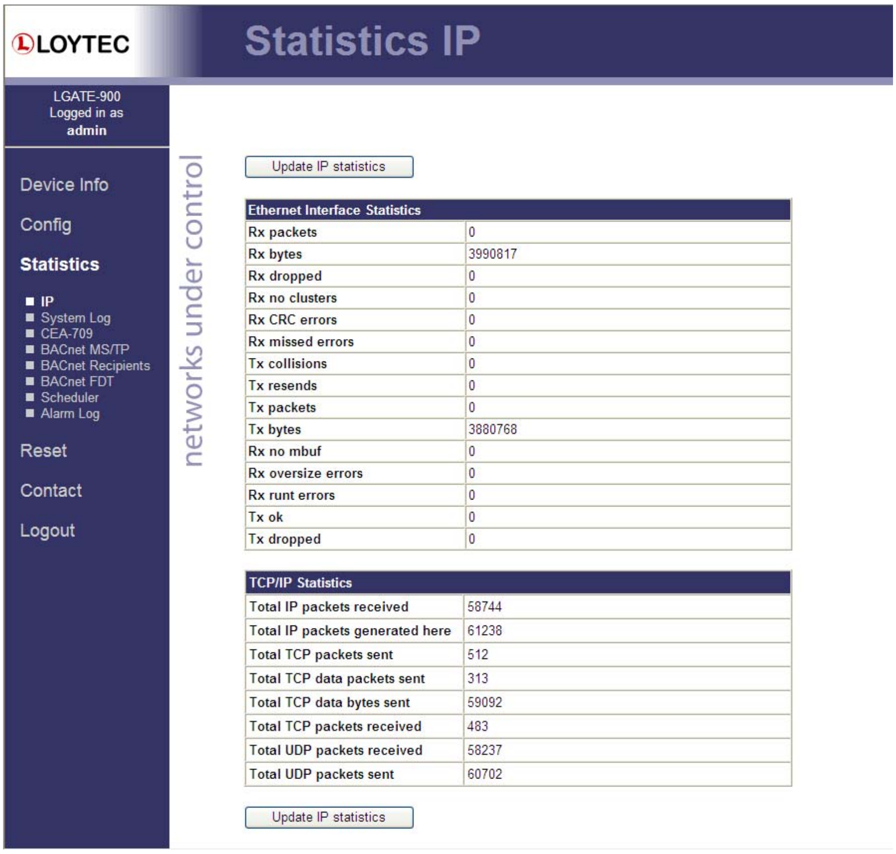


```
2009-07-14 18:00:47.349|Last message repeated 1 times
2009-07-14 18:00:47.349|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:00:47.372|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:00:47.392|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:00:47.413|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:00:47.450|Last message repeated 1 times
2009-07-14 18:00:47.450|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:00:47.473|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:00:47.493|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:03:38.396|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:13:44.027|Last message repeated 1 times
2009-07-14 18:13:44.027|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:13:54.253|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:14:05.502|Last message repeated 1 times
2009-07-14 18:14:05.502|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:14:07.662|Last message repeated 1 times
2009-07-14 18:14:07.662|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:14:07.764|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:14:16.885|NOTE||Application|||CEA-709 application on interface 'CEA-
2009-07-14 18:14:48.097|NOTE||Application|||Shutdown
2009-07-14 18:15:08.324|NOTE||Application|||Log initialized - LGATE-900 V3.1.0 Bu
2009-07-14 18:15:08.332|NOTE||Application|||Power-on reset detected (valid reset :
```

Figure 33: System Log Page.

4.3.2 IP Statistics

Figure 34 shows the IP statistics page. It allows finding possible problems related to the IP communication. Specifically any detected IP address conflicts are displayed (if the L-Gate's IP address conflicts with a different host on the network).



Ethernet Interface Statistics	
Rx packets	0
Rx bytes	3990817
Rx dropped	0
Rx no clusters	0
Rx CRC errors	0
Rx missed errors	0
Tx collisions	0
Tx resends	0
Tx packets	0
Tx bytes	3880768
Rx no mbuf	0
Rx oversize errors	0
Rx runt errors	0
Tx ok	0
Tx dropped	0

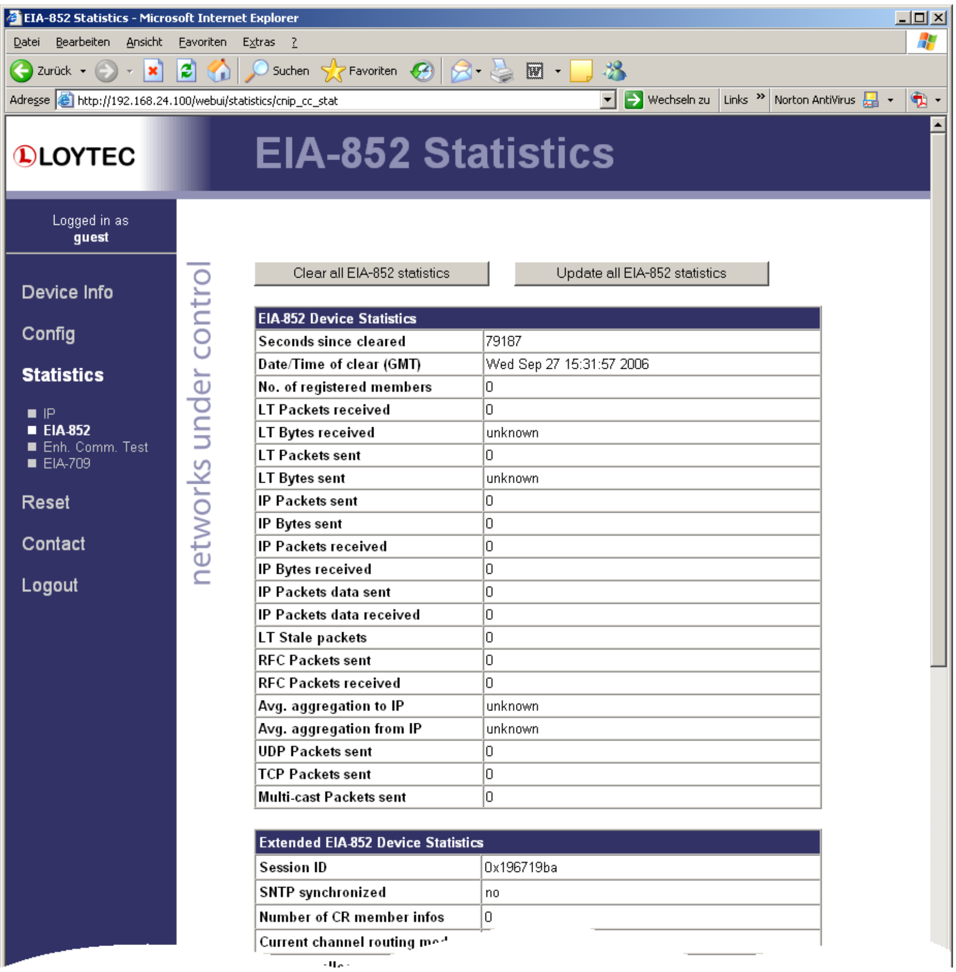
TCP/IP Statistics	
Total IP packets received	58744
Total IP packets generated here	61238
Total TCP packets sent	512
Total TCP data packets sent	313
Total TCP data bytes sent	59092
Total TCP packets received	483
Total UDP packets received	58237
Total UDP packets sent	60702

Update IP statistics

Figure 34: IP Statistics Page

4.3.3 CEA-852 Statistics

The CEA-852 statistics page displays the statistics data of the CEA-852 device on the device. The upper part of the CEA-852 statistics page is depicted in Figure 35. To update the statistics data press the button **Update all CEA-852 statistics**. To reset all statistics counters to zero, click on the button **Clear all CEA-852 statistics**. The field **Date/Time of clear** will reflect the time of the last counter reset.


EIA-852 Statistics - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse http://192.168.24.100/webui/statistics/cnip_cc_stat
Wechseln zu Links Norton AntiVirus
LOYTEC
EIA-852 Statistics
Logged in as guest
Device Info
Config
Statistics
IP
EIA-852
Enh. Comm. Test
EIA-709
Reset
Contact
Logout
networks under control
Clear all EIA-852 statistics
Update all EIA-852 statistics

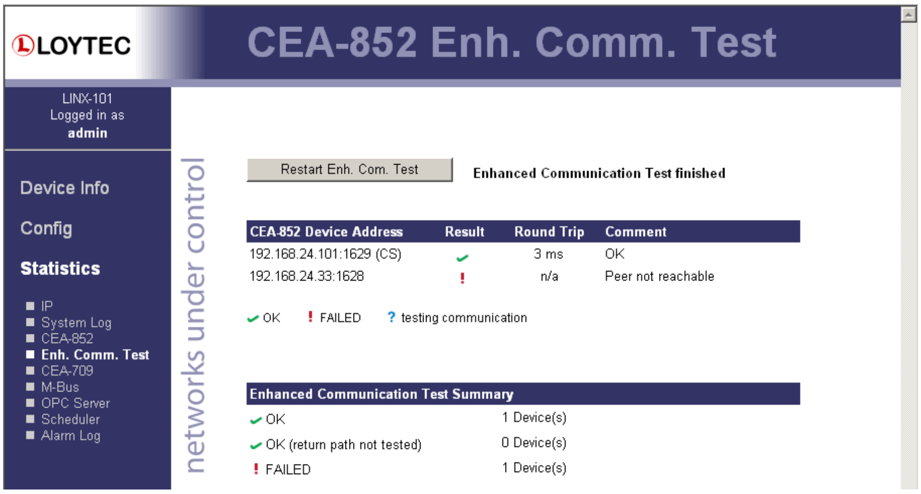
EIA-852 Device Statistics	
Seconds since cleared	79187
Date/Time of clear (GMT)	Wed Sep 27 15:31:57 2006
No. of registered members	0
LT Packets received	0
LT Bytes received	unknown
LT Packets sent	0
LT Bytes sent	unknown
IP Packets sent	0
IP Bytes sent	0
IP Packets received	0
IP Bytes received	0
IP Packets data sent	0
IP Packets data received	0
LT Stale packets	0
RFC Packets sent	0
RFC Packets received	0
Avg. aggregation to IP	unknown
Avg. aggregation from IP	unknown
UDP Packets sent	0
TCP Packets sent	0
Multi-cast Packets sent	0

Extended EIA-852 Device Statistics	
Session ID	0x196719ba
SNTP synchronized	no
Number of CR member infos	0
Current channel routing mo	

Figure 35: Part of the CEA-852 Statistics Page

4.3.4 Enhanced Communications Test

The Enhanced Communications Test allows testing the CEA-852 communication path between the CEA-852 device on the L-Gate and other CEA-852 devices as well as the configuration server. The test thoroughly diagnoses the paths between individual members of the IP channel and the configuration server in each direction. Port-forwarding problems are recognized. For older devices or devices by other manufacturers, which do not support the enhanced test features, the test passes as soon as a device is reachable, but adds a comment, that the return path could not be tested. A typical output is shown in Figure 36.



Enhanced Communication Test finished

CEA-852 Device Address	Result	Round Trip	Comment
192.168.24.101:1629 (CS)	✓	3 ms	OK
192.168.24.33:1628	!	n/a	Peer not reachable

✓ OK ! FAILED ? testing communication

Enhanced Communication Test Summary	
✓ OK	1 Device(s)
✓ OK (return path not tested)	0 Device(s)
! FAILED	1 Device(s)

Figure 36: Enhanced Communication Test Output

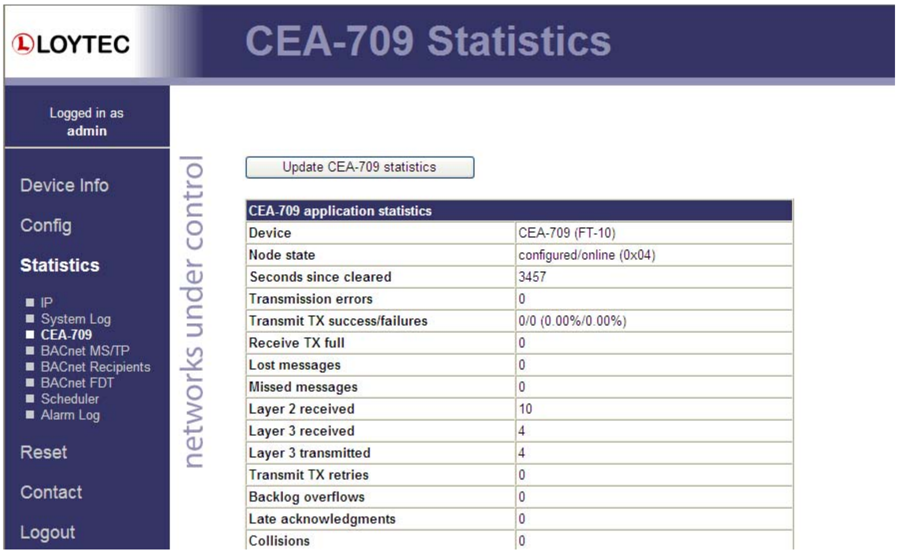
The Round Trip Time (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the device. It is a measure for general network delay. If the test to a specific member fails, a text is displayed to describe the possible source of the problem. The reasons for failure are summarized in Table 6.

Text displayed (Web icon)	Meaning
OK, Return path not tested (green checkmark)	Displayed for a device which is reachable but which does not support the feature to test the return path (device sending to this CEA-852 device). Therefore a potential NAT router configuration error cannot be detected. If the tested device is an L-IP, it is recommended to upgrade this L-IP to 3.0 or higher.
Not reachable/not supported (red exclamation)	This is displayed for the CS if it is not reachable or the CS does not support this test. To remove this uncertainty it is recommended to upgrade the L-IP to 3.0 or higher.
Local NAT config. Error (red exclamation)	This is displayed if the CEA-852 device of the LINX-10X is located behind a NAT router or firewall, and the port-forwarding in the NAT-Router (usually 1628) or the filter table of the firewall is incorrect.
Peer not reachable (red exclamation)	Displayed for a device, if it is not reachable. No RTT is displayed. The device is either not online, not connected to the network, has no IP address, or is not reachable behind its NAT router. Execute this test on the suspicious device to determine any NAT configuration problem.

Table 6: Possible Communication Problems.

4.3.5 CEA-709 Statistics

The CEA-709 statistics page displays statistics data of the CEA-709 port on the L-Gate as shown in Figure 37. This data can be used to troubleshoot networking problems. To update the data, click on the button **Update CEA-709 statistics**.

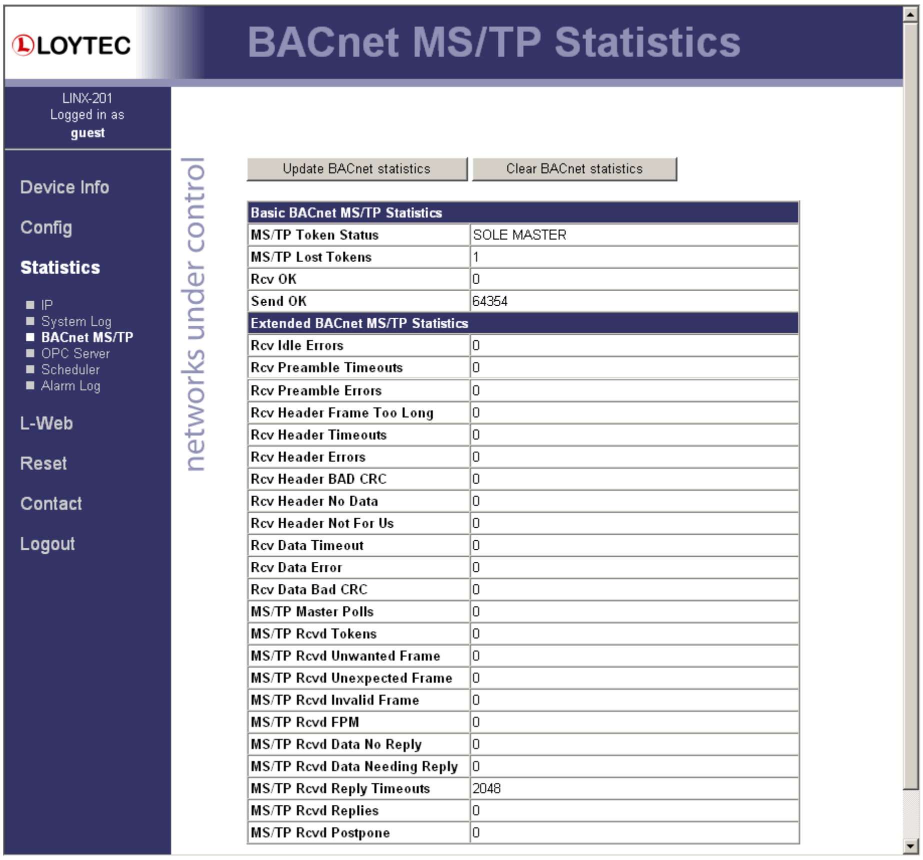


CEA-709 application statistics	
Device	CEA-709 (FT-10)
Node state	configured/online (0x04)
Seconds since cleared	3457
Transmission errors	0
Transmit TX success/failures	0/0 (0.00%/0.00%)
Receive TX full	0
Lost messages	0
Missed messages	0
Layer 2 received	10
Layer 3 received	4
Layer 3 transmitted	4
Transmit TX retries	0
Backlog overflows	0
Late acknowledgments	0
Collisions	0

Figure 37: CEA-709 Statistics Page

4.3.6 BACnet MS/TP Statistics

The BACnet MS/TP statistics page is only available, when the BACnet port is configured for the MS/TP data link layer (see Section 4.2.7). An example is shown in Figure 38. The separated part on the top of the table contains the most important statistics data.



Basic BACnet MS/TP Statistics	
MS/TP Token Status	SOLE MASTER
MS/TP Lost Tokens	1
Rcv OK	0
Send OK	64354
Extended BACnet MS/TP Statistics	
Rcv Idle Errors	0
Rcv Preamble Timeouts	0
Rcv Preamble Errors	0
Rcv Header Frame Too Long	0
Rcv Header Timeouts	0
Rcv Header Errors	0
Rcv Header BAD CRC	0
Rcv Header No Data	0
Rcv Header Not For Us	0
Rcv Data Timeout	0
Rcv Data Error	0
Rcv Data Bad CRC	0
MS/TP Master Polls	0
MS/TP Rcvd Tokens	0
MS/TP Rcvd Unwanted Frame	0
MS/TP Rcvd Unexpected Frame	0
MS/TP Rcvd Invalid Frame	0
MS/TP Rcvd FPM	0
MS/TP Rcvd Data No Reply	0
MS/TP Rcvd Data Needing Reply	0
MS/TP Rcvd Reply Timeouts	2048
MS/TP Rcvd Replies	0
MS/TP Rcvd Postpone	0

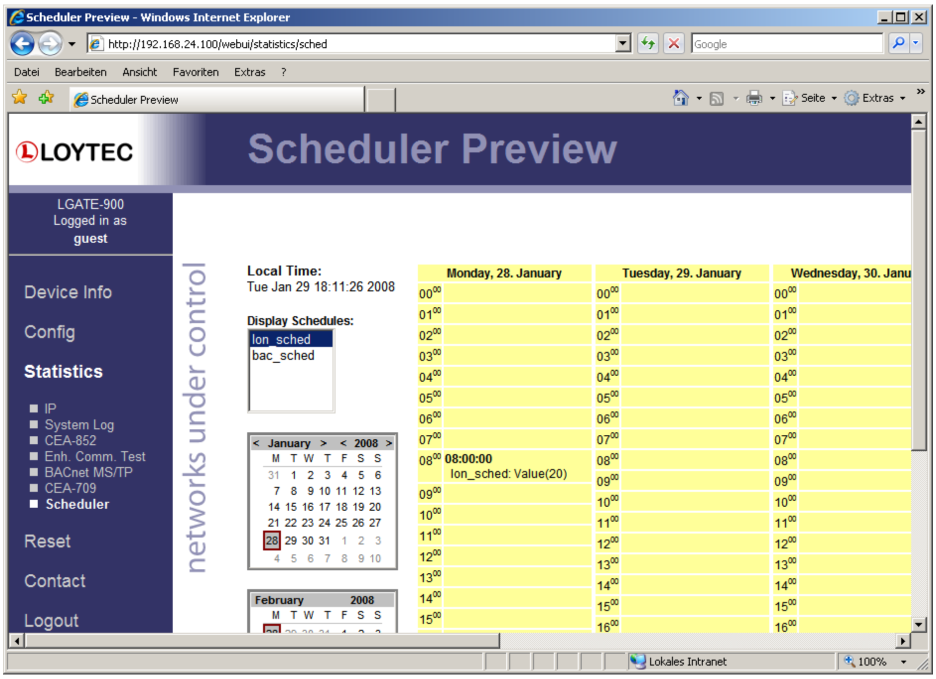
Figure 38: BACnet MS/TP Statistics Page

The MS/TP token status reports the current token passing state. In state **OK**, the token is circulating between the masters. This is the normal state, when multiple masters are on the MS/TP network. The state **SOLE MASTER** is the normal state when the device is the only master on the network. If there are multiple masters on the network, this state is a hint to a broken cable. In state **TOKEN LOST**, the token is currently not circulating.

The counter **MS/TP lost tokens** is an indicator for communication problems on the MST/TP network. If it increases, there is a cabling, ground, or termination problem. The counters **Rcv OK** and **Send OK** reflect the number of successfully received or transmitted MS/TP frames. Check these counters to verify that communication is flowing on the MS/TP segment.

4.3.7 Scheduler Statistics Page

The scheduler statistics page provides an overview of what is scheduled at which day and which time. In the **Display Schedules** list select a single schedule to view its scheduled values and times. Use the multi-select feature to get the overview of more schedules. An example is shown in Figure 39.



Local Time:
Tue Jan 29 18:11:26 2008

Display Schedules:
lon_sched
bac_sched

08:00:00
lon_sched: Value(20)

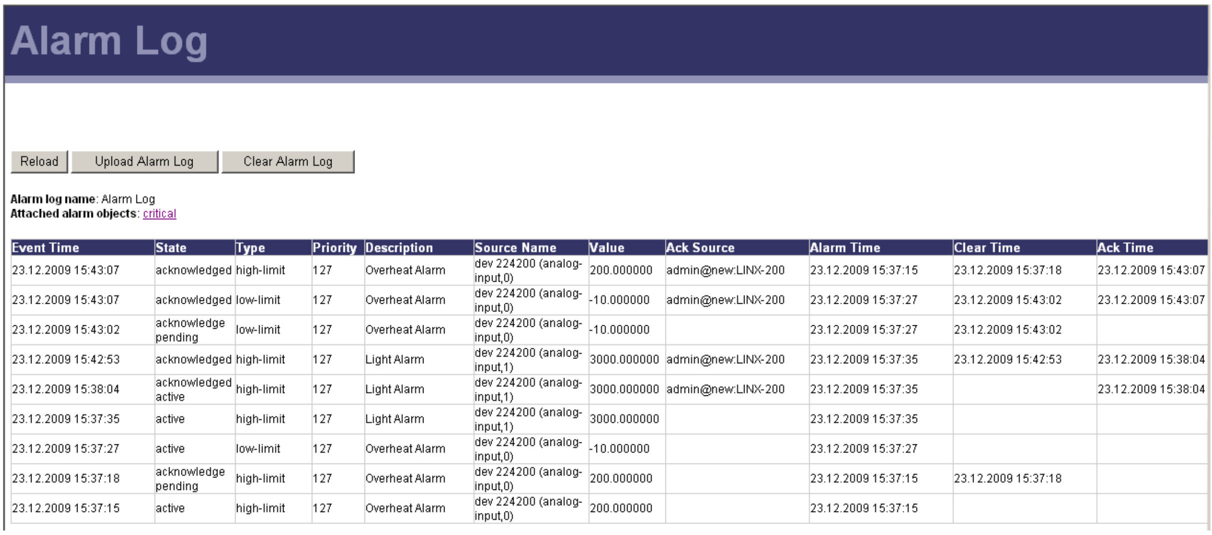
Figure 39: Scheduler Statistics Page

4.3.8 Alarm Log Page

The alarm log page provides an overview of all alarm logs on the system. Click on one of the links to view a specific alarm log. Each alarm log contains a historical log of alarm transitions. When an inactive and acknowledged alarm disappears from the alarm summary page (live list), the alarm log contains this last transition and maintains it over a reboot. An example is shown in Figure 40.

To refresh the alarm log contents click on the **Reload** button. Currently active alarms cannot be acknowledged in this historical view. Follow the link to the attached alarm objects to get to the respective live lists, where alarms can be acknowledged on the Web interface (see Section 4.2.16).

The alarm log contents can be uploaded from the device in a CSV formatted file. Click on the button **Upload Alarm Log** to upload the current log. To clear the log, press the button **Clear Alarm Log**. Please note, that this permanently purges all historical alarm log data of this alarm log.



Alarm log name: Alarm Log
Attached alarm objects: critical

Event Time	State	Type	Priority	Description	Source Name	Value	Ack Source	Alarm Time	Clear Time	Ack Time
23.12.2009 15:43:07	acknowledged	high-limit	127	Overheat Alarm	dev 224200 (analog-input,0)	200.000000	admin@new:LINX-200	23.12.2009 15:37:15	23.12.2009 15:37:18	23.12.2009 15:43:07
23.12.2009 15:43:07	acknowledged	low-limit	127	Overheat Alarm	dev 224200 (analog-input,0)	-10.000000	admin@new:LINX-200	23.12.2009 15:37:27	23.12.2009 15:43:02	23.12.2009 15:43:07
23.12.2009 15:43:02	acknowledge pending	low-limit	127	Overheat Alarm	dev 224200 (analog-input,0)	-10.000000		23.12.2009 15:37:27	23.12.2009 15:43:02	
23.12.2009 15:42:53	acknowledged	high-limit	127	Light Alarm	dev 224200 (analog-input,1)	3000.000000	admin@new:LINX-200	23.12.2009 15:37:35	23.12.2009 15:42:53	23.12.2009 15:38:04
23.12.2009 15:38:04	acknowledged active	high-limit	127	Light Alarm	dev 224200 (analog-input,1)	3000.000000	admin@new:LINX-200	23.12.2009 15:37:35		23.12.2009 15:38:04
23.12.2009 15:37:35	active	high-limit	127	Light Alarm	dev 224200 (analog-input,1)	3000.000000		23.12.2009 15:37:35		
23.12.2009 15:37:27	active	low-limit	127	Overheat Alarm	dev 224200 (analog-input,0)	-10.000000		23.12.2009 15:37:27		
23.12.2009 15:37:18	acknowledge pending	high-limit	127	Overheat Alarm	dev 224200 (analog-input,0)	200.000000		23.12.2009 15:37:15	23.12.2009 15:37:18	
23.12.2009 15:37:15	active	high-limit	127	Overheat Alarm	dev 224200 (analog-input,0)	200.000000		23.12.2009 15:37:15		

Figure 40: Alarm Log Page.

4.4 Reset, Contact, Logout

The menu item **Reset** allows two essential operations:

- Rebooting the L-Gate from a remote location, or
- resetting the data point configuration from a remote location. This option clears all data points and the entire port configuration. It leaves the IP settings intact.

The **Contact** item provides contact information and a link to the latest user manual and the latest firmware version.

The **Logout** item closes the current session.

5 Concepts

5.1 CEA-709/BACnet Gateway

The operating principle of the L-Gate is to connect data points of one network technology to data points of another technology. Data points in the CEA-709 network are known as network variables (NVs). For more information on this technology refer to Section 5.5. Data points in the BACnet technology are known as BACnet server objects. They have a specific type (e.g. analog input or binary output) and a set of properties, which describe the data point more closely. The actual value is stored in the “Present_Value”. For more information on this technology refer to Section 5.6.

The typical task in configuring the L-Gate consists of the following steps:

1. Selecting the data points of the network to be mapped (e.g., select the NVs in the CEA-709 network nodes or create new NVs)

2. Select or create matching counterparts of the other technology (e.g., create matching BACnet objects)

3. Create connections between the data points (e.g. connect NVs and BACnet objects).

The connection is the central part of the gateway functionality. It defines, which data points are mapped to which data points. Refer to Section 5.3 about the nature of connections in the device.

5.2 Data Points

5.2.1 Overview

Data points are part of the fundamental device concept to model process data. A data point is the basic input/output element on the device. Each data point has a value, a data type, a direction, and a set of meta-data describing the value in a semantic context. Each data point also has a name and a description. The entire set of data points is organized in a hierarchy.

At the data point level, the specific technological restrictions are abstracted and hidden from the user. Working with different technologies at this level involves common work-flows for all supported technologies.

The direction of a data point is defined as the “network view” of the data flow. This means, an input data point obtains data from the network. An output data point sends data to the network. This is an important convention to remember as different technologies may define other direction semantics.

The basic classes of data points are:

- **Analog**: An *analog* data point typically represents a scalar value. The associated data type is a *double precision* machine variable. Meta-data for analog data points include information such as value range, engineering units, precision, and resolution.
- **Binary**: A *binary* data point contains a Boolean value. Meta-data for binary data points includes human-readable labels for the Boolean states (i.e., active and inactive texts).
- **Multi-state**: A *multi-state* data point represents a discrete set of states. The associated data type is a signed integer machine variable. Each state is identified by an integer value, the *state ID*. State IDs need not be consecutive. Meta-data of a multi-state data point includes human-readable descriptions for the individual states (state texts) and the number of available states.
- **String**: A *string* data point contains a variable-length string. The associated data type is a character string. International character sets are encoded in UTF-8. A string data point does not include any other meta-data.
- **User**: A *user* data points contains un-interpreted, user-defined data. The data is stored as a byte array. A user data point does not include any other meta-data. This type of data point also serves as a container for otherwise structured data points and represents the entirety of the structure.

5.2.2 Timing Parameters

Apart from the meta-data, data points can be configured with a number of timing parameters. The following properties are available to input or output data points, respectively:

- **Pollcycle** (input): The value is given in seconds, which specifies that this data point periodically polls data from the source.
- **Receive Timeout** (input): This is a variation on the poll cycle. When receive timeout is enabled, the data point actively polls the source unless it receives an update. For example, if poll cycle is set to 10 seconds and an update is received every 5 seconds, no extra polls are sent.
- **Poll-on-startup** (input): If this flag is set, the data point polls the value from the source when the system starts up. Once the value has been read, no further polls are sent unless a poll cycle has been defined.
- **Minimum Send Time** (output): This is the minimum time that elapses between two consecutive updates. If updates are requested more often, they are postponed and the last value is eventually transmitted after the minimum send time. Use this setting to limit the update rate.
- **Maximum Send Time** (output): This is the maximum time without sending an update. If no updates are requested, the last value is transmitted again after the maximum send time. Use this setting to enable a heart-beat feature.

5.2.3 Default Values

Default values can be defined for data points when needed. The value of a data point will be set to the defined default value, if no other value source initializes the data point. Default values are beneficial, if certain input data points are not used by the network and need a pre-defined value, e.g., for calculations. Default values are overridden by persistent values or values determined by poll-on-startup.

5.2.4 Persistency

Data point values are by default not persistent. This means that their value is lost after a power-on reset. There exist different strategies for initializing data points with an appropriate value after the device has started.

For input data points, the value can be actively polled from the network when starting up. Use the Poll-on-Startup feature for this behavior. Polling the network values has the advantage that intermediate changes on the network are reflected. An input data point can be made persistent, if the last received value shall be available after a power-on reset before a poll-on-startup completes. This can be beneficial, if the remote device is temporarily offline and the last value is considered usable.

For output data points, the value can be restored after starting up by the application. For example, if the output data point's value is determined by an input data point and a math object, or the output data point is in a connection with an input, the input can poll its value on startup. If the output data point has no specific other value source, e.g., it is a configuration parameter set by the user, it can be made *persistent*.

To make a data point persistent, enable the Persistent property of the respective data point. The persistency option is only available for the base data point classes analog, binary, multi-state, string and user. More complex objects such as calendars, schedules, etc., have their own data persistency rules.

For structured data points, only all or none of the structure members can be made persistent. The configuration of the top-level data point, which represents the entire structure, serves as a master switch. Setting the top-level data point to be persistent enables persistency for all sub-data points. Clearing it disables persistency for all sub-data points.

5.2.5 Behavior on Value Changes

The value of a data point can change, if it is written by the application or over the network. For all data points (input and output) the application (connection, user control, etc.) can be notified, when the value is written to. The property **Only notify on COV** defines, whether the notification is done with each write or only if the value changes (change-of-value, COV). If only notify on COV is disabled, writing the same value multiple times will result in multiple notifications.

When the value of an output data point is updated, an update is usually sent out onto the network. The property **Send-On-Delta** decides how the update is reflected on the network. If send-on-delta is inactive, each update of the value is sent. If send-on-delta is active, value changes only are sent. The send-on-delta property is only valid for output data points.

For analog data points, the COV or send-on-delta takes an extra argument, which specifies by what amount the value must change to regard it as a change for action. Both, COV and send-on-delta for analog data points check the **Analog Point COV Increment** property. A change is detected, if the value increment is bigger or equal to the specified increment. If the property is zero, all updates are considered.

5.2.6 Custom Scaling

Custom scaling is applied to all analog data points when they communicate values to or from the network. This feature can be used, if a network data point has engineering units not suitable for the application (e.g., grams instead of kilograms). The scaling is linear and applied in the direction from the network to the application as:

$$A = k\,N + d,$$

where N is the network value, *k* the *custom scaling factor*, *d* the *custom scaling offset*, and A the application value. When sending a value to the network, the reverse scaling is applied. If this property is enabled, the analog values are pre-scaled from the technology to the data point. The custom scaling is in addition to any technology-specific scaling factors and can be applied regardless of the network technology.

5.2.7 System Registers

The L-Gate provides a number of built-in system registers. They are present without a data point configuration. The system registers, such as the System time or the CPU load, can be exposed to the OPC server. By default, all system registers are checked for being exposed to OPC. To reduce the number of needed OPC tags, you may deselect certain system registers, which are not useful in a specific project.

System register can also serve as a testing setup for the OPC XML-DA communication without a network data point configuration. The *System Time* register is updated every second and may serve for testing subscriptions. The *Authentication Code* register can be used to verify writing to OPC tags.

5.2.8 User Registers

The L-Gate can be configured to contain user registers. In contrast to system registers, these are only available as a part of the data point configuration. User registers are data points on the device that do not have a specific technological representation on the control network. Thus, they are not accessible over a specific control network technology.

A register merely serves as a container for intermediate data (e.g., results of math objects). The register can have the following, basic data types:

- **Double**: A register of base type *double* is represented by an *analog* data point. It can hold any scalar value. No specific scaling factors apply.
- **Signed Integer**: A register of base type *signed integer* is represented by a *multi-state* data point. This register can hold a set of discrete states, each identified by a signed stats ID.
- **Boolean**: A register of base type *Boolean* is represented by a *binary* data point. This register can hold a Boolean value.

Since a register has no network direction, it can be written and read. Therefore, two data points are generated for each register, one for writing the register (output) and one for reading the register (input). A suffix is added to the register name to identify the respective data point. For example, the register *MyValue* will have two data points generated for: *MyValue_Read* and *MyValue_Write*.

5.2.9 Math Objects

Math objects are advanced application objects that can execute mathematical operations on data points. A math object takes a number of input data points (variables v_1, v_2, …, v_n) and calculates a result value according to a specified formula. The result is written to a set of output data points. The formula is calculated each time one of the input data points updated its value. The formula is only evaluated if all of the input data points have a valid value (i.e., don’t show the *invalid value* status).

5.3 Connections

With the use of connections, data points can interact with each other. Connections specify which data points exchange values with each other. Both types of connections – “1:*n*” and “*m*:1” connections – are supported. The single data point is referred to as the *hub* data point, whereas the other data points are the *target* data points.

This means, the following connections are possible:

- 1 input data point is connected to *n* output data points,
- *m* inputs data points are connected to 1 output data point.

The most common connection will be the 1:1 connection. This is the type of connection that is auto-generated by the Configurator software. Other types must be created manually in the Configurator.

In the 1:*n* connection the input value is distributed to all n output data points. In the *m*:1 connection, the most current input value is written to the output data point. When polling the output data point in poll-through mode (maximum cache age is set on the output), the value from the first input data point is polled.

Connections can connect data points of different technologies with each other (also mixed among the target data points) but are restricted to the same class of data points. This means only data points of class *analog* can exchange values within a connection.

For certain classes of data points, additional restrictions exist:

- **Analog**: The value range is capped on the output data points. This means, if the input value in the hub does not fit into the range of an output data point, the value is capped to the biggest or smallest allowed value.
- **Binary**: No special restrictions exist.
- **Multi-state**: Only multi-state data points of an equal number of states can be placed into a connection. The actual state Ids need not be equal. They are ordered and the *n*-th state is propagated over a connection. For example, the 2nd state on the hub has the state ID ‘2’, while on the target the 2nd state has the state ID ‘0’.
- **String**: No special restrictions exist.
- **User**: Only user data points of the same length can be placed in a connection.

5.4 AST Features

5.4.1 Alarming

The alarming architecture comprises a number of entities. Objects that monitor values of data points and generate alarms depending on an *alarm condition* are called *alarm sources*. The alarms are reported to an *alarm server* on the same device. The alarm server maintains a list of alarm records, called the *alarm summary*. The alarm server is the interface to access the local alarms. This can be done over the network or the Web UI.

An alarm record contains the information about the alarm. This includes information about the alarm time, the source of the alarm, an alarm text, an alarm value, an alarm type, an alarm priority, and an alarm state. An alarm record undergoes a number of state changes during its life-cycle. When the alarm occurs, it is *active*. When the alarm condition subsides, the alarm becomes *inactive*. Active alarms can be acknowledged by an operator. Then they become *active acknowledged*. Active alarms can also become inactive, but an acknowledgement is still required. Then they become *ack-pending*. When an alarm is inactive and was acknowledged it disappears from the alarm summary.

Other devices can access the alarm information of an alarm server. These devices are *alarm clients*. They register with the alarm server and get notified about changes to the alarm summary. Alarm clients can be used to display the current alarm summary and acknowledge alarms.

Depending on the underlying technology, some restrictions to the available alarm information and acknowledgement behavior may exist.

5.4.2 Historical Alarm Log

The alarm summary of the alarm objects contains a live list of currently active and acknowledge-pending alarms. As soon as an alarm becomes inactive and has been acknowledged, it disappears from the alarm summary. To store a historical log of alarm transitions an *alarm log* is utilized. An alarm log can log transitions of one or more alarm objects.

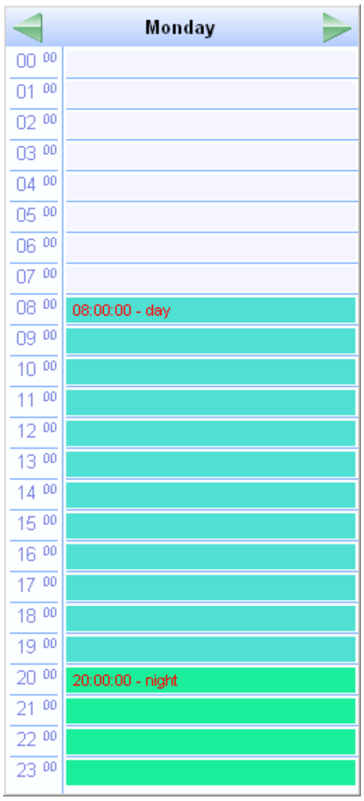
The alarm log is always local and stored as a file on the device. The size of an alarm log is configurable. The alarm log operates as a ring buffer. As soon as its size limit is reached, the oldest alarm log records are overwritten by newer alarm transitions. The alarm log is available on the Web UI or can be uploaded from the device as a CSV file. The CSV file can also be used as an e-mail attachment.

5.4.3 Scheduling

Schedulers are objects that schedule values of data points on a timely basis. A scheduler object is configured by which data points it shall schedule. This configuration is done by the system engineer once when the system is designed. The configuration of the times and values that shall be scheduled is not part of that initial configuration and may be changed later. This distinction has to be kept in mind.

A scheduler object sets its data points to pre-defined values at specified times. The function of the scheduler is state-based. This means, that after a value is scheduled, the scheduler maintains its state for this value. It can re-transmit the scheduled values as appropriate (e.g., when rebooting). The pre-defined values are called /value presets/. A value preset contains one or more values under a single label (e.g., "day" schedules the values {20.0, TRUE, 400}).

Which value preset is scheduled at what time is defined through a *daily schedule*. The daily schedule defines the times and value presets in a 24-hour period. A schedule typically contains daily schedules for the weekdays Monday through Sunday. See Figure 41 for an example of a daily schedule.



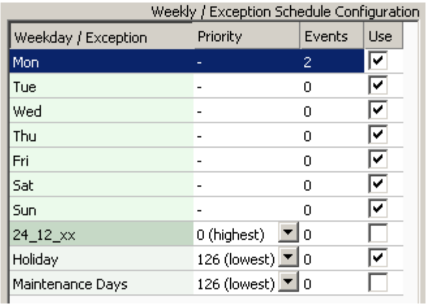
08:00:00 - day

20:00:00 - night

Figure 41: Example of a Daily Schedule.

For some tasks the daily schedules on weekdays is sufficient. However, on some specific dates, there may be exceptions to the regular week. This can be implemented by defining daily schedules for *exception days*. For instance, there may be a separate daily schedule for *Holidays*. The exception days are defined through a *calendar*. The calendar contains a number of *calendar patterns*. Each calendar pattern describes a pattern of dates that define the class of an exception, e.g., *Holidays*.

When a calendar is defined on a system, the exception days are available in all schedules. When a schedule wants to define daily schedules for some of the available exception days, they need to be enabled in the schedule. See Figure 42 for an example where *Holidays* is used.



Weekly / Exception Schedule Configuration

Weekday / Exception	Priority	Events	Use
Mon	-	2	☑
Tue	-	0	☑
Wed	-	0	☑
Thu	-	0	☑
Fri	-	0	☑
Sat	-	0	☑
Sun	-	0	☑
24_12_xx	0 (highest)	0	□
Holiday	126 (lowest)	0	☑
Maintenance Days	126 (lowest)	0	□

Figure 42: Example of on used Exception Day.

The function of the exception is simple. The daily schedule of a regular weekday is overridden by the daily schedule of the exception, when one of the specified date patterns is in effect (e.g., July 14th in Holidays overrides the regular weekday). If more than one exception days are in use, there may be conflicts on specific dates. These conflicts are resolved by defining *priorities* for the different exceptions. The daily schedule of the exception with the higher priority is eventually in effect. If two exceptions with the same priority exist, it is not defined, which one is in effect. Therefore, always use distinct priorities.

Apart from the defined value presets, there exist special events that can be scheduled in a daily schedule. They affect how the scheduler behaves and which exception is active:

- **Invalid**: If this value is scheduled, the scheduler transmits the invalid value. The numeric representation of that invalid value is defined by the underlying data point and is technology-specific.

- **Withdraw**: If this value is scheduled, the scheduler takes the previously value preset out of effect. This means that the daily schedule with the next lower priority becomes effective. If no daily schedule with lower priority applies, the scheduler behaves as if it was disabled. Figure 43 presents an example of the *Maintenance* exception day, which schedules the *maint* value at 6 am and goes out of effect at 10 am. If the maintenance day falls on a Monday, the regular schedule for Monday will be overridden by the Maintenance schedule at 6 am and become effective again at 10 am sending the *day* value.

- **Temporary Disable**: If this value is scheduled, the entire scheduler is disabled until a new event is scheduled in a daily schedule of the same or higher priority than the one that has the temporary disable event. This type of event can be used to define periods for manual override.

Please also refer to the technology-specific limitations described in Section 6.12 to learn about special behavior of the respective networking technology.

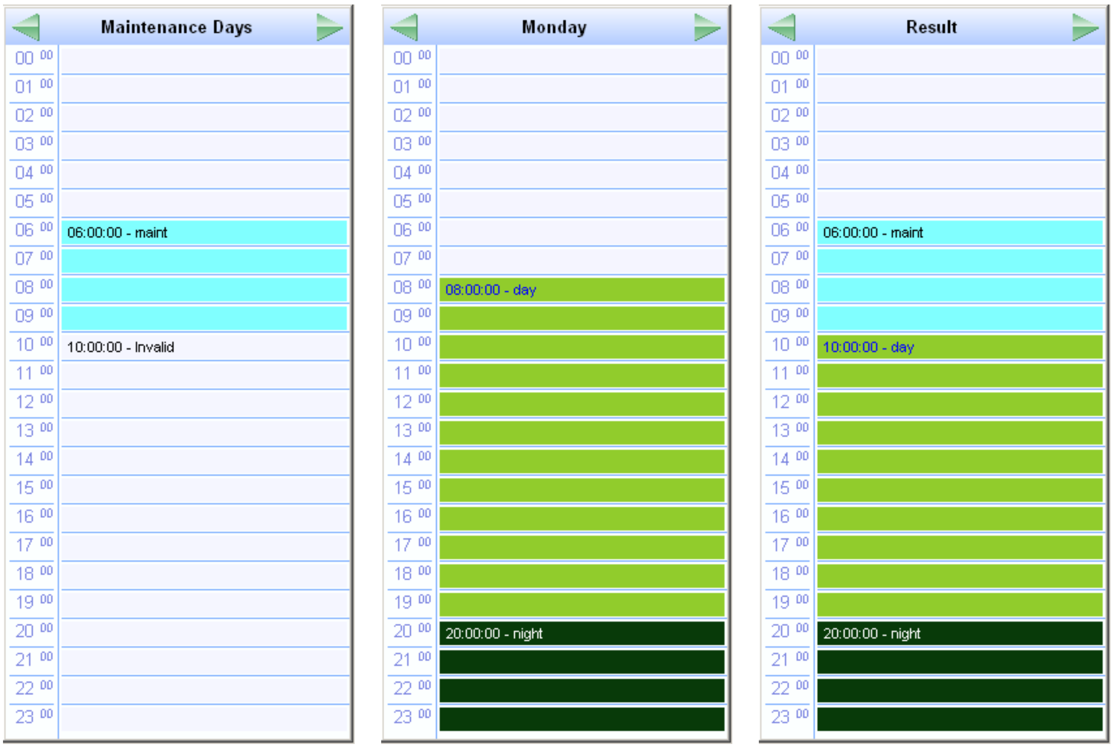


Figure 43: Example using withdraw in an exception schedule.

The configuration of exceptions is done by calendar patterns in the calendar. Each calendar pattern contains a number of pattern entries. These entries can define the following:

- A single date: This defines a singe date. Wildcards may be used in the year to specify July 14th of every year.

- A date range: This defines a range. Starting with a start date and ending with the end date. No wildcards should be used.
- A Week-and-Day definition: This defines dates based on a week, such as every 1st Friday in a month, every Monday, every last Wednesday of a month.

While exception days of a calendar are accessible to all schedules on a device, specific exceptions can be defined, which are embedded into a specific schedule. These are referred to as an *embedded calendar*. In contrast to a regular calendar each calendar pattern of an embedded calendar can hold exactly one date entry. This can be a single date or a date range. The embedded exception days are only visible to the schedule they are defined in. Apart from these restrictions, embedded calendars behave like the regular calendar. Figure 42 shows an example for an embedded exception day named ‘24_12_xx’.

A schedule defines at which time instants certain states of the scheduled data points are maintained. The *next-state* feature allows to look ahead into the future and predict when the next scheduled state will occur. There are two data points involved: the time-to-next-state is a counter in minutes to the next scheduled event, and the next-state data point is the state of the next scheduled event. This information can be used by controllers to optimize their algorithms (e.g., pre-heat a room for the scheduled occupancy state). Use the SNVT_tod_event in CEA-709 to accomplish this task.

When a scheduler is executing the schedule on the local device, it is called a *local scheduler*. Such a scheduler is configured to schedule data points and later its daily schedules can be modified. When accessing the daily schedules of a scheduler, which executes on a remote device, the object is called a *remote scheduler*. A remote scheduler has the same interface to the user to modify daily schedules. A remote scheduler object can be used as a user-interface for schedulers that execute on different devices.

5.4.4 Trending

Trending refers to the ability to log values of data points over time. A trend log object is responsible for this task. It is configured, which data points shall be trended. Log records are generated either in fixed time intervals, on change-of-value conditions, or when a trigger is activated. Trend log objects can trend either local or remote data points.

The trend data is stored in a binary format on the device. The capacity of a given trend log is configured. The trend log can be operated in one of two modes: (1) In linear mode the trend file fills up until it reaches its capacity. It then stops logging. (2) In ring buffer mode. In this mode the oldest log records are overwritten when the capacity is reached.

Trended data points can be logged as their actual values at given time instants or as an aggregated value over the defined log interval. Aggregation can be calculated as minimum, maximum, or average. Aggregation can be beneficial, if the trended value changes more frequently than the selected log interval. Using aggregation, the log interval can be chosen to limit the amount of logged data while preserving information of the trended value.

How many data points can be trended in one trend log is limited by the underlying technology. So are some of the log modes. Refer to the technology sections for more information.

5.4.5 E-Mail

The e-mail function can be combined with the other AST features. The format of an e-mail is defined through *e-mail templates*. An e-mail template defines the recipients, the e-mail text, value parameters inserted into the text and triggers, which invoke the transmission of an e-mail. An e-mail template can also specify one or more files to be sent along as an attachment.

A prerequisite to sending E-Mails is the configuration of an E-Mail account on the L-Gate. This can be done on the Web UI (see Section 4.2.11). It is recommended to use the e-mail server of your Internet provider. For public mailers enable the required authentication. Please note that the L-Gate does currently not support the SSL/TLS E-Mail authentication mechanism. Therefore, Hotmail and gmail cannot be used.

The amount of generated e-mails can be limited using a rate limit algorithm. The transmission of e-mails can be disabled altogether by using a special data point. That data point can be scheduled or driven over the network.

If an E-Mail cannot be sent (e.g. the mail server is not reachable), the mail delivery is retried up to 24 times every 30 minutes.

5.5 CEA-709 Technology

5.5.1 CEA-709 Data Points

Data points in the CEA-709 network are known as network variables (NVs). They have a direction, a name, and a type, known as the standard network variable type (SNVT) or user-defined network variable type (UNVT). In addition to NVs, also configuration properties (CPs) in the CEA-709 network can be accessed as data points. Both standard CP types (SCPTs) and user-defined CP types (UCPTs) are supported.

The CEA-709 NVs on the L-Gate can be created in three different ways:

- **Static NV**: For each selected NV on the network there is a static NV created on the L-Gate. This NV can be bound to the NV on the network. Note that adding static NVs to the L-Gate results in a change to the default XIF file. The L-Gate is assigned a new “model number” to reflect this change (see Section 5.5.2). Static NVs are the way to use NVs in non-LNS systems, where NVs shall be bound instead of using polling.
- **Dynamic NV**: For each selected NV on the network there is a dynamic NV created on the L-Gate. Compared to static NVs, dynamic NVs do not change the XIF interface of the L-Gate. The dynamic NVs are created by the network management tool. Currently, only LNS-based tools can manage dynamic NVs. As for static NVs, with dynamic NVs it is possible to use bindings instead of polling.
- **External NV**: The selected NVs on the network are treated as external NVs to the L-Gate. The L-Gate doesn’t create any NVs on the device, but instead uses polling to read from those NVs and explicit updates to write to the NVs. Therefore, no bindings are necessary for external NVs. For input data points using external NVs however, a poll cycle must be configured. If not configured explicitly, a default poll cycle of 10 sec. is chosen. The default poll cycle can be changed in the project settings menu.

Based on the NV the data point is derived from, the following kinds of data points are created:

- Simple NVs that hold only one scalar value, e.g., SNVT_amp: Those kinds on NVs are represented as analog data points. The data points holds the current value, NV scaling factors are applied.
- Simple NVs based on an enumeration, e.g., SNVT_date_day: Enumeration types result in multi-state data points. They represent the state of the NV.
- Structured NVs that consists of a number of fields, e.g., SNVT_switch: All structured NVs are represented as user point. That is, the data point is structured similar to the NV it is based on. Beneath the user data point, the individual structure fields are presented as “sub-data points”.

For more information on the different types of network variables and their implications please refer to the application note in Section 11.2. For CPs the allocation type “File” is used.

5.5.2 Static Interface Changes

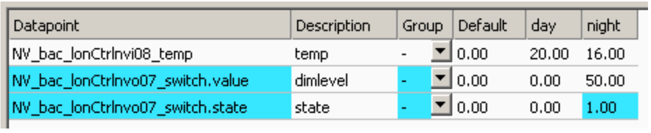
The L-Gate can be configured to use static NVs. Unlike dynamic NVs, static NVs cannot be created in the network management tool. They are part of the static interface and are usually compiled into the device. When static NVs are used, the L-Gate changes its static interface and boots with a new one.

Each time the static interface of the L-Gate changes (i.e., static NVs are added, deleted, or modified), the model number is changed. The model number is the last byte of the program ID. Thus, a change in the static interface results in a change of the program ID and a new device template needs to be created in the network management tool. A new device template usually means that the device has to be deleted and added again in the database. All bindings and dynamic NVs have to be created again for the new device.

When the L-Gate Configurator is connected via LNS, it supports the process of changing the device template for the new static interface. It automatically upgrades the device template of the L-Gate device in the LNS database and restores the previous bindings and dynamic NVs. If the L-Gate is not configured with an LNS-based tool, this support is not available. The new static interface is only available in a new XIF file or by uploading the new device template into the database. For more information on the static interface and device templates please refer to the application note in Section 11.2.

5.5.3 Limitations for Local CEA-709 Schedulers

CEA-709 schedulers and the CEA-709 calendar adhere to the LONMARK standard objects. For CEA-709, certain restrictions exist that need to be kept in mind. Attached data points can either represent an entire NV or individual elements of a structured NV. CEA-709 schedulers may have several different groups of data points attached, i.e., the value preset may consist of more than one element. For example, a CEA-709 scheduler might schedule a SNVT_temp and a SNVT_switch and have 3 elements in each value preset as depicted in Figure 44.



Datapoint	Description	Group	Default	day	night
NV_bac_lonCtrlnvi08_temp	temp	-	0.00	20.00	16.00
NV_bac_lonCtrlnvo07_switch.value	dimlevel	-	0.00	0.00	50.00
NV_bac_lonCtrlnvo07_switch.state	state	-	0.00	0.00	1.00

Figure 44: Example value presets in CEA-709 schedulers.

Priorities of exception days in a CEA-709 scheduler range from 0 (the highest) to 126 (the lowest). The value 127 is reserved as a default for weekdays.

Further, the implementation as LONMARK standard objects requires the use of configuration properties. If the number of CEA-709 schedulers or their capacities for daily schedules and value presets is changed, the resource and static interface of the CEA-709 port changes. The resources reserved for LONMARK calendar and scheduler objects can be changed in the project settings (see Section 6.3.4). When downloading a project, the software verifies if sufficient resources have been configured. If it detects a problem, the user is notified to update the project settings. The Auto-Set feature automatically selects the right amount of resources.

5.5.4 Limitations for CEA-709 Alarm Servers

Local CEA-709 alarming supports only one alarm server object. This alarm server object is represented by the device’s LONMARK node object and facilitates the SNVT_alarm2 output network variable. Acknowledging alarms in the alarm server is adhering to the LONMARK specification and relies on the RQ_CLEAR_ALARM mechanism.

5.5.5 Limitations for Local CEA-709 Trends

Local CEA-709 trend objects support trending multiple data points in all trend modes, interval, COV, and trigger. The enable data point is also supported. All data points can be NVs, registers or of any other technology. There is no LONMARK object linked to the trend object. Consequently, trend data cannot be accessed over a LONMARK mechanism.

5.6 BACnet Technology

5.6.1 BACnet Data Points

Data points in the BACnet technology are known as BACnet objects. They have a specific type (e.g. analog input or binary output) and a set of properties, which describe the data point more closely. The actual value is stored in the “Present_Value”.

On the device, there exist two classes of BACnet data points:

- **BACnet server objects** (SO): These BACnet objects configured by the Configurator software to be allocated *locally* on the device. These objects can be accessed by the BACnet building control system or operating workstations. They support COV subscriptions to deliver value changes in an event-driven way.

- **BACnet client mappings** (CM): For certain applications, it is necessary that the device acts as a BACnet client. This functionality can be configured by activating a *client mapping*. Client mappings can be of the type *Poll*, *COV*, *Write*, or *Auto*. This specifies how the BACnet client accesses other BACnet objects on the BACnet network. The *Auto* method determines the best way (poll, COV, or write) to talk with other server objects. *Poll* is used for objects that need to read data from other BACnet objects in a periodic manner. *COV* is used to subscribe for COV at other BACnet objects in order to get updates in an event-driven fashion. *Write* is used to send updates to other BACnet objects.

The direction of BACnet server objects deserves a closer look. The direction specified for data points in the Configurator software always refers to the network view of the communication. The definition of input and output objects in BACnet, however, refers to the process view, which is opposite to the network. Therefore, a BACnet analog input (AI) object is modeled as an analog output data point. The direction of client mappings naturally refers to the network communication. Therefore, a write client mapping is represented as an analog output data point.

In BACnet commandable objects can be written with values at a certain priority. The value with the highest priority is in effect. When revoking a written value, the NULL value is written. This takes back the value. When all written values are withdrawn, the Relinquish_Default value is in effect.

The default value feature of a data point is mapped to the Relinquish_Default property for commandable objects. For BACnet objects, which are not commandable, the Present_Value is initialized with the specified default value.

5.6.2 BACnet Alarming

BACnet alarming on the device is based on the *intrinsic reporting* mechanism. Currently, algorithmic reporting is not supported. Alarm conditions can only be applied to data points, which map to BACnet server objects. If defined, the intrinsic reporting properties of the underlying BACnet objects are enabled. Alarm conditions can be specified for analog input, output, value objects (AI, AO, AV), for binary input, value objects (BI, BV), and for multi-state input, value objects (MSI, MSV). To define alarm conditions for binary output (BO) and multi-state output (MSO) objects map the Feedback_Value property of the respective server objects to a data point. This data point must be used to supply the feedback value to the server object.

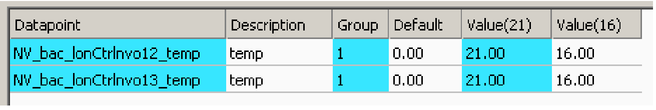
Alarm servers in the BACnet technology are mapped to BACnet Notification Class (NC) objects. Each alarm server is mapped to one NC. The notification class number can be configured in the object instance number property of the alarm server object.

Remote alarms in the BACnet technology refer to a remote NC object. When the device starts up, the remote alarm object reads out the current alarm state of the remote NC and reporting objects. To get notified about alarm transitions during run-time, the device registers in the Recipient_list of the remote NC object.

5.6.3 BACnet Schedulers and Calendars

BACnet schedulers and the BACnet calendar adhere to the standard schedule and calendar object in BACnet. For each scheduler a BACnet Schedule object is created. The calendar deserves a closer look. For each calendar pattern a BACnet Calendar object is created. The visible calendar on the Web UI is therefore a collection of BACnet calendar objects. Each calendar pattern therefore is associated with a BACnet object instance number. The calendar pattern “Holidays” is for example visible as CAL,1 on the BACnet port.

The BACnet schedule object allows only objects of one selected data type to be scheduled. Therefore, schedulers on BACnet can only schedule one class of data points (e.g., only one group of analog data points). As a consequence, the value preset in BACnet always has only one element. The name of the value preset is not stored in BACnet. It is not accessible over the BACnet network, either. Therefore, a default name is created, such as ‘Value(22)’ for an analog value. An example of two scheduled BACnet objects is shown in Figure 45.



Datapoint	Description	Group	Default	Value(21)	Value(16)
NV_bac_lonCtrlnvo12_temp	temp	1	0.00	21.00	16.00
NV_bac_lonCtrlnvo13_temp	temp	1	0.00	21.00	16.00

Figure 45: Example value presets in BACnet schedulers.

Priorities of exception days in a BACnet scheduler range from 1 (the highest) to 16 (the lowest). Weekdays in BACnet have no priority.

Changing the number of calendar patterns in a BACnet calendar can only be done through the configuration software and not during run-time. The individual calendar pattern entries in the calendar patterns can be changed at run-time. Therefore, it is advisable to reserve a suitable number of calendar patterns in a BACnet calendar and leave them empty if not needed immediately.

5.6.4 BACnet Trend Logs

A number of restrictions apply to trend log objects in BACnet. Trend log objects must be created by the Configurator software. These objects are accessible over the BACnet network for other BACnet devices and operator workstations (OWS). All configuration properties can be modified by the Configurator software as well as an OWS. The number of trend log objects cannot be changed at run-time. Therefore, if it is intended that an OWS configures the trend logs, a suitable number of empty trend log objects (i.e., without attached data points) must be created in the Configurator software.

In BACnet trend logs, only one data point can be trended per trend log object. The trended data point can be either a local BACnet server object or a remote BACnet object accessed through a client mapping. Data points of other technologies and the min/max/avg algorithms cannot be trended in this firmware version.

BACnet trend logs are limited to interval and COV logs. The trigger mode is not supported in BACnet. The setting linear and ring-buffer logging is mapped to the Stop_When_Full property of the underlying BACnet trend log object. This setting in the Configurator software is a default and can be overridden by writing to the Stop_When_Full property by the OWS.

If an enable data point is configured by the Configurator software, the Log_Enable property is written with the value of that data point. If no enable data point is configured, the Log_Enable is TRUE as a default and can be modified over the network.

The fill-level action is mapped to generating a buffer event notification in the BACnet trend log object. The fill-level trigger can still be used for e-mails even if no notification class is configured in the BACnet trend log object. The fill-level percentage maps to the Notification_Threshold property. The percentage setting in the Configurator software is a default and can be changed by the OWS over the network.

5.7 Automatic Generation of Connections

When generating matching counter parts to NVs, there are two types of NVs to be considered: Simple NVs that hold only one value (scalar or enumeration), and structured NVs, that consist of a number of fields. For simple NVs only one BACnet object per NV is generated. For structured NVs, one BACnet object is generated for each structure member.

Which type of BACnet object is created depends on the type of the simple NV or of the structure member. For scalar types, analog objects are created. The scaling factors are applied to the NV to get the resulting scalar value for the Present_Value property. Other properties of analog objects are derived from the SNVT, including the engineering units, min and max present value. Multi-state objects are created for NV enumeration types. The CEA-709 state IDs are sorted and renumbered to start at ‘1’ in BACnet (i.e., a ‘-1’ of MOTOR_NUL in CEA-709 maps to a ‘1’ of MOTOR_NUL in BACnet). This is necessary as the SNVT states ‘-1’ and ‘0’ cannot be represented in BACnet as a raw value, because allowed BACnet multi-states start at 1. Which state IDs exist is documented in the BACnet multi-state texts array. Optionally, binary objects are created for enumerated NVs with three states, excluding the ‘-1’ state.

In BACnet commandable objects can be written with values at a certain priority. The value with the highest priority is in effect. When revoking a written value, the NULL value is written. This takes back the value. When all written values are withdrawn, the Relinquish_Default value is in effect. In CEA-709 there is no notion of taking a value back. To model this behavior, a distinctive *invalid* value can be written to an NV. Most SNVTs have such an invalid value. For those that do not an invalid value, it can be specified when editing the data point. To make a BACnet object convey that invalid value to the CEA-709 side, enable the property “Relinquish to Invalid”.

6 The L-Gate Configurator

This Chapter gives step-by-step instructions on how to commission the device, create a data point configuration with input and output network variables, and how to map those data points to BACnet and vice-versa. We show the configuration steps using LonMaker TE but other LNS-based network management tools can be used as well to install and configure the device. We also show how to configure the device without LNS.

6.1 Installation

6.1.1 Software Installation

The L-Gateway Configuration software must be used to setup the data point configuration of the L-Gate. This configuration utility is installed as a plug-in tool for all LNS-based network management tools as well as a stand-alone tool (for systems without LNS).

System requirements:

- LNS 3.1, Service Pack 8 or LNS TE SP5 or higher (for LNS mode),
- Windows XP, Windows 2003 Server, Windows Vista, Windows 7, or Windows 2008 Server.

The L-Gate Configurator can be downloaded from the LOYTEC Web site http://www.loytec.com. When asked for the type of installation, there are two options to choose from. Select **Typical** to install the required program files. Select **Full** to install the LONMARK resource files along with the software. This option is useful, when the system does not have the newest resource files.

6.1.2 Registration as a Plug-In

If the L-Gate shall be configured using LNS-based tools (e.g., NL200 or LonMaker), the L-Gate Configurator needs to be registered as an LNS plug-in. In the following, the process is described for LonMaker TE. Otherwise, please refer to the documentation of your network management tool on how to register an LNS plug-in.

To Register in LonMaker TE

1. Open LonMaker and create a new network.
2. Click **Next** until the plug-in registration tab appears in the Network Wizard. Select the **LOYTEC L-Gate Configurator (Version X.Y)** from the list of **Not Registered** (see Figure 46).

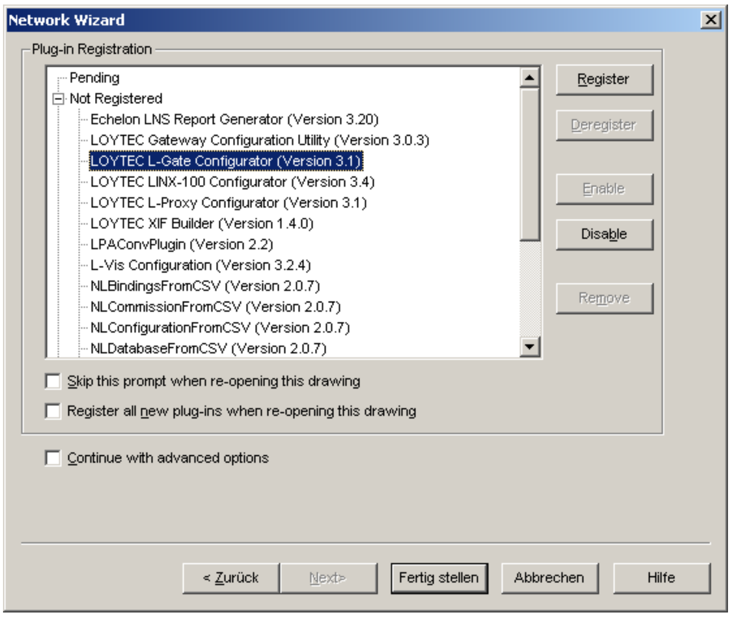

Network Wizard
Plug-in Registration
Pending
Not Registered
Echelon LNS Report Generator (Version 3.20)
LOYTEC Gateway Configuration Utility (Version 3.0.3)
LOYTEC L-Gate Configurator (Version 3.1)
LOYTEC LINX-100 Configurator (Version 3.4)
LOYTEC L-Proxy Configurator (Version 3.1)
LOYTEC XIF Builder (Version 1.4.0)
LPAConvPlugin (Version 2.2)
L-Vis Configuration (Version 3.2.4)
NLBindingsFromCSV (Version 2.0.7)
NLCommissionFromCSV (Version 2.0.7)
NLConfigurationFromCSV (Version 2.0.7)
NLDatabaseFromCSV (Version 2.0.7)
Register
Deregister
Enable
Disable
Remove
Skip this prompt when re-opening this drawing
Register all new plug-ins when re-opening this drawing
Continue with advanced options
< Zurück
Next>
Fertig stellen
Abbrechen
Hilfe

Figure 46: Select the Plug-in to be registered.

3. Click **Register**. The Configurator now appears in the **Pending** list.

4. Click **Finish** to complete the registration. Device templates for the L-Gate are added automatically and XIF files are copied into the LNS import directory.

Note: *If you are using multiple databases (projects) make sure you have registered the plug-in in each project.*

5. Under **LonMaker → Network Properties → Plug-In Registration** make sure that the **LOYTEC L-Gate Configurator (Version X.Y)** shows up under **Already Registered**.

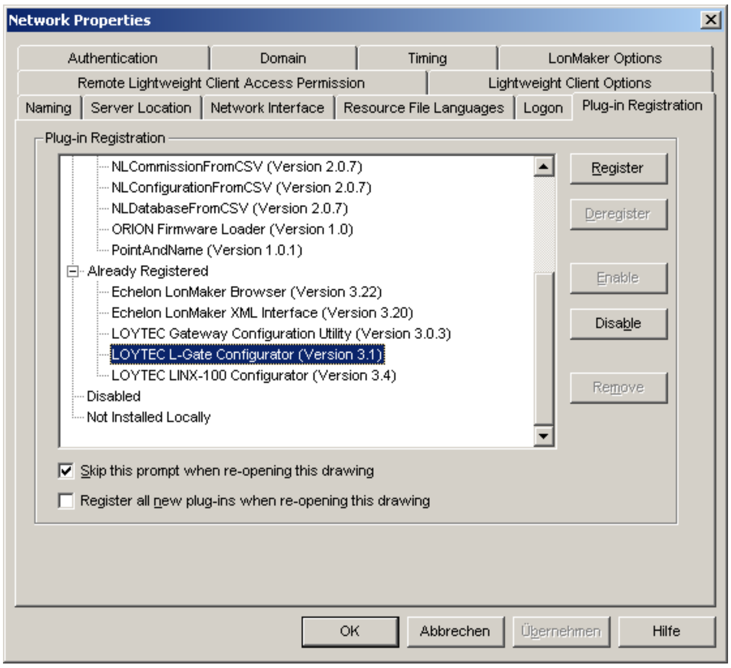

Network Properties
Authentication
Domain
Timing
LonMaker Options
Remote Lightweight Client Access Permission
Lightweight Client Options
Naming
Server Location
Network Interface
Resource File Languages
Logon
Plug-in Registration
Plug-in Registration
NLCommissionFromCSV (Version 2.0.7)
NLConfigurationFromCSV (Version 2.0.7)
NLDatabaseFromCSV (Version 2.0.7)
ORION Firmware Loader (Version 1.0)
PointAndName (Version 1.0.1)
Already Registered
Echelon LonMaker Browser (Version 3.22)
Echelon LonMaker XML Interface (Version 3.20)
LOYTEC Gateway Configuration Utility (Version 3.0.3)
LOYTEC L-Gate Configurator (Version 3.1)
LOYTEC LINX-100 Configurator (Version 3.4)
Disabled
Not Installed Locally
Register
Deregister
Enable
Disable
Remove
Skip this prompt when re-opening this drawing
Register all new plug-ins when re-opening this drawing
OK
Abbrechen
Übernehmen
Hilfe

Figure 47: Check that the L-Gate Configurator is properly registered.

6.1.3 Operating Modes

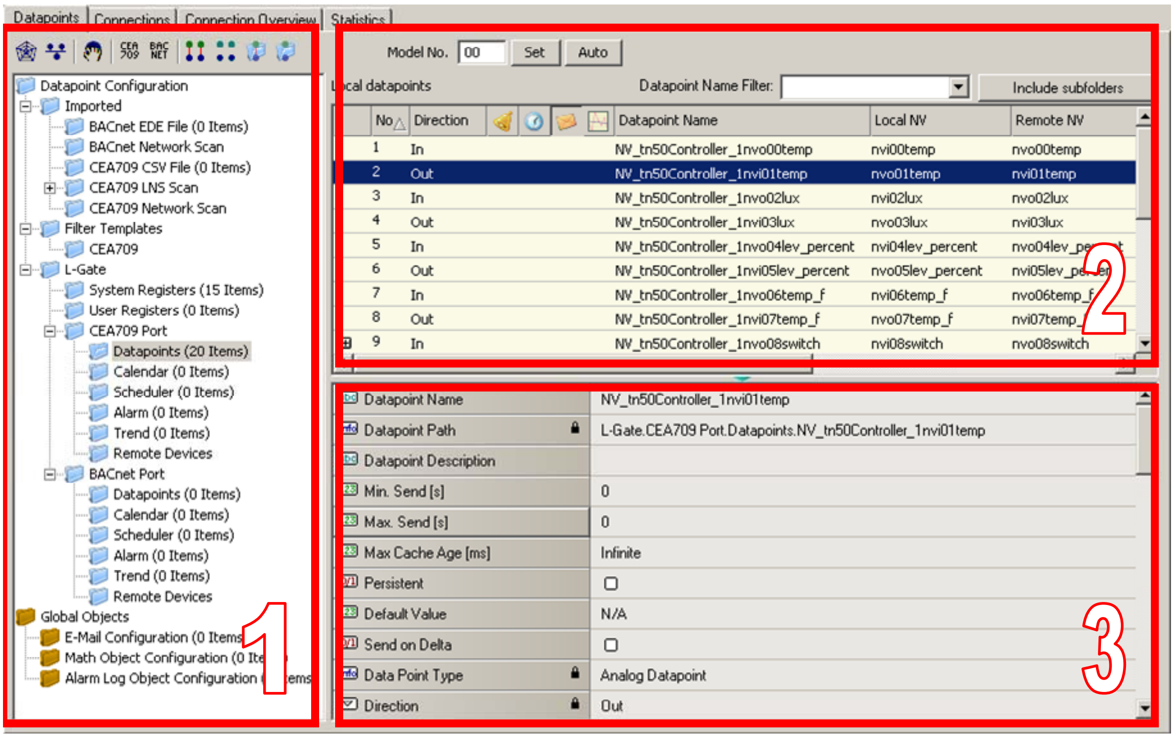
The Configurator can be used in on-line, off-line, and stand-alone mode. On-line and off-line mode refers to the 2 operating modes of your LNS network management software.

- **On-line Mode**: This is the preferred method to use the configuration utility. The network management tool is attached to the network and all network changes are directly propagated into the network. This mode must be used to add the device, commission the device, extract the port interface definition, and download the configuration into the device.
- **Off-line Mode**: In off-line mode, the network management software is not attached to the network or the device is not attached to the network, respectively. This mode can be used to add the device using the device templates, create the port interface definition and to make the internal connections.
- **Stand-alone Mode**: The Configurator can also be executed as a stand-alone program. This mode is useful for the engineer who doesn't want to start the configuration software as a plug-in from within network management software (e.g., NL-220, LonMaker or Alex). Instead the engineer can work directly with the device when online or engineer it offline.

6.2 Data Point Manager

The configuration software uses a central concept to manage data points. The data point manager as shown in Figure 48 is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (number 1 in Figure 48),
- The data point list (number 2 in Figure 48),
- And a property view (number 3 in Figure 48).



Model No. 00

Local datapoints

Datapoint Name Filter:

No	Direction	Datapoint Name	Local NV	Remote NV
1	In	NV_tn50Controller_1nvo00temp	nvi00temp	nvo00temp
2	Out	NV_tn50Controller_1nvi01temp	nvo01temp	nvi01temp
3	In	NV_tn50Controller_1nvo02lux	nvi02lux	nvo02lux
4	Out	NV_tn50Controller_1nvi03lux	nvo03lux	nvi03lux
5	In	NV_tn50Controller_1nvo04lev_percent	nvi04lev_percent	nvo04lev_percent
6	Out	NV_tn50Controller_1nvi05lev_percent	nvo05lev_percent	nvi05lev_percent
7	In	NV_tn50Controller_1nvo06temp_f	nvi06temp_f	nvo06temp_f
8	Out	NV_tn50Controller_1nvi07temp_f	nvo07temp_f	nvi07temp_f
9	In	NV_tn50Controller_1nvo08switch	nvi08switch	nvo08switch

Datapoint Name	NV_tn50Controller_1nvi01temp
Datapoint Path	L-Gate.CEA709 Port.Datapoints.NV_tn50Controller_1nvi01temp
Datapoint Description	
Min. Send [s]	0
Max. Send [s]	0
Max Cache Age [ms]	Infinite
Persistent	□
Default Value	N/A
Send on Delta	□
Data Point Type	Analog Datapoint
Direction	Out

Figure 48: Datapoint Manager Dialog.

6.2.1 Folder List

At the left is a list of folders which is used to sort the available data objects by their category. There are a number of predefined folders available:

- **Imported**: This folder has a number of sub-folders for different import methods:
  - **BACnet Network Scan**: This folder is used to display data points retrieved by an online scan of the BACnet network.
  - **BACnet EDE File**: This folder is used to display data points imported from an EDE file.
  - **CEA-709 CSV File:** This folder is used to display data points imported from CSV files.
  - **CEA-709 LNS Scan**: This folder is used to hold data retrieved from a network database scan.
  - **CEA709 Network Scan**: This folder holds NVs scanned online from an attached CEA-709 network.

  Data objects in the import folder are not stored on the device when the project is downloaded. They represent data objects which are available on remote devices and are shown here as templates to create suitable data objects for use on the device by selecting the **Use on Device** option.
- **Filter Templates**: This folder contains the created data point templates. They contain a set of properties, which are applied to data points, when they are created on the device. There is a sub-folder for filter templates specific to different technologies, e.g. CEA-709.
- **L-Gate**: This is the device folder of the L-Gate. It contains all the necessary data points which constitute to the L-Gate's port interface definition. These data points are created on the L-Gate when the configuration is downloaded. The three subfolders represent
  - **System Registers**: This folder contains system registers, which provide information on the device itself.
  - **User Registers**: This folder holds user-definable registers. These registers are not visible on the underlying network and are intended for internal usage.
  - **CEA-709 Port**: This folder contains data points, schedulers, calendars, trend logs, statistics, and remote data points of the CEA-709 network technology. See Section 6.2.2.
  - **BACnet Port**: This folder contains data points, schedulers, calendars, trend logs, statistics, and remote data points of the BACnet network technology. See Section 6.2.2.
- **Global Objects**: This top-level folder contains sub-folders that organize specific application objects that operate on data points.
  - **E-mail Configuration**: This folder contains e-mail templates. An e-mail template defines the destination address and text body of an e-mail, which is triggered by data points and may contain data point values or file attachments. To create an e-mail template, select the folder and use the context menu.
  - **Math Objects Configuration**: This folder contains math objects. Math objects are used to perform a predefined calculation on a number of input data points and write the result to a defined set of output data points. Each math object contains one formula. To create a math object, select the folder and use the context menu.
  - **Alarm Log Configuration**: This folder contains the alarm log objects. Each alarm log object creates a historical log of alarm transitions of one or more

alarm objects (alarm server or client). To create an alarm log, select the folder and use the context menu.

Using the context menu on a folder, sub-folders may be created to organize the available objects. If new objects are created automatically, they are usually placed in the base folder and can then be moved by the user to any of his sub-folders. Note, that the folder structure described above cannot be changed by adding or deleting folders at that level.

6.2.2 Network Port Folders

Each network port folder on the device has the same structure of sub folders. These sub folders are:

- **Datapoints**: This folder holds all data points, which are allocated on the network port. To create a data point, select the folder and use the context menu.
- **Calendar**: This folder is used to hold a locally available calendar object with its calendar patterns (definitions of day classes like holiday, maintenance day, and so on). Current devices allow one local calendar object. To create a calendar, select the folder and use the context menu.
- **Scheduler**: This folder is used for local scheduler objects. Each of these objects will map to a local scheduler on the device's network port. Configuring schedules through these objects actually transfers *schedule configuration data* to the underlying scheduler objects on the network port. To create a scheduler, select the folder and use the context menu.
- **Alarm**: This folder is used for local alarm server objects. Each of these alarm server objects represent an alarm class, which other objects can report alarms to. Other devices can use the alarm server object to get notified about alarms. To create an alarm server object, select the folder and use the context menu.
- **Trend**: This folder is used for local trend log objects. Each of these objects will be able to trend data points over time and store a local trend log file. To create a trend log object, select the folder and use the context menu.
- **Statistics**: This folder contains registers, which provide communication statistics specific to the network port.
- **Remote Devices**: This folder is used to collect all remote calendars, schedulers, trend logs, and alarm client objects, which were created from network scan data. For each remote device, a subfolder will be created where the objects referencing this device are collected.

6.2.3 Data Point List

At the top right, a list of all data objects which are available in the selected folder is shown. From this list, objects may be selected (including multi-select) in order to modify some of their properties. Click on the **Include Subfolders** button to show all data points of the selected data point folder and all its sub-folders. This can be a convenient way for multi-select across folders. To filter for data point names, enter a search text into the **Datapoint Name Filter** text box and hit *Enter*. A drop-down list holds the previously used filters available.

The list can be sorted by clicking on one of the column headers. For example, clicking on the **Direction** column header will sort the list by direction. Other columns display data point name, NV name, and SNVT. To apply the current sort order as the new data point order on the device, right-click on the column header and select **Renumber Datapoints**. Alternatively, select from the menu **Tools → Renumber Datapoints**.

New objects may be created in the selected folder by pressing the **New** button to the right of the list or via the **New** command in the context menu. A plus ⊞ sign in the list indicates that the data point contains sub-points. These can be structure members for structured SNVTs. Clicking on the plus ⊞ sign expands the view.

For the alarming, scheduling, trending (AST) features, there are columns, which display icons for data points that are attached to an AST function. See Table 7 for details.

Icon	Data Point Usage
🕒	Data point is scheduled
🔔	Data point has an active alarm condition
🔕	Data point has an inactive alarm condition.
✉	Data point is a trigger for E-Mails

Table 7: Icons for used data points in the data point list view.

6.2.4 Property View

When one or multiple data points are selected, the available properties are displayed in the property view. Properties which are read-only are marked with a lock 🔒 sign. When applying multi-select, only those properties common to all selected data points are displayed. Depending on the network technology and data point class, different properties may exist.

Data point properties common to all technologies:

- **Datapoint Name**: This is the technology-independent data point name. This name may be longer than and different to the name of the native communication object (i.e., network variable). Data point names must be unique within a given folder. The maximum length is limited to 64 ASCII characters.
- **Datapoint Path**: This informational property specifies the entire path of the data point within the data point hierarchy. The maximum length is limited to 64 ASCII characters.
- **Datapoint Description**: This is a human-readable description of the data point. There are no special restrictions for a description.
- **Use Pollcycle value as**: For input data points, this property defines whether the input shall use a receive timeout or be constantly polling. See Section 5.2.2.
- **Poll on Startup**: For input data points this property defines, whether the data point shall be polled once at start-up. Poll-on-startup can be enabled independently of the poll cycle. See Section 5.2.2.
- **Pollcycle**: For input data points, this property defines the poll cycle in seconds. Set this property to 0 to disable polling. See Section 5.2.2.
- **Receive Timeout**: For input data points, this property defines the receive timeout in seconds. Set this property to 0 to disable polling. See Section 5.2.2.
- **Min Send**: For output data points, this property defines the min send time in seconds. See Section 5.2.2.
- **Max Send**: For output data points, this property defines the max send time in seconds. See Section 5.2.2.
- **Send-on-delta**: For output data points this property defines, if value updates shall be sent only once they meet the COV condition of the data point. For analog data points the analog COV increment is used. If not checked, updates are always transmitted according to min and max send times. See Section 5.2.6.
- **Use Linear Scaling**: If this property is enabled, the analog values are pre-scaled from the technology to the data point. This scaling is in addition to any technology-specific

scaling factors. If enabled, the properties **Custom Scaling Factor** and **Custom Scaling Offset** accept the scaling factors. See Section 5.2.6.

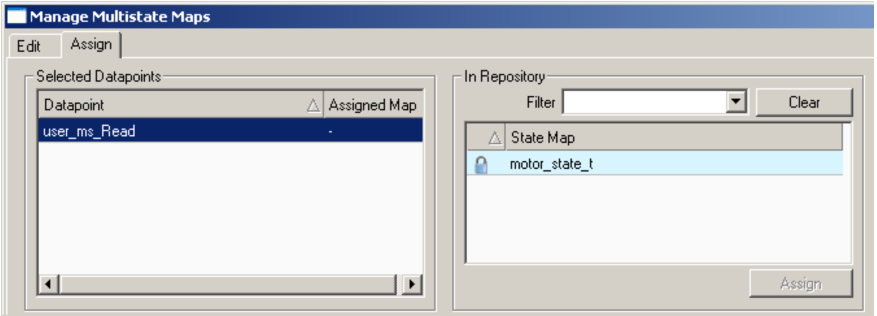
- **Custom Scaling Factor, Custom Scaling Offset**: These properties only exist, if linear scaling is enabled. They apply to analog data points only. See Section 5.2.6.
- **Only notify on COV**: This property assists for binary and multi-state input data points. It defines, if a data point shall trigger an update only when the value changes or on every write. If this is enabled, consecutive writes with the same value do not trigger an update. If you want to convey every write, disable COV on the data point.
- **Persistent**: This property defines, if the last written value shall be stored as a persistent value. Persistent data points restore that value after a restart from the persistent storage. See Section 5.2.4.
- **Default Value**: This property defines a default value (see Section 5.2.3). Enter a default value to enable this feature in the data point. Delete the value entirely to remove the default value. If no default value is defined, this property reads “N/A”. The default is no default value.
- **Point Type**: This is the base data point type, e.g., “Analog Datapoint”.
- **Direction**: This is the data point direction. Use input or output as directions.
- **Unit Text**: For analog data points this property contains a human-readable text for the engineering units of the scalar value, e.g., “kilogram”.
- **Analog Datapoint Max Value**: For analog data points this property contains the upper limit of the supported value range. Note that this does not define an alarm limit.
- **Analog Datapoint Min Value**: For analog data points this property contains the lower limit of the supported value range. Note that this does not define an alarm limit.
- **Analog Datapoint Precision**: For analog data points this property defines the number of decimals. ‘0’ specifies an integer value. Display units may use this to format the floating point value accordingly.
- **Analog Datapoint Resolution**: For analog data points this property defines the smallest possible value increment.
- **Analog Point COV Increment**: This property is valid for analog input data points. It specifies by which amount the value needs to change, before an update is generated. If every write shall generate an update even when the value does not change, specify 0 as the COV increment. If any value change shall generate an update, delete the value, which results in **Any**.
- **Active Text**: For binary data points this property defines a human-readable text for the active state (true).
- **Inactive Text**: For binary data points this property defines a human-readable text for the inactive state (false).
- **State Count**: For multi-state data points this property defines the number of discrete states.
- **State Text**: For multi-state data points this property defines a human-readable state label for each state.

6.2.5 Managing Multistate Maps

Multistate data points have a descriptive set of state texts for their state IDs. To manage those state IDs and state texts among many multistate data points, they refer to *multistate maps*. Some technologies have a fixed set of such multistate maps others have freely configurable multistate maps (e.g, user registers). Editing a multistate map affects all multistate data points, which are using that particular map. It is not necessary to edit each data point individually.

To Edit a Multistate Map

1. Click on the ... button in the State Count property of a multistate data point. This opens the multistate map manager as shown in Figure 49.



Datapoint	Assigned Map
user_ms_Read	-

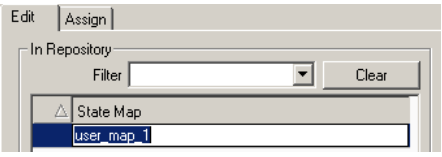
State Map
🔒 motor_state_t

Figure 49: Assign multistate maps in the multistate map manager.

2. Select an existing state map in the **State Map** list and click on **Assign**. Maps that are fixed and cannot be changed are marked with a lock symbol 🔒.

3. If a new multistate map shall be created, change to the **Edit** tab.

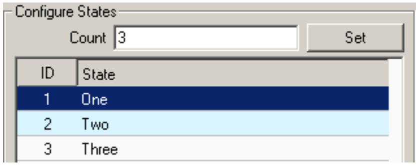
4. Click on the **Create** button and enter a new multistate map name. Then hit **Enter**.



State Map
user_map_1

5. In the **Configure States** box enter the desired number of states and click **Set**.

6. Edit the state texts as needed.

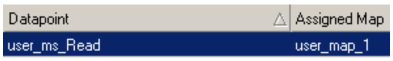


Count 3

ID	State
1	One
2	Two
3	Three

7. Change back to the **Assign** tab.

8. Select the newly created multistate map and click the **Assign** button. The assigned map is now displayed next to the data point.



Datapoint	Assigned Map
user_ms_Read	user_map_1

6.2.6 CEA-709 Properties

Apart from the common data point properties discussed in Section 6.2.4 the data points of the CEA-709 technology have additional properties. Depending on if a NV is local or external (remote), the properties may vary.

- **NV Allocation**: This property defines how a data point shall be allocated on the device. Choices are “Static NV”, “Dynamic NV”, and “External NV”. If the allocation type cannot be changed, this property is locked.
- **SNVT**: This property defines the SNVT of the NV, e.g., “lux (79)”.

- **Invalid Value**: This property defines the “invalid value” for the NV. If set, this specific value will be interpreted as “invalid” in the data point. If known by the SNVT, the invalid value is filled in. Otherwise, the user can specify an invalid value.
- **CEA-709 Mapping Information**: This information is derived from the SNVT. It defines how the NV contents are mapped to the data point.
- **NV Scaling A, B, C**: These are the scaling factors known from the SNVT table. The scaling factors are applied to translate a raw NV value into the scalar representation of the data point.
- **Data Type**: This is the basic NV data type. This is usually filled in from the SNVT definition.
- **Local NV Member Index**: This property specifies the NV member index within a given functional block. This must be a unique index in the functional block, which identifies the NV after other NVs have been added or removed from the interface.
- **Local/Remote NV Index**: This property specifies the NV index. For local, static NVs this is the NV index of the static NV. For external NVs, this is the NV index of the NV on the remote device.
- **Local/Remote NV Name**: This property specifies the programmatic name of the NV. For local, static NVs this is the programmatic name of the static NV. For external NVs, this is the programmatic name of the NV on the remote device.
- **Local/Remote Functional Block**: This property specifies the programmatic name of the NV. For local, static NVs, one of the reserved functional blocks can be selected.
- **Local/Remote NV Flags**: This property specifies the NV flags. For local (static or dynamic) NVs, the flags can be configured. For external NVs, these flags are only informational.
- **Remove NV Information**: For external NVs, this property contains the information on the remote device and the NV selector on that device.
- **Remote Device ID**: For external NVs, this property contains information on the remote device by listing the program ID and location string.
- **Remote Device Address**: For external NVs, this property contains the CEA-709 network addressing information to access the node, i.e., subnet, node, and NID.
- **Retry Count**: For external NVs, this property defines the retry count. The default is 3.
- **Repeat Timer**: For external NVs, this property defines the repeat timer in milliseconds. The default is 96 ms.
- **Transmit Timer**: For external NVs, this property defines the transmit timer in milliseconds. The default is 768 ms.
- **LNS Network Path**: If available from an LNS scan, this property specifies the LNS network path of the device where the given NV exists.
- **LNS Channel Name**: If available from an LNS scan, this property specifies the LNS channel name of the device where the given NV exists.

6.2.7 BACnet Properties

Apart from the common data point properties discussed in Section 6.2.4 the data points of the BACnet technology have additional properties. Depending on if a NV is local or external (remote), the properties may vary,

- **Engineering Units**: For analog BACnet server objects, this property defines the engineering units from the BACnet standard. One of those units can be chosen from a drop-down box, if this property is not locked.

- **Server Object Type**: This property defines the BACnet object type of the underlying BACnet server object. It can be changed within the class, i.e., for an analog data point, the server object type analog input, analog output, or analog value can be chosen.
- **Commandable**: This property defines, if the underlying BACnet server object is commandable. For BACnet value objects (AV, BV, MSV) this property can be edited to create commandable or non-commandable BACnet value objects.
- **Relinquish to invalid value**: This property defines whether the data point maintains the Relinquish_Default value, if the priority array is empty or assumes the invalid value. By default, this property is false and the Relinquish_Default value is used. Setting this property to true can be beneficial when used in a connection to withdraw a value in another technology.
- **Server Object Name**: This property defines the object name of the underlying BACnet server object. It must be unique among all server objects. It can be up to 64 characters.
- **Server Object Instance No**: This property defines the object instance number of the underlying BACnet server object.
- **Server Object Description**: This property defines the object description of the underlying BACnet server object. It can be left blank.
- **Server Object Device Type**: This property defines the object device type of the underlying BACnet server object. It can be left blank.
- **Allocate Server Object**: This Boolean property defines, if a server object shall be allocated for the data point. This option is useful, when a local server object shall be allocated for a client mapping.
- **Allocate Client Mapping**: This Boolean property defines, if a client mapping shall be allocated for the data point. This option is always set, if at least on client mapping is attached.
- **Client Map Count**: This property defines the number of client mappings attached to a data point. A data point can have one read client map or *n* write client mappings.
- **Client Map [n]**: This is a list of client mappings. The property shows a summary of the client mapping parameters. To edit a client mapping click on the **…** button.
- **Confirmed COV**: This Boolean property defines, if a client map subscribes with the confirmed COV service. If not enabled, the unconfirmed COV is used.

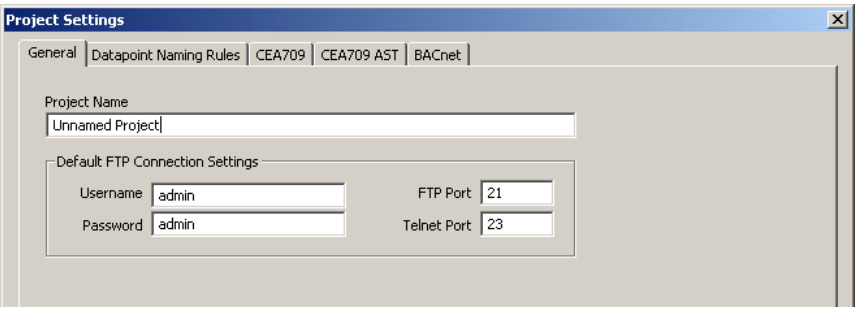
6.3 Project Settings

The project settings allow defining certain default behavior and default settings used throughout the project. To access the project settings go to the menu **Settings → Project Settings…** . This opens the project settings dialog, which provides several tabs as described in the following sections.

6.3.1 General

The general tab of the project settings as shown in Figure 50 contains settings independent of the technology port. The settings are:

- **Project Name**: This setting allows entering a descriptive name for the project.
- **Default FTP Connection Settings**: Enter a user name and password for the default FTP access. This access method is used implicitly when connected via LNS and the device is accessible over IP. For this implicit connection, there is no dialog to ask for a username and password and the username and the default password from the project settings are used.



Project Settings

General | Datapoint Naming Rules | CEA709 | CEA709 AST | BACnet

Project Name: Unnamed Project

Default FTP Connection Settings

Username: admin

Password: admin

FTP Port: 21

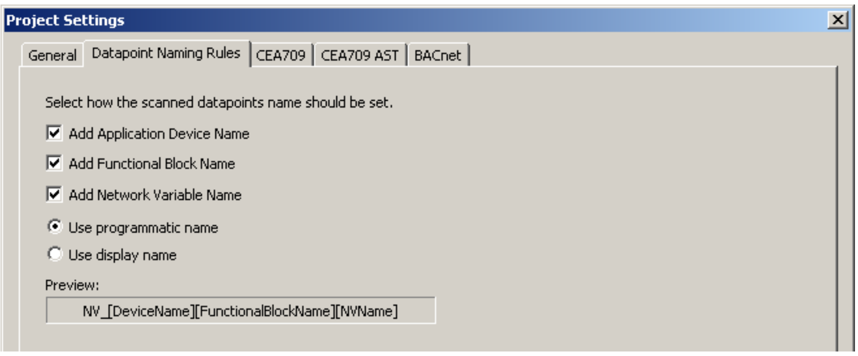
Telnet Port: 23

Figure 50: General Project Settings.

6.3.2 Data Point Naming Rules

The data point naming rules tab (see Figure 51) allows specifying, how data point names are automatically derived from scanned network variables. The preview shows how names would look like, when the check marks are modified.

The option **Use programmatic name** and **Use display name** decides whether the data point name is assembled of the programmatic NV name or the LNS display name.



Project Settings

General | Datapoint Naming Rules | CEA709 | CEA709 AST | BACnet

Select how the scanned datapoints name should be set.

☑ Add Application Device Name

☑ Add Functional Block Name

☑ Add Network Variable Name

● Use programmatic name

○ Use display name

Preview: NV_[DeviceName][FunctionalBlockName][NVName]

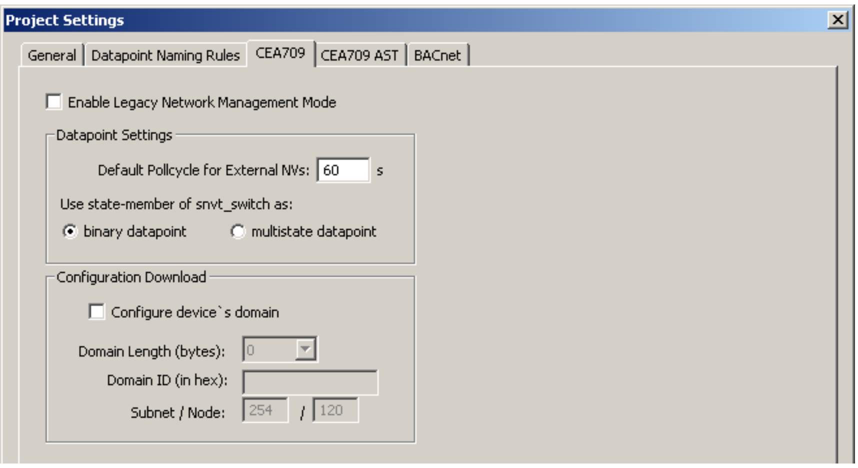
Figure 51: Data Point Naming Rules Project Settings.

6.3.3 CEA-709 Settings

The CEA-709 configuration tab as shown in Figure 52 allows configuring properties of the device’s CEA-709 port. The options are:

- **Enable Legacy Network Management Mode**: This group box contains check boxes for each CEA-709 port of the device. Put a check mark on the port, if this port shall be operated in the legacy network management mode. In that mode, the port does not use the extended command set (ECS) of network management commands. This can be necessary to operate the device with some network management tools, that do not support the ECS. See Section 6.4.3 for more information on how to configure such a system.
- **Default Pollcycle for External NVs**: When using external NVs, this poll cycle is set as a default for input data points. The poll cycle can be edited individually in the properties view of the data point manager.
- **Use state-member of SNVT_switch as**: This setting defines how the state member of the SNVT_switch shall be mapped to a data point. Depending on how the data point shall be used, it can be binary or multi-state. The multi-state setting allows setting the UNSET state explicitly. As a binary point the UNSET state is implicitly chosen, if the value is invalid.
- **Configuration Download**: This group box contains self-configuration settings for the CEA-709 ports. This is necessary, when the device shall be used without being commissioned by a network management tool. Set the check mark and enter the CEA-

709 domain and subnet/node information. If operated in self-configured mode, the CEA-709 network can be scanned using the network scan (see Section 6.7.6) and external NVs can be used on the device. Note, that the domain must match the nodes' domain on the network and the subnet/node address must not be used by another device.



□ Enable Legacy Network Management Mode

Datapoint Settings

Default Pollcycle for External NVs: 60 s

Use state-member of snvt_switch as:

● binary datapoint ○ multistate datapoint

Configuration Download

□ Configure device`s domain

Domain Length (bytes): 0

Domain ID (in hex):

Subnet / Node: 254 / 120

Figure 52: CEA-709 Project Settings.

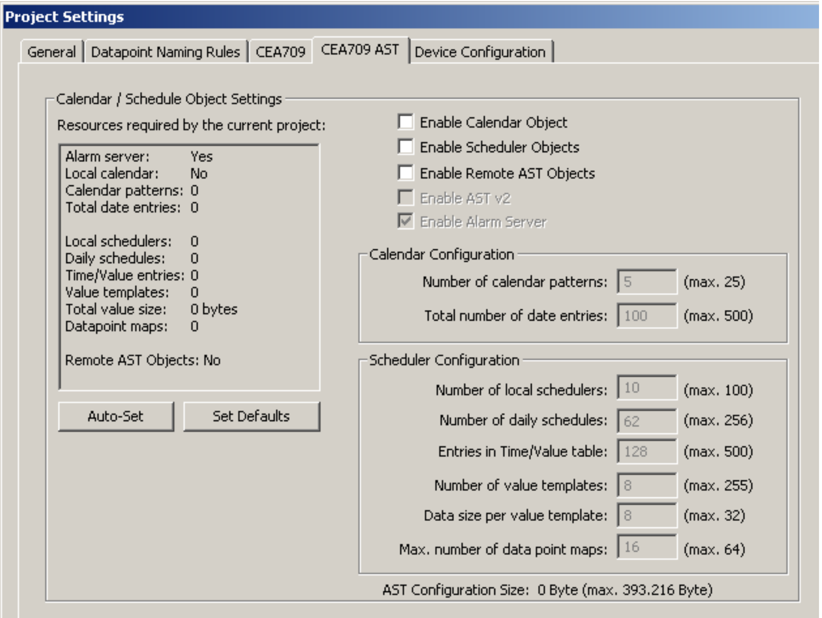
6.3.4 AST Settings

For CEA709 devices, the use of alarming, scheduling, trending (AST) features requires additional resources (functional objects and NVs). The dialog is shown in Figure 53. Changes made there affect the static interface. Since the number of used resources also influences the performance, the CEA-709 AST tab allows configuring those resources for the project. In this tab the required number of scheduler units that may be instantiated and their capacity may be configured (how many time/value entries, value templates, bytes per value template, and so on). It contains the following options and settings, which are relevant to calendar and scheduler functionality of the device:

- **Enable Calendar Object:** This checkbox enables a LONMARK compliant calendar object on the device. It is automatically enabled together with local schedulers, since the two are always used together.
- **Enable Scheduler Objects:** This checkbox enables local LONMARK compliant scheduler objects on the device. Checking this box will automatically enable the calendar as well.
- **Enable Remote AST Objects:** This checkbox enables the functional object for NVs, which are used to access remote AST objects. If this box is checked, the *Clients* functional block is included in the static interface.
- **Enable AST v2:** This checkbox enables the AST interface version 2 for local CEA-709 schedulers on the device. This interface is not compatible with older devices. The new interface provides access to the value label descriptions in schedule presets for remote schedulers.
- **Number of calendar patterns:** Specifies the maximum number of different exception schedules (day classes like holiday, maintenance day) supported by this calendar object.
- **Total number of date entries:** Specifies the maximum number of date definitions which may be stored by the calendar. This is the sum of all date definitions from all calendar entries. A date definition is for example a single date, a date range, or a week and day pattern (every last Friday in April).
- **Number of local schedulers:** This is the number of local scheduler objects which should be available on the device. Each local scheduler data point created in the data

point manager will connect to one of these scheduler objects. There may be more scheduler objects available on the device than are actually used at a certain time. It is a good idea to have some spare scheduler objects ready, in case another scheduler is needed.

- **Number of daily schedules:** This is the maximum number of schedules supported by each scheduler object. This number must at least be 7, since a scheduler always needs to provide one schedule for each day of the week (default weekly schedule). For each special day defined by the calendar or embedded exception day, an additional daily schedule is required to support it.
- **Entries in Time/Value table:** This is the total number of entries in each scheduler defining a value template that should apply on a specific day starting at a specific time (the time table).
- **Number of value templates:** This is the maximum number of value templates supported by each scheduler.
- **Data size per value template:** This specifies the buffer size reserved to hold the data for each value template. More data points or bigger data structures require a bigger value buffer.
- **Max. number of data point maps:** Specifies the maximum number of individual data points that this scheduler is able to control.



Calendar / Schedule Object Settings

Resources required by the current project:

```
Alarm server:       Yes
Local calendar:     No
Calendar patterns:  0
Total date entries: 0

Local schedulers:   0
Daily schedules:    0
Time/Value entries: 0
Value templates:    0
Total value size:   0 bytes
Datapoint maps:     0

Remote AST Objects: No
```

☐ Enable Calendar Object
☐ Enable Scheduler Objects
☐ Enable Remote AST Objects
☐ Enable AST v2
☑ Enable Alarm Server

Calendar Configuration

Number of calendar patterns:	5	(max. 25)
Total number of date entries:	100	(max. 500)

Scheduler Configuration

Number of local schedulers:	10	(max. 100)
Number of daily schedules:	62	(max. 256)
Entries in Time/Value table:	128	(max. 500)
Number of value templates:	8	(max. 255)
Data size per value template:	8	(max. 32)
Max. number of data point maps:	16	(max. 64)

AST Configuration Size: 0 Byte (max. 393.216 Byte)

Figure 53: CEA-709 AST Project Settings.

As can be seen from the above list, it is not easy to configure a LONMARK scheduler object. There are many technical parameters which need to be set and which require some knowledge of how these scheduler objects work internally. Therefore, the configuration software provides the following mechanisms to help in choosing the right settings:

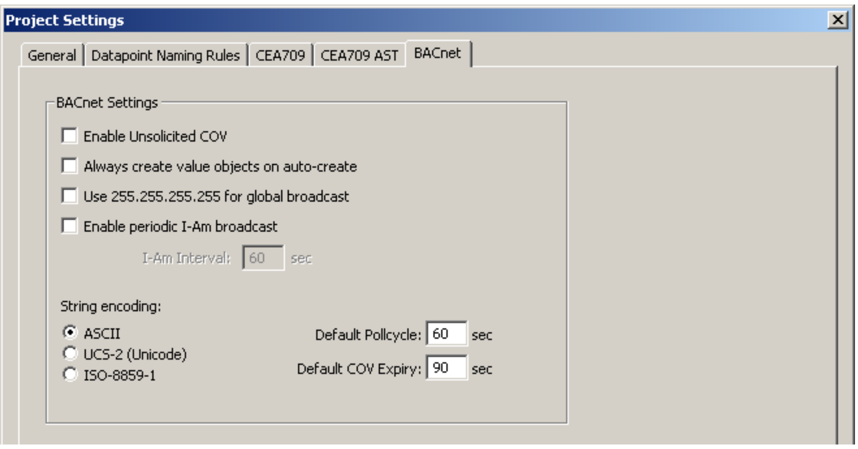
- **Resources required by the current project:** The absolute minimum settings required by the current project are shown in a table at the left side of the window. This data may be used to fill in the values at the right side, but some additional resources should be planned to allow for configuration changes which need more resources.
- **Auto-Set:** This button may be used to let the configuration software decide on the best settings to use, based on the current project. Since the current projects resource usage is taken as a starting point, all schedulers and calendar patterns in the project should first be configured as required before this button is used.

- **Set Defaults:** This button will choose standard values for all settings. In most cases, these settings will provide more resources than necessary.

6.3.5 BACnet Settings

The BACnet configuration tab as shown in Figure 54 allows configuring properties of the device's BACnet port. The options are:

- **Enable Unsolicited COV**: Put a check mark on this option to enable COV-U on the BACnet port. When active, the device sends unsolicited COV broadcast on all BACnet objects, when their value changes in accordance to the respective COV rules.
- **Always create value objects on auto-create**: If activated, the auto-create BACnet points function of the configuration software creates commandable value objects (AV, BV, MV) instead of output objects (AO, BO, MO) and non-commandable value objects (AV, BV, MV) instead of input objects (AI, BI, MI). This feature can be activated if the regular input/output model is not desired.
- **Use 255.255.255.255 for global broadcast**: This setting overrides the standard behavior of BACnet to send broadcasts as global IP broadcasts. This can solve scanning problems with some BACnet devices.
- **Enable periodic I-Am broadcast**: This setting enables the periodic transmission of I-Am broadcasts. Specify the interval in seconds. If disabled, the device sends an I-Am only when starting up. This is the default behavior of BACnet devices.
- **Encode all strings**: This setting defines how strings in BACnet objects are encoded. By default it is ASCII, which is compatible with most BACnet software. To support characters of Western European languages, choose ISO-8859-1. To support Unicode character sets (e.g., Japanese) select UCS-2.
- **Default Poll cycle, Default COV Expiry**: This setting defines the default values that are used when creating new client mappings. Changing this option does not affect already existing client mappings.



☐ Enable Unsolicited COV
☐ Always create value objects on auto-create
☐ Use 255.255.255.255 for global broadcast
☐ Enable periodic I-Am broadcast
I-Am Interval: 60 sec

String encoding:
● ASCII
○ UCS-2 (Unicode)
○ ISO-8859-1

Default Pollcycle: 60 sec
Default COV Expiry: 90 sec

Figure 54: BACnet Project Settings.

6.4 Workflows for the L-Gate

This section discusses a number of work flows for configuring the L-Gate in different use cases in addition to the simple use case in the quick-start scenario (see Section 2.3). The description is intended to be high-level and is depicted in a flow diagram. The individual steps refer to later Sections, which describe each step in more detail. In principle, the L-Gate Configurator supports the following use cases:

- Network Management Tool based on LNS 3.x (see Section 6.4.2)

- Non-LNS 3.x network management tool with polling (see Section 6.4.3)
- Non-LNS 3.x network management tool with bindings (see Section 6.4.4)

6.4.1 Involved Configuration Files

In the configuration process, there are a number of files involved:

- XIF file: This is the standard file format to exchange the static interface of a device. This file can be used to create a device in the database without having the L-Gate on-line. There exists a standard XIF file for the FT port (L-Gate-900 FT-10.xif) and one for the IP-852 port (L-Gate-900 10L.xif).
- L-Gate Configurator project file: This file contains all ports, data points, and connections of a project. These files end with “.gtw”. It stores all relevant configuration data and is intended to be saved on a PC to backup the L-Gate’s data point configuration.

6.4.2 Configure with LNS

The flow diagram in Figure 55 shows the steps that need to be followed in order to configure the L-Gate in a network with LNS 3.x. In this scenario the L-Gate will use dynamic NVs and bindings.

First, the L-Gate device must be added to LNS (see Section 6.4.6). Then the L-Gate Configurator must be started in plug-in mode to configure the L-Gate (see Section 6.7.1). In the Configurator scan for the data points in the LNS database (see Section 6.7.4). Select the NVs that the L-Gate shall expose to BACnet (see Section 6.7.7). Generate BACnet objects and connections from the used NVs (see Section 6.7.11). Finally, the configuration needs to be downloaded onto the L-Gate (see Section 6.7.13). It is recommended to save the complete configuration to a disk file for being able to replace an L-Gate in the network.

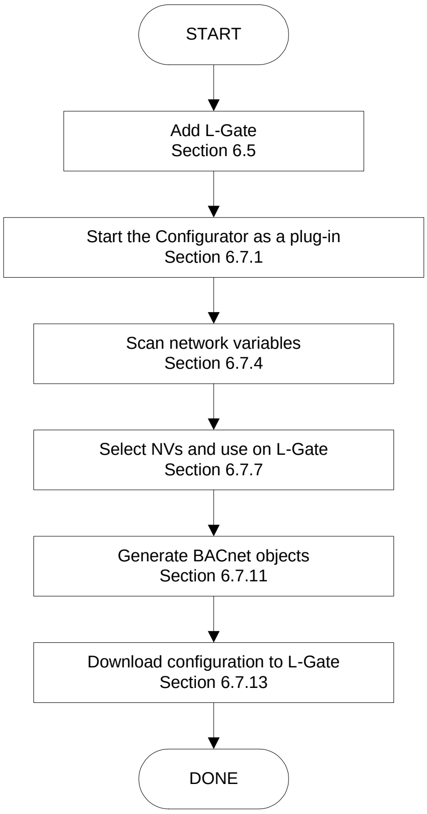


Figure 55: Basic design-flow with LNS.

To add more NVs when all bindings are in place and the L-Gate is being used simply repeat the steps described above. The Configurator software will back up the bindings, create or delete the dynamic NVs, and re-create the bindings again.

6.4.3 Configure without LNS

The flow diagram in Figure 56 shows the steps that need to be followed in order to configure the L-Gate without LNS 3.x. In this scenario the L-Gate will use external NVs and polling. The advantage of this solution is that no bindings in the non-LNS tool (or self-binding nodes) need to be changed. This comes at the cost of a constant network load caused by polling.

Start the Configurator in stand-alone mode and connect to the L-Gate via the FTP method (see Section 6.7.2). If changing an existing configuration upload the current configuration from the L-Gate (see Section 4). In the Configurator import data points from a CSV import file (see Section 6.7.5) or scan an CEA-709 network online (see Section 6.7.6). Select the NVs that the L-Gate shall expose to BACnet (see Section 6.7.7). Alternatively, you can create external NVs manually (see Section 6.7.10). Generate BACnet objects and connections from the used NVs (see Section 6.7.11). Finally, the configuration needs to be downloaded onto the L-Gate (see Section 6.7.13). It is recommended to save the complete configuration to a disk file for being able to replace an L-Gate in the network.

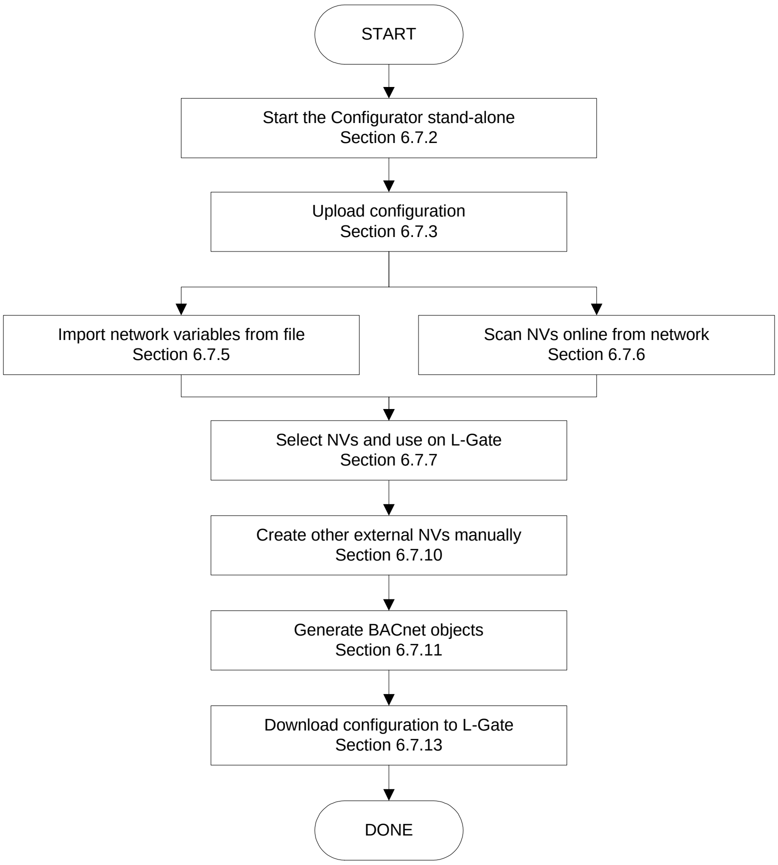

START
Start the Configurator stand-alone
Section 6.7.2
Upload configuration
Section 6.7.3
Import network variables from file
Section 6.7.5
Scan NVs online from network
Section 6.7.6
Select NVs and use on L-Gate
Section 6.7.7
Create other external NVs manually
Section 6.7.10
Generate BACnet objects
Section 6.7.11
Download configuration to L-Gate
Section 6.7.13
DONE

Figure 56: Basic design-flow without LNS.

6.4.4 Configure without LNS Using Bindings

The flow diagram in Figure 57 shows the steps that need to be followed in order to configure the L-Gate without LNS 3.x. In this scenario the L-Gate will use static NVs and bindings. The advantage of this solution is that the network load is minimized. However, the non-LNS management tool must create bindings for the L-Gate and update an existing network.

Start the L-Gate Configurator in stand-alone mode and connect to the L-Gate via the FTP method (see Section 6.7.2). In the Configurator import data points from a CSV import file (see Section 6.7.5) or scan a CEA-709 network online (see Section 6.7.6). Select the NVs that the L-Gate shall expose to BACnet (see Section 6.7.7). For the NVs used on the L-Gate select the "static NV" allocation type (see Section 6.7.8). Alternatively, you can create static NVs manually (see Section 6.7.9).

For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured (see Section 6.7.15). Please contact the tool's vendor for information whether ECS is supported or not.

Generate BACnet objects and connections from the used NVs (see Section 6.7.11). Download the configuration onto the L-Gate (see Section 6.7.13). Finally, export a XIF file (see Section 6.7.14). It is recommended to save the complete configuration to a disk file for being able to replace an L-Gate in the network.

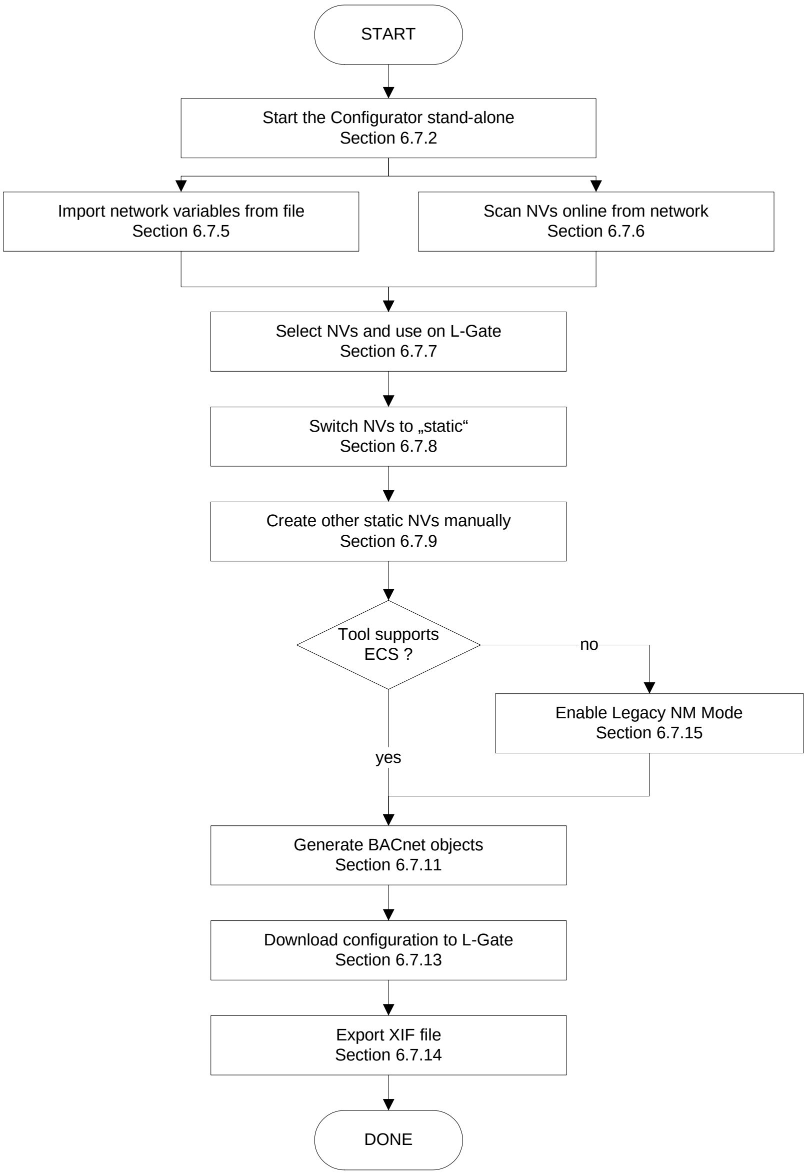


Figure 57: Basic design-flow without LNS using bindings.

To use the L-Gate in the non-LNS management tool, commission the L-Gate using the exported XIF file and create the bindings.

When changing a running L-Gate configuration with existing bindings, it is recommended to create additional data points as external NVs with polling as described in Section 6.4.3. Otherwise, a new XIF file needs to be exported and replacing the L-Gate in the non-LNS tool requires the user to create all bindings again from scratch (see Section 5.5.2).

6.4.5 Replace an L-Gate

An L-Gate can be replaced in the network by another unit. This might be necessary, if a hardware defect occurs. First of all, the replacement L-Gate needs to be configured with the appropriate IP settings, including all relevant BACnet device settings. The remainder of this section focuses on the L-Gate data point configuration. The work flow is depicted in Figure 58.

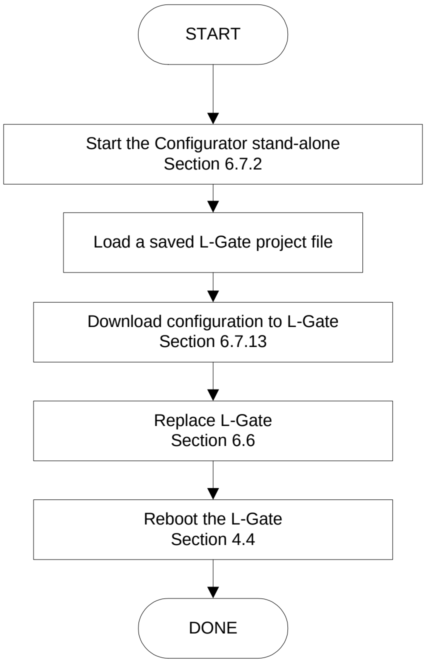

START
Start the Configurator stand-alone
Section 6.7.2
Load a saved L-Gate project file
Download configuration to L-Gate
Section 6.7.13
Replace L-Gate
Section 6.6
Reboot the L-Gate
Section 4.4
DONE

Figure 58: Basic work flow to configure a replacement device.

Start the L-Gate Configurator software stand-alone and connect via the FTP method (see Section 6.7.2). Then load the L-Gate configuration project file from disk, which has been saved when the original L-Gate has been configured or modified. Double-check, if the data point configuration seems sensible. Then download the configuration to the L-Gate (see Section 6.7.13).

If using an LNS-based tool, the L-Gate device needs to be replaced in that tool (see Section 6.6). If you are not using LNS, then refer to your network management tool’s reference manual on how to replace a device. After replacing the device in the network management tool, reboot the L-Gate (see Section 4.4)

6.4.6 Configure from BACnet

The flow diagram in Figure 59 shows the steps that need to be followed in order to configure the L-Gate from the BACnet side. In this scenario the L-Gate will be configured with BACnet data points from the BACnet network. The CEA-709 side of the gateway has to be engineered as described in the previous section, but without automatic BACnet object creation. The remainder of this section assumes that NVs and the static interface have been configured already.

Start the L-Gate Configurator in stand-alone mode and connect to the L-Gate via the FTP method (see Section 6.7.2). In the Configurator use the BACnet network scan to find BACnet objects in the network (see Section 6.10.1) or import BACnet objects from an EDE file (see Section 6.10.2). Select the remote BACnet objects, that the L-Gate shall access and use them on the device to create client mappings on the L-Gate (see Section 6.10.3). Alternatively, you can create BACnet server objects manually (see Section 6.10.5).

Once the BACnet client mappings or server objects have been created on the BACnet port, connections need to be created (see Section 6.9.1). This has to be done manually by selecting the BACnet object and the NV, where this BACnet object shall be exposed to.

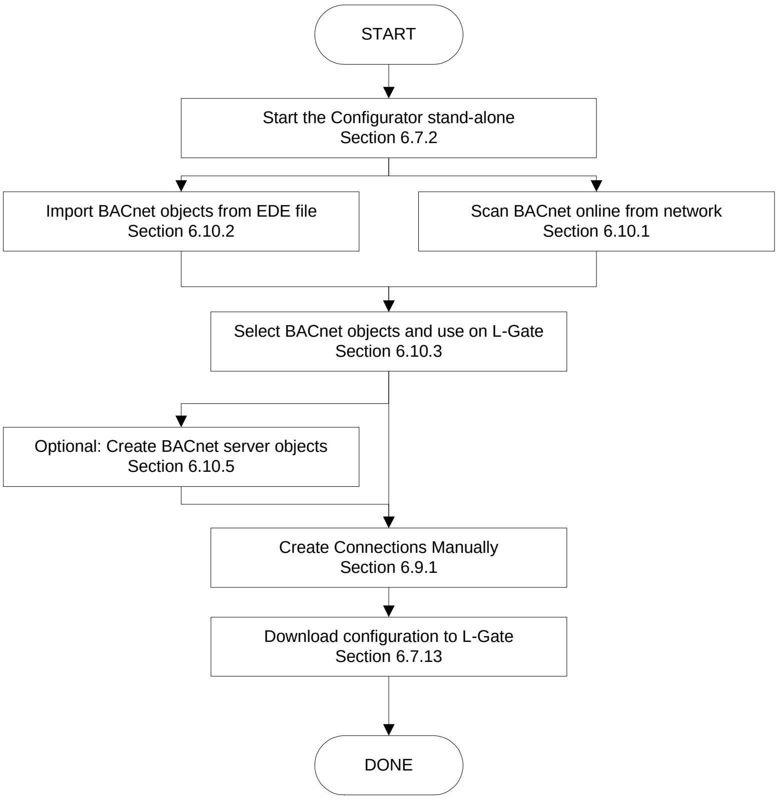

START
Start the Configurator stand-alone
Section 6.7.2
Import BACnet objects from EDE file
Section 6.10.2
Scan BACnet online from network
Section 6.10.1
Select BACnet objects and use on L-Gate
Section 6.10.3
Optional: Create BACnet server objects
Section 6.10.5
Create Connections Manually
Section 6.9.1
Download configuration to L-Gate
Section 6.7.13
DONE

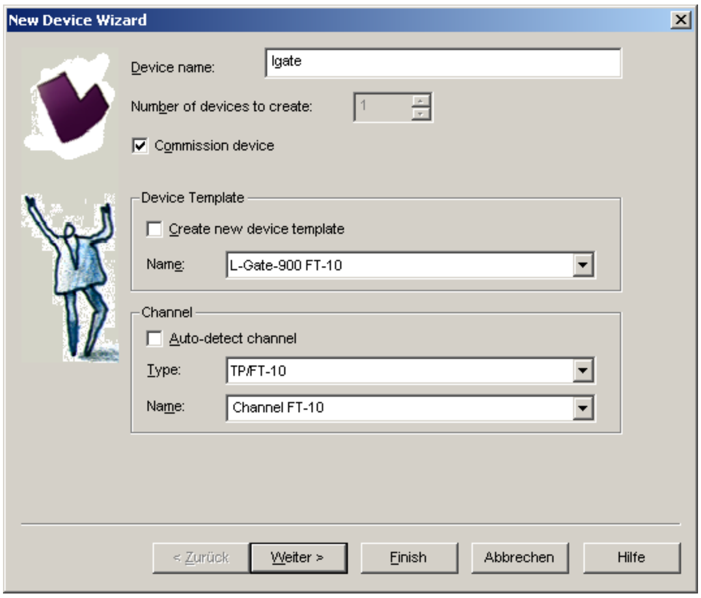
Figure 59: Basic design-flow from BACnet.

6.5 Adding L-Gate

To configure an L-Gate in your LonMaker drawing, the device needs to be added to the LNS database and commissioned. This Section refers to LonMaker TE and describes how to add an L-Gate to your database.

To Add a Device to LonMaker TE

1. In your LonMaker drawing, drag a device stencil into the drawing. Enter an appropriate name as shown in Figure 60.



New Device Wizard

Device name: lgate

Number of devices to create: 1

☑ Commission device

Device Template

□ Create new device template

Name: L-Gate-900 FT-10

Channel

□ Auto-detect channel

Type: TP/FT-10

Name: Channel FT-10

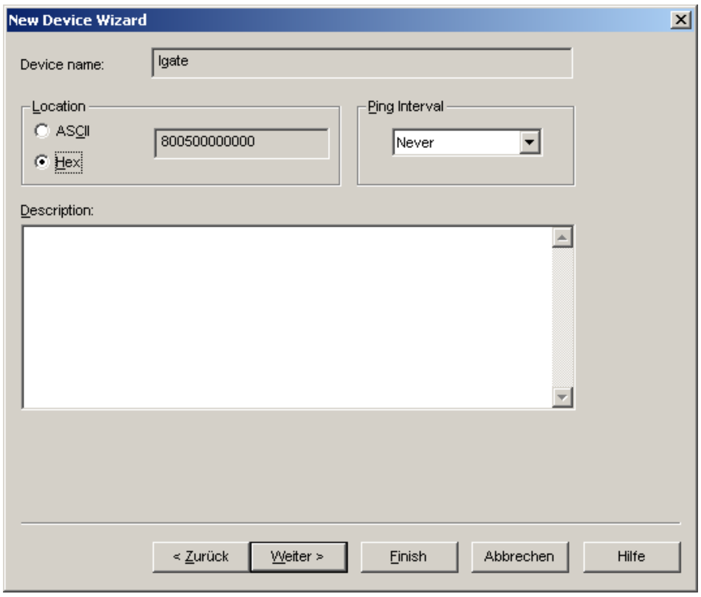
Figure 60: Create a new device in the drawing.

2. Select **Commission Device** if the device is already connected to the network.

3. In the **Device Template** group box select the existing device template of the L-Gate. Select "L-Gate-900 FT-10", if the L-Gate is configured to use the FT-10 interface, or "L-Gate-900 IP-10L", if the L-Gate is configured to be on the IP channel. For information on how to configure which port to use, refer to Section 4.2.5 for the Web UI.

4. Select the channel, which the device is connected to and click **Next**.

5. The following dialog shown in Figure 61 appears, click **Next**.



New Device Wizard

Device name: lgate

Location

○ ASCII

● Hex

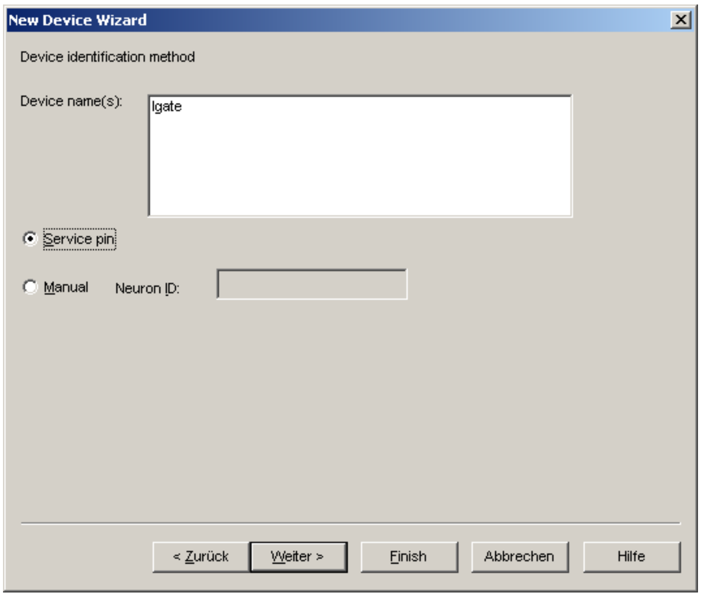
800500000000

Ping Interval: Never

Description:

Figure 61: Leave defaults for Location.

6. Check Service Pin as the device identification method as shown in Figure 62 and click **Next**.



New Device Wizard

Device identification method

Device name(s): lgate

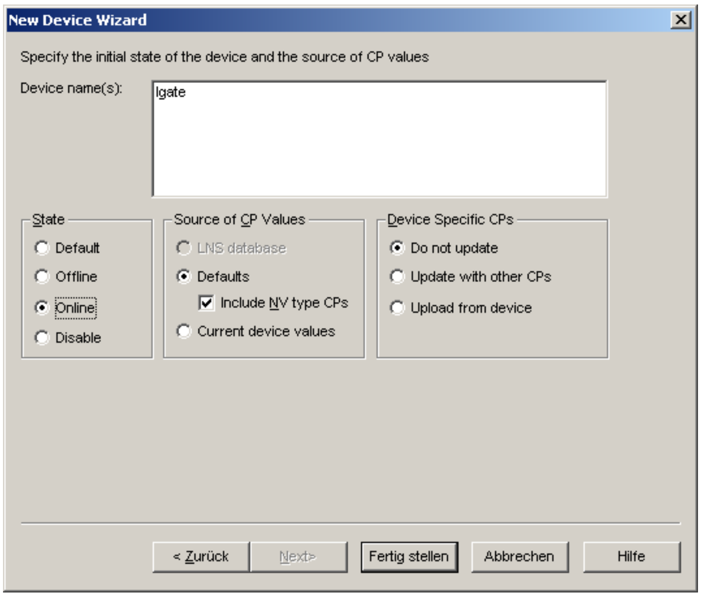
● Service pin

○ Manual   Neuron ID:

Figure 62: Use Service Pin.

7. Click **Next** in the following screens until you get to the final dialog shown in Figure 63.

8. If the device is already on-net, select **Online**.



New Device Wizard

Specify the initial state of the device and the source of CP values

Device name(s): lgate

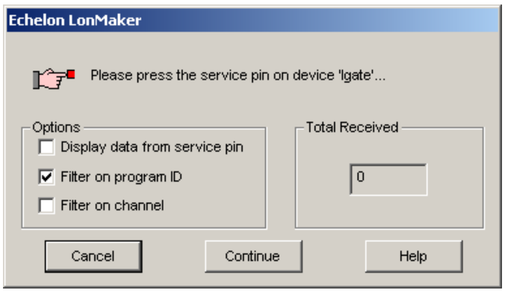
State
○ Default
○ Offline
● Online
○ Disable

Source of CP Values
○ LNS database
● Defaults
☑ Include NV type CPs
○ Current device values

Device Specific CPs
● Do not update
○ Update with other CPs
○ Upload from device

Figure 63: Final dialog.

9. Click **Finish**. A dialog will prompt to press the service pin.



Echelon LonMaker

Please press the service pin on device 'lgate'...

Options
- ☐ Display data from service pin
- ☑ Filter on program ID
- ☐ Filter on channel

Total Received: 0

10. Finally, you should get the device added to your drawing as depicted in Figure 64.

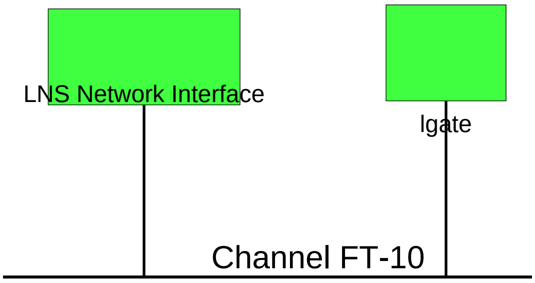


Figure 64: The L-Gate has been added to the drawing.

6.6 Replace an L-Gate

This Section describes how to replace an L-Gate in your LNS database. The description refers to LonMaker TE. Let’s assume there is a device ‘lgate’ in the LNS database as shown in Figure 65.

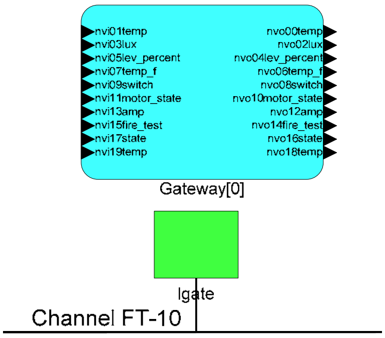
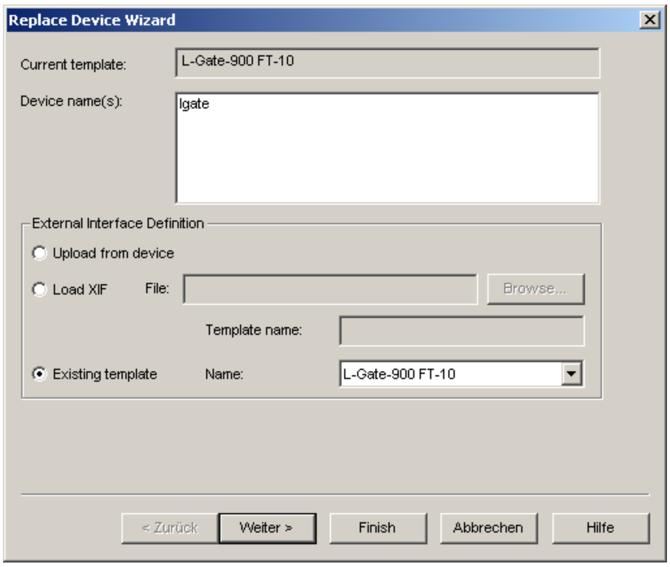


Figure 65: LonMaker drawing with one L-Gate.

To Replace a Device in LonMaker TE

1. Select the device and right-click on the device shape.

2. Select **Commissioning → Replace…**. This opens the LonMaker Replace Device Wizard as shown in Figure 66.


Replace Device Wizard

Current template: L-Gate-900 FT-10

Device name(s): lgate

External Interface Definition

○ Upload from device

○ Load XIF File:

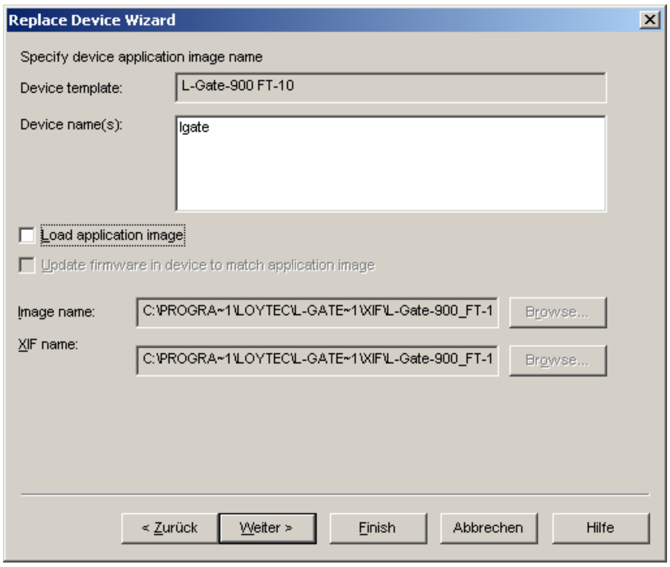
Template name:

● Existing template Name: L-Gate-900 FT-10

Figure 66: LonMaker replace device wizard.

3. Choose the existing device template and click **Next**.

4. In the following window shown in Figure 67 click **Next**.


Replace Device Wizard

Specify device application image name

Device template: L-Gate-900 FT-10

Device name(s): lgate

□ Load application image

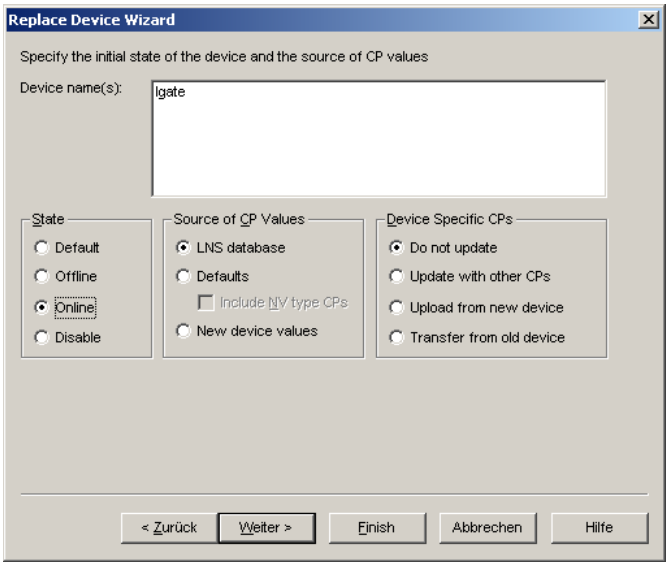
□ Update firmware in device to match application image

Image name: C:\PROGRA~1\LOYTEC\L-GATE~1\XIF\L-Gate-900_FT-1

XIF name: C:\PROGRA~1\LOYTEC\L-GATE~1\XIF\L-Gate-900_FT-1

Figure 67: Click Next without loading an application image.

5. Then select **Online** as shown in Figure 68 and click **Next**.



Replace Device Wizard

Specify the initial state of the device and the source of CP values

Device name(s): lgate

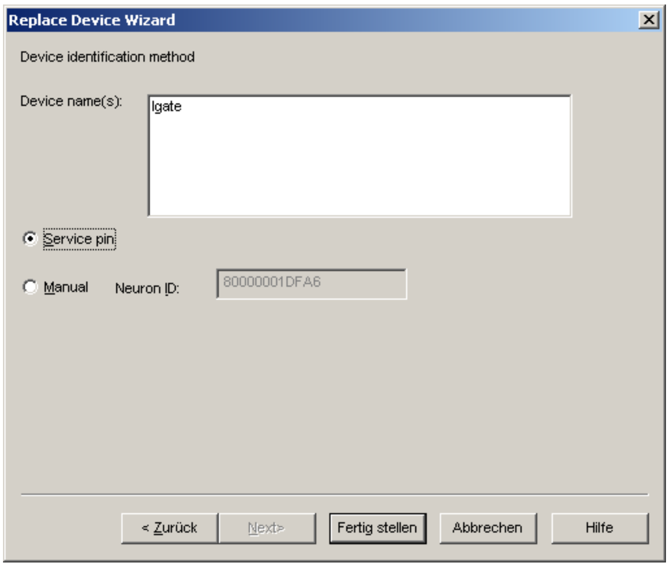
State
○ Default
○ Offline
● Online
○ Disable

Source of CP Values
● LNS database
○ Defaults
□ Include NV type CPs
○ New device values

Device Specific CPs
● Do not update
○ Update with other CPs
○ Upload from new device
○ Transfer from old device

Figure 68: Select online state.

6. Select the **Service pin** method and click on **Finish** as shown in Figure 69.



Replace Device Wizard

Device identification method

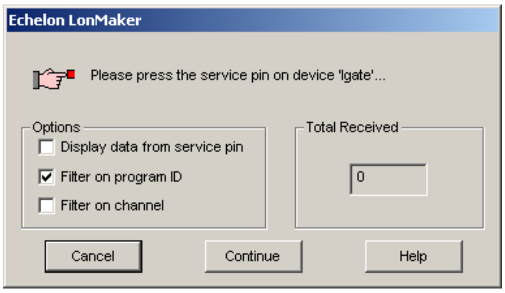
Device name(s): lgate

● Service pin

○ Manual Neuron ID: 80000001DFA6

Figure 69: Select Service Pin and click Finish.

7. Then the service pin requestor opens as shown in Figure 70. Press the service pin on the replacement L-Gate on the correct port. You can also send the service pin using the Web interface (see Section 4.1).



Echelon LonMaker

Please press the service pin on device 'lgate'...

Options
□ Display data from service pin
☑ Filter on program ID
□ Filter on channel

Total Received: 0

Figure 70: Wait for the service pin from the device.

8. After the service pin has been received, LonMaker commissions the replacement device, creates the dynamic NVs again (if any), and installs the bindings.

6.7 Using the L-Gate Configurator

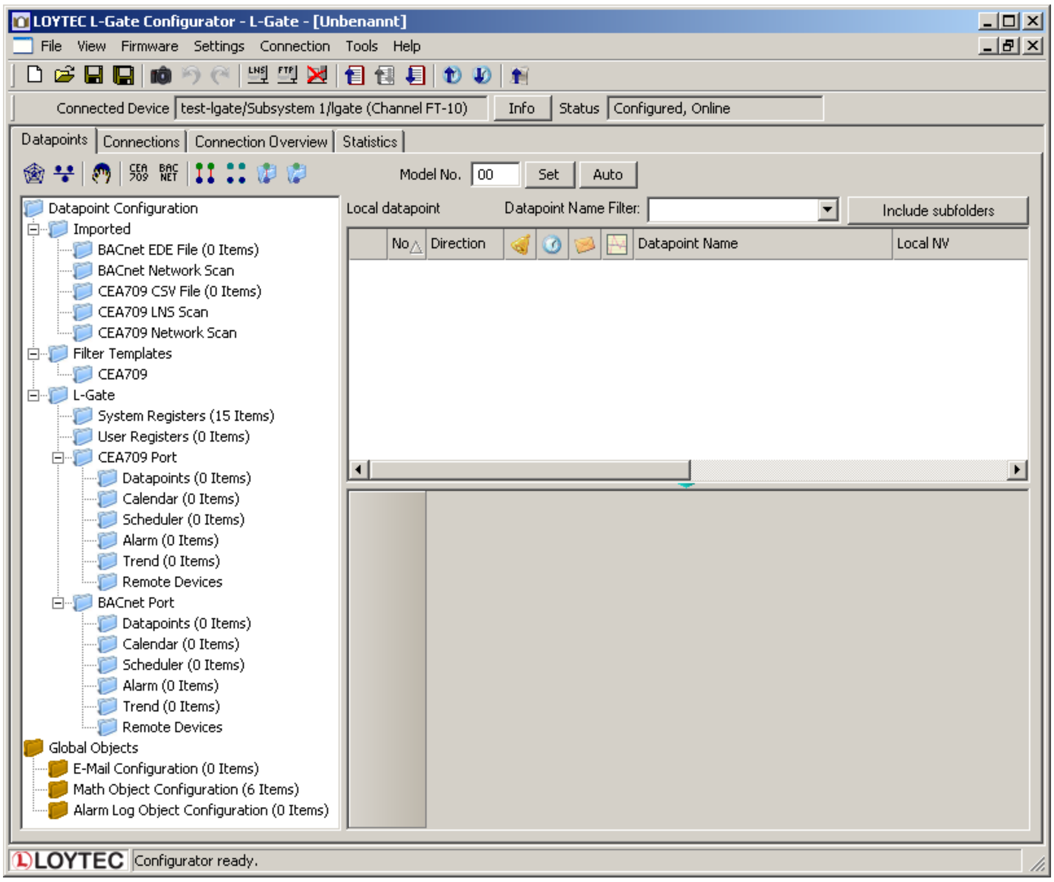
6.7.1 Starting as an LNS Plug-In

In LonMaker the plug-in is started by right-clicking on the L-Gate device shape or the Gateway functional block and selecting **Configure…** from the pop-up window.

In NL-220 the Plug-in is started by right clicking on the L-Gate node, then selecting the Option **LOYTEC L-Gate Configurator** in the **PlugIns** sub menu.

In Alex the Plug-in is started by right-clicking on the L-Gate device and selecting the **LOYTEC L-Gate Configurator** in the **Starte PlugIn** sub menu.

A window similar to what is shown in Figure 71 should appear.



Connected Device: test-lgate/Subsystem 1/lgate (Channel FT-10)
Status: Configured, Online
Model No.: 00
Local datapoint
Datapoint Name Filter:

- Datapoint Configuration
  - Imported
    - BACnet EDE File (0 Items)
    - BACnet Network Scan
    - CEA709 CSV File (0 Items)
    - CEA709 LNS Scan
    - CEA709 Network Scan
  - Filter Templates
    - CEA709
  - L-Gate
    - System Registers (15 Items)
    - User Registers (0 Items)
    - CEA709 Port
      - Datapoints (0 Items)
      - Calendar (0 Items)
      - Scheduler (0 Items)
      - Alarm (0 Items)
      - Trend (0 Items)
      - Remote Devices
    - BACnet Port
      - Datapoints (0 Items)
      - Calendar (0 Items)
      - Scheduler (0 Items)
      - Alarm (0 Items)
      - Trend (0 Items)
      - Remote Devices
- Global Objects
  - E-Mail Configuration (0 Items)
  - Math Object Configuration (6 Items)
  - Alarm Log Object Configuration (0 Items)

Configurator ready.

Figure 71: L-Gate Configurator main window.

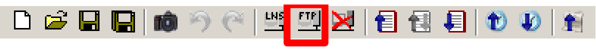
6.7.2 Starting Stand-Alone

The L-Gate can also be used without LNS-based tools. In this case, the L-Gate Configurator needs to be started as a stand-alone application. Go to the Windows **Start** menu, select **Programs**, **LOYTEC L-Gate Configurator** and then click on **Configure L-Gate**. This starts the L-Gate Configurator and the main connections screen is displayed.

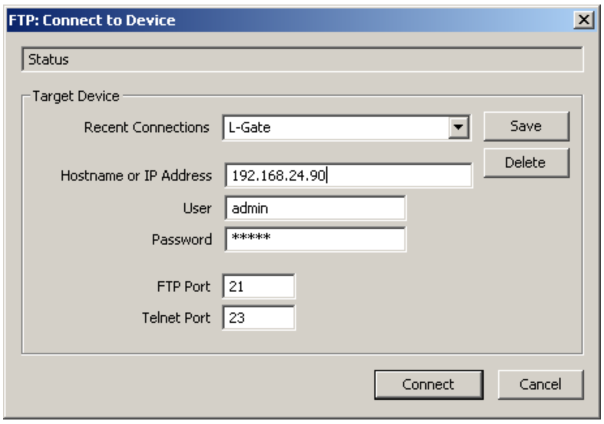
If the L-Gate is not yet connected to the network, go to the **Firmware** menu and select the firmware version of the L-Gate to be configured. If the L-Gate is already connected to the network it is recommended to connect the configuration software to the L-Gate.

To Connect to an L-Gate Stand-Alone

1. Select the FTP connection method by clicking on the **FTP connect** button



in the tool bar of the main connections window. The FTP connect dialog as shown in Figure 72 opens.


FTP: Connect to Device

Status

Target Device

Recent Connections: L-Gate

Hostname or IP Address: 192.168.24.90

User: admin

Password: *****

FTP Port: 21

Telnet Port: 23

Figure 72: FTP connection dialog.

2. Enter the IP address of the L-Gate, the user and password. The default user is ‘admin’ and the default password is ‘admin’.

3. Optionally, click into the **Recent Connections** field and enter a user-defined name for this connection. That name can be selected later to connect. Click on **Save** to store that connection.

4. If your device is located behind a NAT router of firewall, you may change the FTP and Telnet ports to your needs for accessing the device. Clicking **Save** also stored these settings.

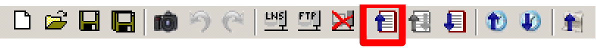
5. Click on **Connect**. This establishes the connection to the device.

6.7.3 Uploading the Configuration

To get the current network variable configuration of the L-Gate, the port interface needs to be uploaded. This will upload the entire configuration from the L-Gate, including data points, dynamic NVs and schedules.

To Upload a Configuration

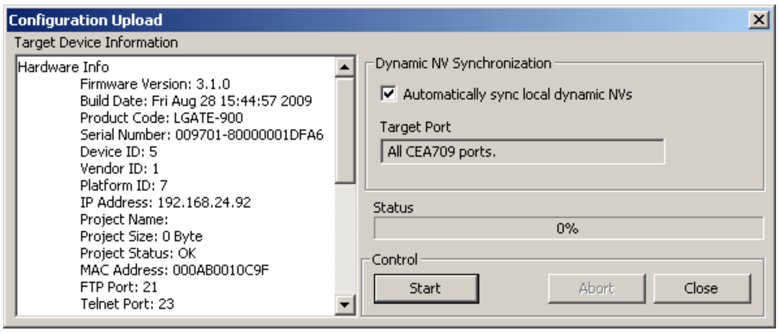
1. Click on the **Upload Configuration** button



in the tool bar. The configuration upload dialog opens up as shown in Figure 73.

2. If the check-box **Automatically sync local dynamic NVs** is marked, any manually created dynamic NVs will be uploaded and merged into the data point configuration.

3. Click on the button **Start** to start the transfer. This will upload the configuration of all ports, if the software is connected stand-alone via FTP or the network variable interface, for which the LNS plug-in was started for.



Configuration Upload

Target Device Information

Hardware Info
Firmware Version: 3.1.0
Build Date: Fri Aug 28 15:44:57 2009
Product Code: LGATE-900
Serial Number: 009701-80000001DFA6
Device ID: 5
Vendor ID: 1
Platform ID: 7
IP Address: 192.168.24.92
Project Name:
Project Size: 0 Byte
Project Status: OK
MAC Address: 000AB0010C9F
FTP Port: 21
Telnet Port: 23

Dynamic NV Synchronization
☑ Automatically sync local dynamic NVs
Target Port: All CEA709 ports.

Status: 0%

Figure 73: Configuration upload dialog.

4. When asked, if schedules shall be uploaded also, click **Yes**, if you want the current schedule configuration be extracted from the device. Note, that when doing so, the original schedules in the project are replaced by the uploaded schedules.

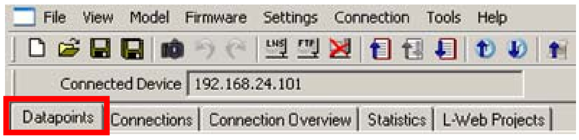
5. If dynamic NVs were synchronized, click on **Finish**.

6.7.4 Scanning for Network Variables

When the Configurator software is connected to an LNS database, network variables can be scanned in from that data base.

To scan network variables from the LNS database

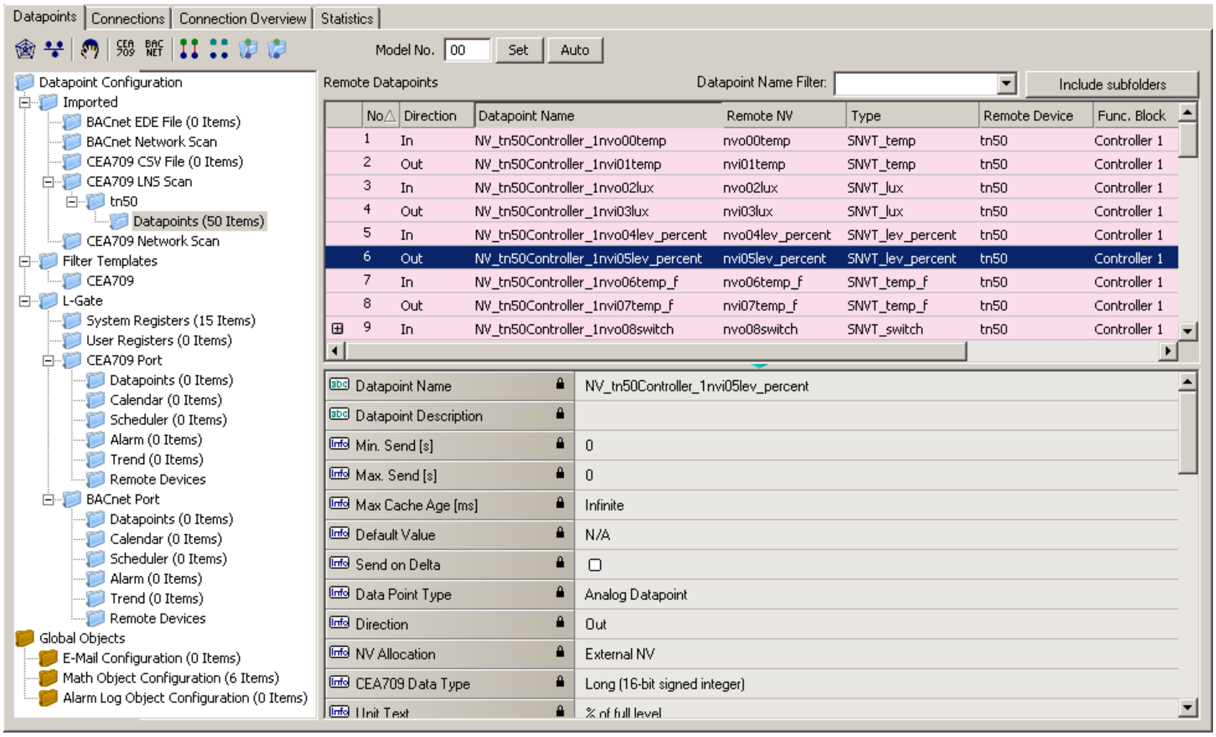
1. Click on the **Datapoints** tab.



Connected Device: 192.168.24.101

2. Click on the button **Scan channel**. This scans in all NVs on all devices connected to the CEA-709 channel of the device.

3. After the scan has completed, the folder **LNS Database Scan** is populated with the found NVs. Data point names for those NVs are automatically generated, following the data point naming rules defined in the project settings (see Section 6.3.2). By default the name is generated from node name, object name, and NV name. These names are ensured to be unique by adding a counter for multiple occurrences of the same name.



Model No. 00

Remote Datapoints

Datapoint Name Filter:

No	Direction	Datapoint Name	Remote NV	Type	Remote Device	Func. Block
1	In	NV_tn50Controller_1nvo00temp	nvo00temp	SNVT_temp	tn50	Controller 1
2	Out	NV_tn50Controller_1nvi01temp	nvi01temp	SNVT_temp	tn50	Controller 1
3	In	NV_tn50Controller_1nvo02lux	nvo02lux	SNVT_lux	tn50	Controller 1
4	Out	NV_tn50Controller_1nvi03lux	nvi03lux	SNVT_lux	tn50	Controller 1
5	In	NV_tn50Controller_1nvo04lev_percent	nvo04lev_percent	SNVT_lev_percent	tn50	Controller 1
6	Out	NV_tn50Controller_1nvi05lev_percent	nvi05lev_percent	SNVT_lev_percent	tn50	Controller 1
7	In	NV_tn50Controller_1nvo06temp_f	nvo06temp_f	SNVT_temp_f	tn50	Controller 1
8	Out	NV_tn50Controller_1nvi07temp_f	nvi07temp_f	SNVT_temp_f	tn50	Controller 1
9	In	NV_tn50Controller_1nvo08switch	nvo08switch	SNVT_switch	tn50	Controller 1

Datapoint Name	NV_tn50Controller_1nvi05lev_percent
Datapoint Description	
Min. Send [s]	0
Max. Send [s]	0
Max Cache Age [ms]	Infinite
Default Value	N/A
Send on Delta	□
Data Point Type	Analog Datapoint
Direction	Out
NV Allocation	External NV
CEA709 Data Type	Long (16-bit signed integer)
Unit Text	% of full level

Figure 74: Scanned NVs in the LNS Database Scan Folder

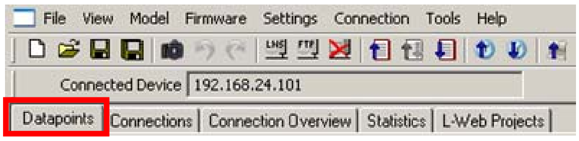
Figure 74 shows an example result of the database scan. The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

6.7.5 Importing Network Variables

Without LNS, the tool cannot connect to an LNS database, where it scans for network variables (NVs). Therefore, the list of NVs to be used on the L-Gate has to be available in a CSV file. This file can be produced by external software or created by hand. The CSV format for importing NVs is defined in 7.2.1.

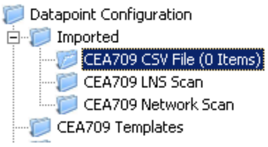
To Import NVs from a File

1. Click on the **Datapoints** tab.

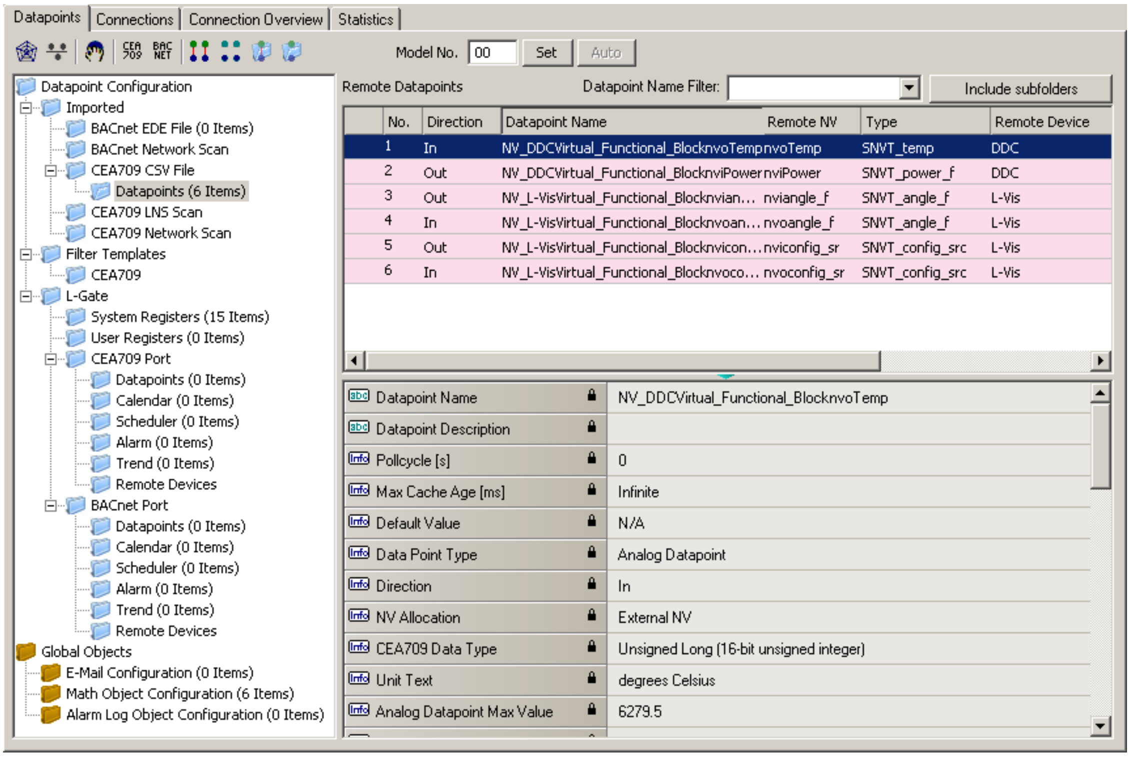


Connected Device 192.168.24.101

2. Select the folder **CEA709 CSV File**



3. Right-click and select **Import File**. In the following file selector dialog, choose the CSV import file and click **Ok**.



No.	Direction	Datapoint Name	Remote NV	Type	Remote Device
1	In	NV_DDCVirtual_Functional_BlocknvoTemp	nvoTemp	SNVT_temp	DDC
2	Out	NV_DDCVirtual_Functional_BlocknviPower	nviPower	SNVT_power_f	DDC
3	Out	NV_L-VisVirtual_Functional_Blocknvian…	nviangle_f	SNVT_angle_f	L-Vis
4	In	NV_L-VisVirtual_Functional_Blocknvoan…	nvoangle_f	SNVT_angle_f	L-Vis
5	Out	NV_L-VisVirtual_Functional_Blocknvicon…	nviconfig_sr	SNVT_config_src	L-Vis
6	In	NV_L-VisVirtual_Functional_Blocknvoco…	nvoconfig_sr	SNVT_config_src	L-Vis

Datapoint Name	NV_DDCVirtual_Functional_BlocknvoTemp
Datapoint Description	
Pollcycle [s]	0
Max Cache Age [ms]	Infinite
Default Value	N/A
Data Point Type	Analog Datapoint
Direction	In
NV Allocation	External NV
CEA709 Data Type	Unsigned Long (16-bit unsigned integer)
Unit Text	degrees Celsius
Analog Datapoint Max Value	6279.5

Figure 75: Imported NVs

4. Now the CSV File folder is populated with the imported NVs as shown in Figure 75.

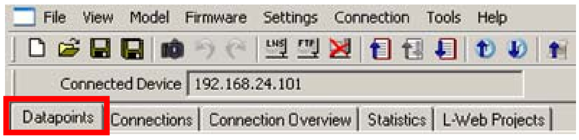
The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

6.7.6 Scanning NVs online from the Network

L-Gate devices also support an online network scan on the CEA-709 network. In this scan the device searches for other devices on the CEA-709 network and pulls in NV information of these devices. These NVs can then be used instead of importing them from a CSV file.

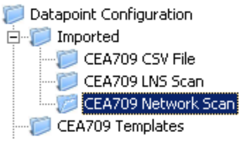
To scan NV online of the CEA-709 network

1. Click on the **Datapoints** tab.

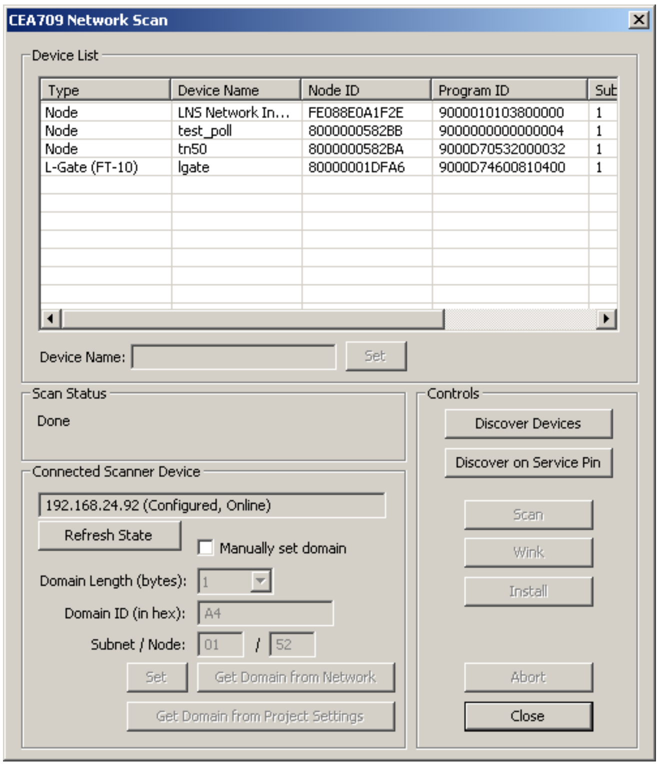


Connected Device 192.168.24.101

2. Select the folder **CEA709 Network Scan**.



3. Right-click on that folder and select **Scan CEA709/852 Network…**. This opens the CEA709/852 Network Scan dialog as shown in Figure 76.



Type	Device Name	Node ID	Program ID	Sub
Node	LNS Network In...	FE088E0A1F2E	9000010103800000	1
Node	test_poll	8000000582BB	9000000000000004	1
Node	tn50	8000000582BA	9000D70532000032	1
L-Gate (FT-10)	lgate	80000001DFA6	9000D74600810400	1

Device Name: Set

Scan Status: Done

192.168.24.92 (Configured, Online)

☐ Manually set domain

Domain Length (bytes): 1

Domain ID (in hex): A4

Subnet / Node: 01 / 52

Figure 76: CEA-709 network scan dialog.

4. If the device has not been installed with a network management tool (e.g. LNS-based tool), select the **Manually set domain** check-box and click the **Set** button. This sets the device configured, online to start the scan.

Note: *You need to set the same domain as the devices to be scanned. Click **Get Domain from Network** and press a service pin on some other, already installed device to retrieve the domain information before setting the device online.*

5. Click on the button **Discover Devices**. This starts a network scan. The results are put in the device list box.

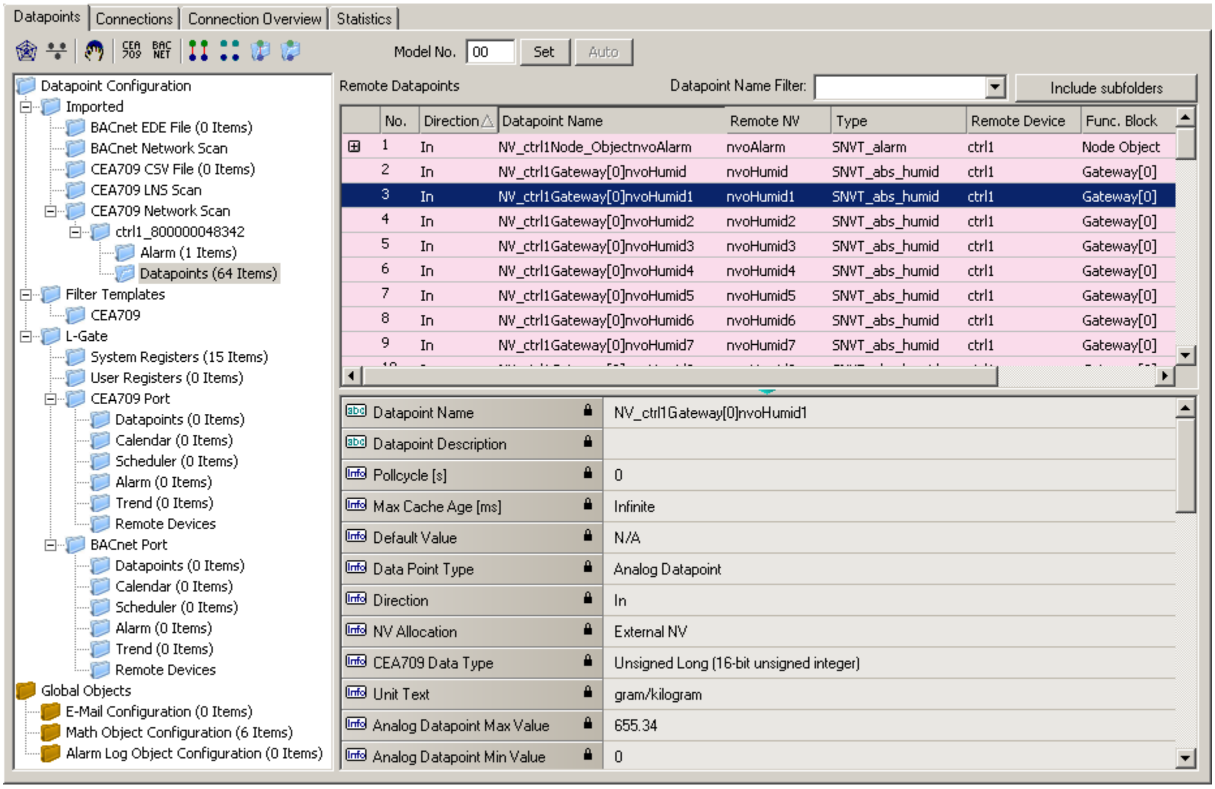
6. Alternatively, click the button **Discover on Service Pin**. Then press the service pin of a particular device on the network. This device will be added to the device list.

7. Select a device in the device list. To give the device a usable name, enter the name below and click on the **Set** button.

Device Name: ctrl1

8. Then click the button **Scan**. This scans the NVs on the selected device and adds them to the CEA709/852 Network Scan folder as a separate sub-folder for the device as shown in Figure 77.

Tip! *If you are not sure, which device you have selected, click on **Wink Device**. The selected device will execute its wink sequence.*



- Datapoint Configuration
  - Imported
    - BACnet EDE File (0 Items)
    - BACnet Network Scan
    - CEA709 CSV File (0 Items)
    - CEA709 LNS Scan
    - CEA709 Network Scan
      - ctrl1_800000048342
        - Alarm (1 Items)
        - Datapoints (64 Items)
  - Filter Templates
    - CEA709
  - L-Gate
    - System Registers (15 Items)
    - User Registers (0 Items)
    - CEA709 Port
      - Datapoints (0 Items)
      - Calendar (0 Items)
      - Scheduler (0 Items)
      - Alarm (0 Items)
      - Trend (0 Items)
      - Remote Devices
    - BACnet Port
      - Datapoints (0 Items)
      - Calendar (0 Items)
      - Scheduler (0 Items)
      - Alarm (0 Items)
      - Trend (0 Items)
      - Remote Devices
- Global Objects
  - E-Mail Configuration (0 Items)
  - Math Object Configuration (6 Items)
  - Alarm Log Object Configuration (0 Items)

	No.	Direction	Datapoint Name	Remote NV	Type	Remote Device	Func. Block
⊞	1	In	NV_ctrl1Node_ObjectnvoAlarm	nvoAlarm	SNVT_alarm	ctrl1	Node Object
	2	In	NV_ctrl1Gateway[0]nvoHumid	nvoHumid	SNVT_abs_humid	ctrl1	Gateway[0]
	3	In	NV_ctrl1Gateway[0]nvoHumid1	nvoHumid1	SNVT_abs_humid	ctrl1	Gateway[0]
	4	In	NV_ctrl1Gateway[0]nvoHumid2	nvoHumid2	SNVT_abs_humid	ctrl1	Gateway[0]
	5	In	NV_ctrl1Gateway[0]nvoHumid3	nvoHumid3	SNVT_abs_humid	ctrl1	Gateway[0]
	6	In	NV_ctrl1Gateway[0]nvoHumid4	nvoHumid4	SNVT_abs_humid	ctrl1	Gateway[0]
	7	In	NV_ctrl1Gateway[0]nvoHumid5	nvoHumid5	SNVT_abs_humid	ctrl1	Gateway[0]
	8	In	NV_ctrl1Gateway[0]nvoHumid6	nvoHumid6	SNVT_abs_humid	ctrl1	Gateway[0]
	9	In	NV_ctrl1Gateway[0]nvoHumid7	nvoHumid7	SNVT_abs_humid	ctrl1	Gateway[0]

Datapoint Name	NV_ctrl1Gateway[0]nvoHumid1
Datapoint Description	
Pollcycle [s]	0
Max Cache Age [ms]	Infinite
Default Value	N/A
Data Point Type	Analog Datapoint
Direction	In
NV Allocation	External NV
CEA709 Data Type	Unsigned Long (16-bit unsigned integer)
Unit Text	gram/kilogram
Analog Datapoint Max Value	655.34
Analog Datapoint Min Value	0

Figure 77: CEA-709 network scan results.

9. Click **Close** when all devices needed have been scanned.

6.7.7 Select and Use Network Variables

Data points in the **CEA709 LNS Scan** folder, the **CEA709 Network Scan** folder or in the **CEA709 CSV File** folder can be selected for use on the device. Select those NVs, which shall be exposed to BACnet objects.

To Use NVs on the Device

1. Go to any of the **CEA709 LNS Scan**, **CEA709 Network Scan** or the **CEA709 CSV File** folder.

2. Use the multi-select feature by holding the *Shift* or *Ctrl* keys pressed.

3. Click on the button **Use on Device** in the tool bar.

4. This creates data points in the L-Gate/CEA709 Port folder. All data points in that folder will actually be created on the L-Gate device after downloading the configuration.

Tip! *Data points can be edited by selecting a single point or using multi-select. The available properties to be edited are displayed in the property view below.*

6.7.8 Change the NV Allocation

After selecting the **Use on device** action on scanned or imported NVs they are assigned a default NV allocation in the L-Gate/CEA709 port folder. This default allocation can be changed, e.g., for imported NVs when they shall be allocated as static NVs on the L-Gate.

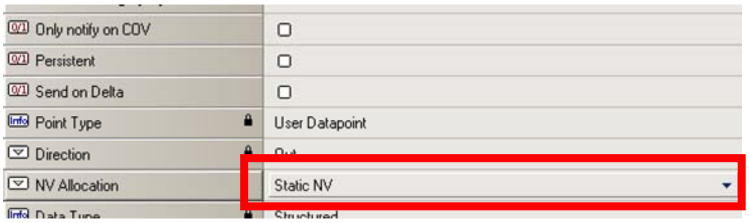
To Change the NV Allocation Type

1. In the data point view select the NVs in the L-Gate/CEA709 port folder, for which the NV allocation shall be changed.

Tip! *By using Ctrl-A all NVs can be selected.*

2. Select the **NV allocation** property as indicated by the red rectangle in Figure 78.

3. To make the data points static NVs on the L-Gate, select **Static NV**.



Only notify on COV	☐
Persistent	☐
Send on Delta	☐
Point Type	User Datapoint
Direction	Out
NV Allocation	Static NV
Data Type	Structured

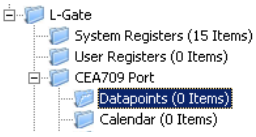
Figure 78: Change the NV allocation type.

6.7.9 Create Static NVs

The L-Gate can be configured to change its static interface and boot with a new one. Apart from creating static NVs from scanned or imported data points, static NVs can also be created manually in the L-Gate/CEA-709 folder.

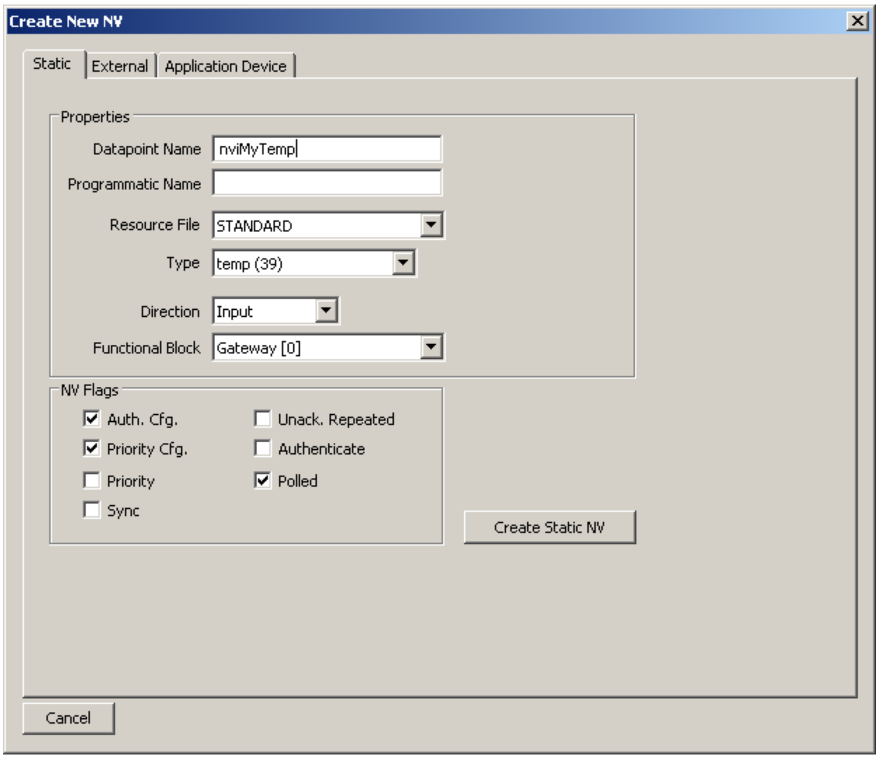
To Create Static NVs Manually

1. Select the L-Gate/CEA-709 Port/Datapoint folder



- L-Gate
  - System Registers (15 Items)
  - User Registers (0 Items)
  - CEA709 Port
    - Datapoints (0 Items)
    - Calendar (0 Items)

2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the NV creation dialog as shown in Figure 79.



Properties

Datapoint Name: nviMyTemp

Programmatic Name:

Resource File: STANDARD

Type: temp (39)

Direction: Input

Functional Block: Gateway [0]

NV Flags

☑ Auth. Cfg.
☑ Priority Cfg.
☐ Priority
☐ Sync
☐ Unack. Repeated
☐ Authenticate
☑ Polled

Figure 79: Create a static NV manually.

3. Enter a data point name and a programmatic name. The programmatic name is the name of the static NV, which is being created, while the data point name is used for exposing the NV as a BACnet object.

4. Select a resource file. To create a SNVT let the STANDARD resource file be selected.

5. Select a SNVT and a direction. If a non-standard resource file has been selected, choose from one of the UNVTs.

6. Choose a functional block where this static NV shall be located in.

7. Click **Create Static NV**. The static NV is created and appears in the data point list.

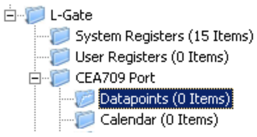
8. Note, that the static interface of the L-Gate will change as soon as static NVs are added or modified in the data point manager. This change is reflected in a new model number, which the L-Gate will have after the configuration download (see Section 5.5.2). Also note that the manually created static NVs are not bound automatically by the L-Gate Configurator. They simply appear on the device and need to be bound in the network management tool.

6.7.10 Create External NVs

External NVs are not actually allocated NVs on the L-Gate. Instead, the L-Gate uses polling to read data from and explicit updates to write data to external NVs. Since external NVs are not affecting the static NV interface of the L-Gate, they can be used to extend an L-Gate’s interface configuration at run-time, when no LNS with dynamic NVs is available.

To Create an external NV manually

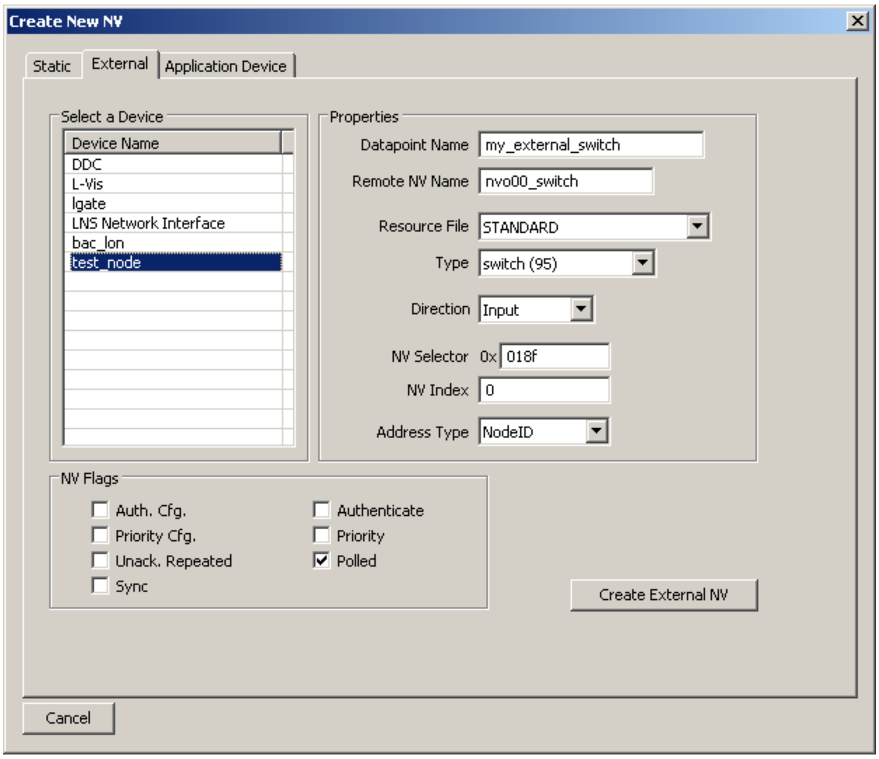
1. Select the L-Gate/CEA-709 Port/Datapoints folder



- L-Gate
  - System Registers (15 Items)
  - User Registers (0 Items)
  - CEA709 Port
    - Datapoints (0 Items)
    - Calendar (0 Items)

2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the NV creation dialog.

3. Click on the tab **External** as shown in Figure 80.



Select a Device

Device Name
DDC
L-Vis
lgate
LNS Network Interface
bac_lon
test_node

Properties

Datapoint Name: my_external_switch
Remote NV Name: nvo00_switch
Resource File: STANDARD
Type: switch (95)
Direction: Input
NV Selector: 0x 018f
NV Index: 0
Address Type: NodeID

NV Flags

☐ Auth. Cfg. ☐ Authenticate
☐ Priority Cfg. ☐ Priority
☐ Unack. Repeated ☑ Polled
☐ Sync

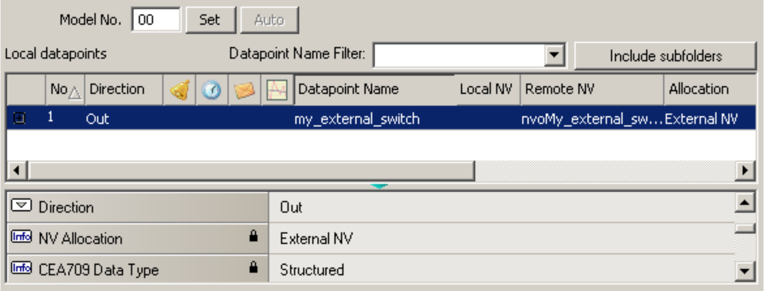
Figure 80: Create a new external NV.

4. Select the device in the box **Select a Device** on the left-hand side.

5. Enter the properties of the external NV on that device, starting with the local data point name, the remote programmatic NV name, the NV type (SNVT) and direction. Note, that the direction is the direction of the external NV on the L-Gate. Therefore, the remote output NV nvo00_switch becomes an input on the L-Gate. Also enter the NV selector in hexadecimal and the NV index in decimal. Choose the preferred addressing mode, e.g., Node ID.

6. Click **Create External NV** to add this NV to the data point list.

7. The external NV now appears in the data point list as shown in Figure 81. For external NVs which are inputs to the L-Gate, adapt the poll cycle property to your needs.



Model No. 00 Set Auto

Local datapoints Datapoint Name Filter: Include subfolders

No	Direction	Datapoint Name	Local NV	Remote NV	Allocation
1	Out	my_external_switch		nvoMy_external_sw...	External NV

Direction	Out
NV Allocation	External NV
CEA709 Data Type	Structured

Figure 81: Manually created external NV in the port interface definition.

6.7.11 Generate BACnet Objects

To actually create BACnet mappings from the used NVs on the L-Gate, use the data point manager tab. This section describes how to automatically generate BACnet objects from NVs. The auto-generation method also adds the NV and the BACnet object to a new connection.

To generate BACnet objects and connections from NVs on the L-Gate

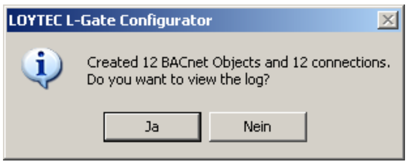
1. Go to the data point manager tab.

2. In the L-Gate/CEA-709 folder select all the NVs, which shall be mapped. The multi-select feature or <Ctrl-A> may be used for doing this.

3. Click on the speed button **Generate Points and auto-connect** in the tool bar.

4. Alternatively, you can select the L-Gate/CEA-709 Port folder and click the speed button **Folder-wide Generate points and auto-connect** in the tool bar. This generates BACnet objects and connections for all NVs in the folder.

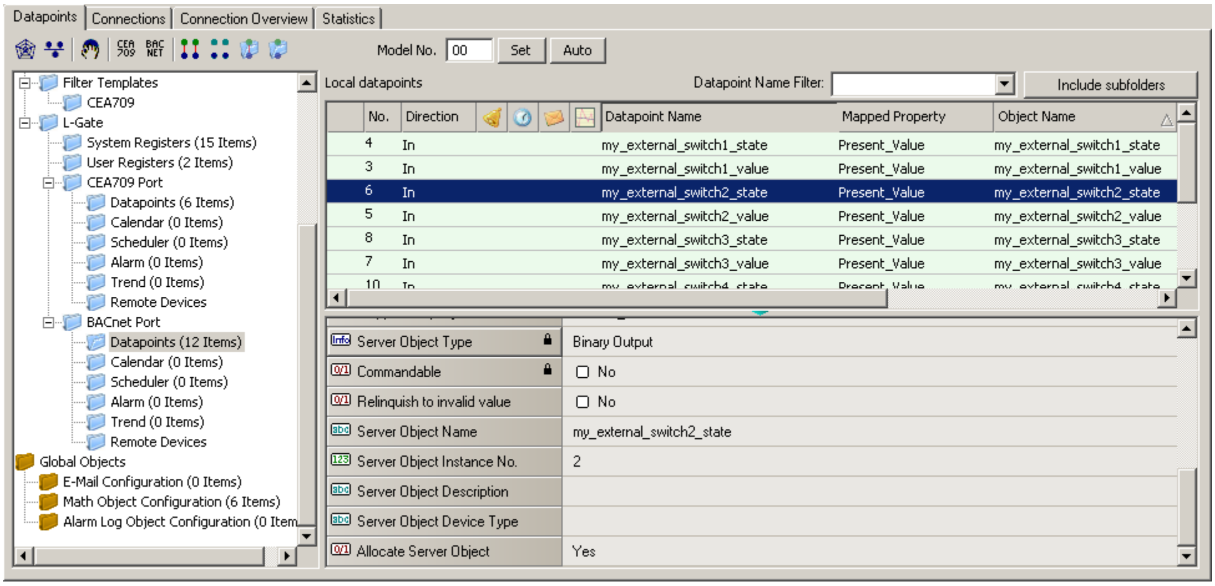
5. When the generation is complete, a dialog reports how many connections have been created. Click **No** to skip the report.



LOYTEC L-Gate Configurator

Created 12 BACnet Objects and 12 connections.
Do you want to view the log?

6. The generated BACnet objects appear in the L-Gate/BACnet Port/Datapoints folder as shown in Figure 82.



Model No. 00

Local datapoints

Datapoint Name Filter:

No.	Direction	Datapoint Name	Mapped Property	Object Name
4	In	my_external_switch1_state	Present_Value	my_external_switch1_state
3	In	my_external_switch1_value	Present_Value	my_external_switch1_value
6	In	my_external_switch2_state	Present_Value	my_external_switch2_state
5	In	my_external_switch2_value	Present_Value	my_external_switch2_value
8	In	my_external_switch3_state	Present_Value	my_external_switch3_state
7	In	my_external_switch3_value	Present_Value	my_external_switch3_value
10	In	my_external_switch4_state	Present_Value	my_external_switch4_state

Server Object Type	Binary Output
Commandable	□ No
Relinquish to invalid value	□ No
Server Object Name	my_external_switch2_state
Server Object Instance No.	2
Server Object Description	
Server Object Device Type	
Allocate Server Object	Yes

Figure 82: Auto-created BACnet Points in the BACnet Folder

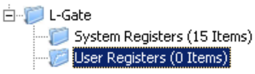
Note, when auto-creating the BACnet objects, the L-Gate Configurator initializes the BACnet properties with default values derived from the properties of the CEA-709 NVs. In particular, the object name, description, minimum and maximum present value, and engineering units are generated. If the default properties do not have the desired values, the user can edit them in the BACnet folder.

6.7.12 Create User Registers

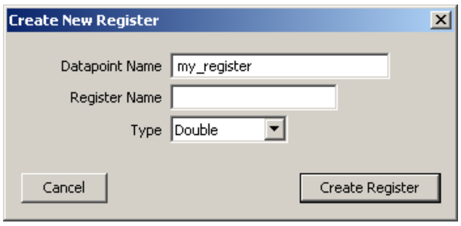
User registers are data points on the device that do not have a representation on the network. Thus, they are not accessible over a specific technology. A register merely serves as a container for intermediate data (e.g., results of math objects). Since a register has no network direction, it can be written and read. Therefore, two data points are generated for each register, one for writing the register (output) and one for reading the register (input).

To Create a User Register

1. Select the L-Gate/User Registers folder



2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the register creation dialog as shown in Figure 83.



Datapoint Name my_register

Register Name

Type Double

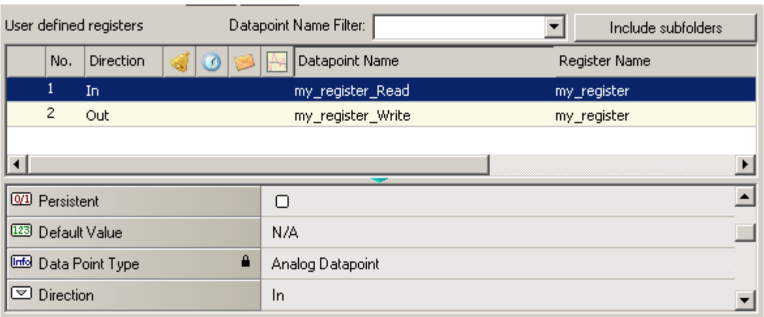
Figure 83: Create a user register.

3. Enter a **Datapoint Name** for the register. You may leave the **Register Name** blank to give the underlying register the same name as the data point.

4. Select a **Type**. Available are “Double”, “Boolean”, or “Signed Integer”.

5. Click **Create Register**.

6. Two data points now appear for the register, one for writing the register and one for reading the register as shown in Figure 84.



User defined registers

Datapoint Name Filter:

No.	Direction	Datapoint Name	Register Name
1	In	my_register_Read	my_register
2	Out	my_register_Write	my_register

Persistent	□
Default Value	N/A
Data Point Type	Analog Datapoint
Direction	In

Figure 84: Manually created user register.

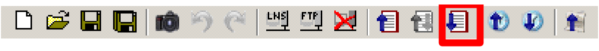
6.7.13 Configuration Download

After the data points have been configured, the configuration needs to be downloaded to the L-Gate. For doing so, the L-Gate must be online. If the L-Gate is not yet connected to the network, the configuration can be saved to a project file on the local hard drive.

If connected via LNS, and the NVs on the L-Gate are “Static NV” or “Dynamic NV”, the Late Configurator can create the bindings automatically. This behavior can be influenced by the download dialog. When connected via LNS, the download procedure also manages the device template upgrade in the LNS database, if the static NV interface has been changed.

To Download a Configuration

1. Click on the **Download Configuration** button



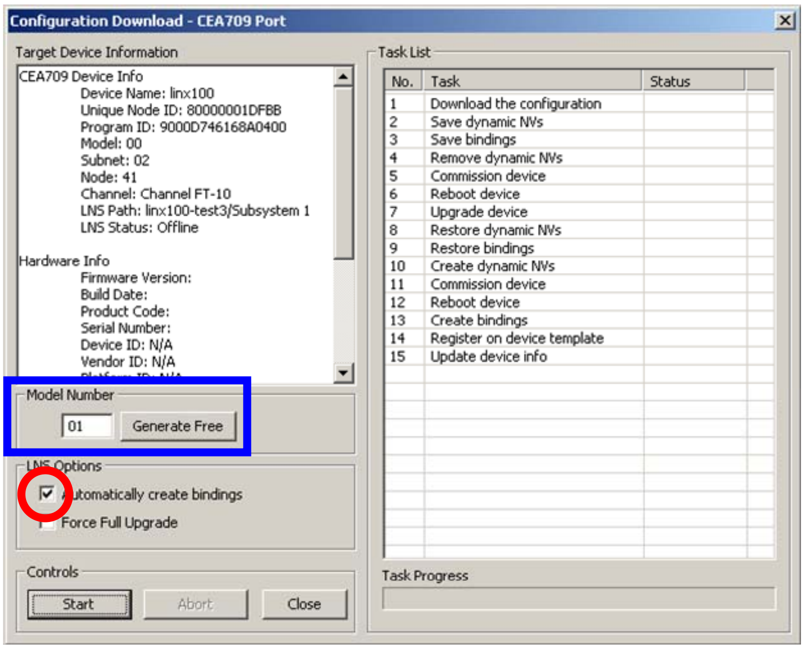
in the tool bar. The configuration upload dialog opens up as shown in Figure 85.

2. If no bindings shall be generated, deselect the **Automatically create bindings** checkbox indicated by the red circle in Figure 85.

3. If the static NV interface has been changed, a new model number for the L-Gate needs to be selected. This is necessary, as the static network interface of the L-Gate changes on the CEA-709 network. The L-Gateway configuration software automatically selects a usable value, which can be overridden in the field **Model Number** marked by the blue rectangle in Figure 85.

4. Click **Start** to start the download. Each of the actions is displayed in the **Task List** section of the dialog. The current progress is indicated by the progress bar below.

5. When the download process has finished, a notification window appears, which has to be acknowledged by clicking Ok.



Configuration Download - CEA709 Port

Target Device Information

CEA709 Device Info
Device Name: linx100
Unique Node ID: 80000001DFBB
Program ID: 9000D746168A0400
Model: 00
Subnet: 02
Node: 41
Channel: Channel FT-10
LNS Path: linx100-test3/Subsystem 1
LNS Status: Offline

Hardware Info
Firmware Version:
Build Date:
Product Code:
Serial Number:
Device ID: N/A
Vendor ID: N/A

Model Number: 01 Generate Free

LNS Options
☑ Automatically create bindings
□ Force Full Upgrade

Controls: Start Abort Close

Task List

No.	Task	Status
1	Download the configuration	
2	Save dynamic NVs	
3	Save bindings	
4	Remove dynamic NVs	
5	Commission device	
6	Reboot device	
7	Upgrade device	
8	Restore dynamic NVs	
9	Restore bindings	
10	Create dynamic NVs	
11	Commission device	
12	Reboot device	
13	Create bindings	
14	Register on device template	
15	Update device info	

Task Progress

Figure 85: Configuration Download Dialog

Note, that after the download is complete, the interface changes become active on the L-Gate (i.e., the static NV interface has changed). Refresh the network management tool to synchronize the tool with the changes to the LNS database made by the L-Gate Configurator (e.g., use the menu "LonMaker|Refresh" in LonMaker or hit *F5* in NL-220).

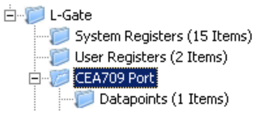
Normally, the Configurator software optimizes the download process by not executing certain LNS operations, if not necessary. For example, only those bindings and dynamic NVs are deleted and re-created, which correspond to real changes in the interface. The user can check the **Force Full Upgrade** option to clean and re-do all steps.

6.7.14 Build XIF for Port Interface

When using static NVs on the L-Gate, the L-Gateway configuration software can export a new XIF file for the changed static interface.

To Create a XIF File

1. Select the **CEA-709 Port** folder



L-Gate
System Registers (15 Items)
User Registers (2 Items)
CEA709 Port
Datapoints (1 Items)

2. Right-click on that folder and in the context menu select **Build XIF …**.

3. This opens a file requestor where the XIF file name needs to be entered. Select a useful name to identify the L-Gate, e.g. as "lgate1.xif".

6.7.15 Enable Legacy NM Mode

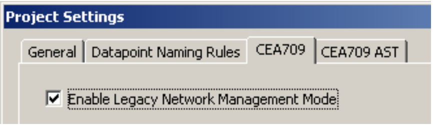
For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured. Please contact the tool's vendor for information whether ECS is supported or not. Note, that changing to legacy network management mode changes the static interface of the device.

To Enable Legacy NM Mode

1. In the L-Gate Configurator menu go to **Settings → Project settings …**

2. Click on the tab **CEA709**.

3. Put a check mark in **Enable Legacy Network Management Mode**.



☑ Enable Legacy Network Management Mode

4. Click **OK.**

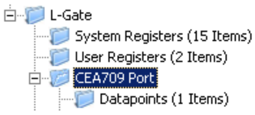
5. Download the configuration to activate the change.

6.7.16 Upload Dynamic NVs from Device

In LNS-based tools it is possible to create dynamic NVs on the device manually. This is a possible workflow to engineer the NV interface of the device in the LNS database. To use those manually created dynamic NVs, the L-Gateway configuration software must synchronize its dynamic NV information with the port.

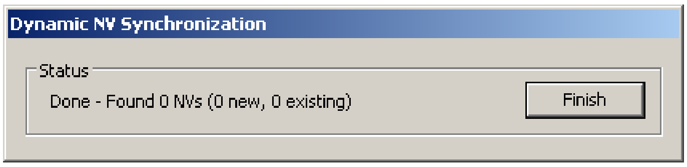
To Upload Dynamic NVs

1. Select **the CEA-709 Port** folder.



```
⊟ L-Gate
   System Registers (15 Items)
   User Registers (2 Items)
 ⊟ CEA709 Port
     Datapoints (1 Items)
```

2. Right-click and select **Sync Dynamic NVs** in the context menu. The L-Gateway configuration software then loads any new dynamic NVs, which have been created and are not yet part of the port interface definition. The process completes when the dialog shown in Figure 86 appears.



Done - Found 0 NVs (0 new, 0 existing)

Figure 86: Synchronizing dynamic NVs from the device.

3. Click on **Finish**. The new dynamic NVs now appear in the data point list and can be edited and used for creating BACnet objects and connections.

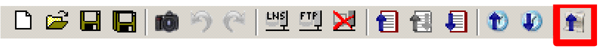
6.7.17 Upload the System Log

The system log on the device contains important log messages. Log messages are generated for important operational states (e.g., last boot time, last shutdown reason) or errors at run-time. This file is important for trouble-shooting and is available on the Web UI (see Section 4.3.1). The file can also be uploaded from the device with the L-Gate Configurator.

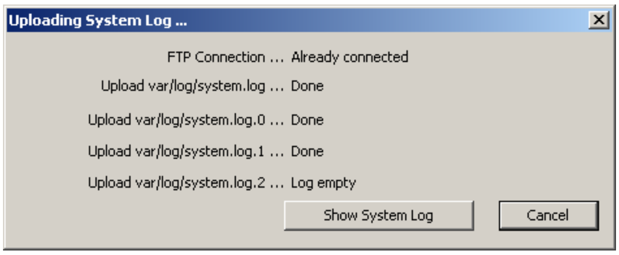
To Upload the System Log

1. Connect to the device via the FTP or LNS method (see Section 6.7.2).

2. Click on the **Upload system log** button



in the tool bar. The upload system log dialog as shown in Figure 87 opens showing the upload progress.



Uploading System Log ...

FTP Connection ... Already connected

Upload var/log/system.log ... Done

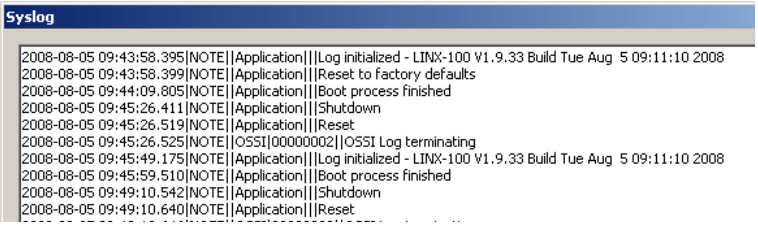
Upload var/log/system.log.0 ... Done

Upload var/log/system.log.1 ... Done

Upload var/log/system.log.2 ... Log empty

Figure 87: Upload system log dialog.

3. When the upload is finished, click on **Show System Log**. The system log window appears as shown in Figure 88.



Syslog

```
2008-08-05 09:43:58.395|NOTE||Application|||Log initialized - LINX-100 V1.9.33 Build Tue Aug  5 09:11:10 2008
2008-08-05 09:43:58.399|NOTE||Application|||Reset to factory defaults
2008-08-05 09:44:09.805|NOTE||Application|||Boot process finished
2008-08-05 09:45:26.411|NOTE||Application|||Shutdown
2008-08-05 09:45:26.519|NOTE||Application|||Reset
2008-08-05 09:45:26.525|NOTE||OSSI|00000002||OSSI Log terminating
2008-08-05 09:45:49.175|NOTE||Application|||Log initialized - LINX-100 V1.9.33 Build Tue Aug  5 09:11:10 2008
2008-08-05 09:45:59.510|NOTE||Application|||Boot process finished
2008-08-05 09:49:10.542|NOTE||Application|||Shutdown
2008-08-05 09:49:10.640|NOTE||Application|||Reset
```

Figure 88: System log window.

4. Click on **Save** to store the system log into a file on your local hard drive.

6.8 Advanced CEA-709 Configuration

6.8.1 Working with Configuration Properties

Configuration properties (CPs) are supported by the LNS network scan and the online network scan. They can be selected and used on the device in a similar way as NVs. There is a notable difference to NVs: CPs are part of files on the remote nodes. Reading and writing CPs on the L-Gate results in a file transfer.

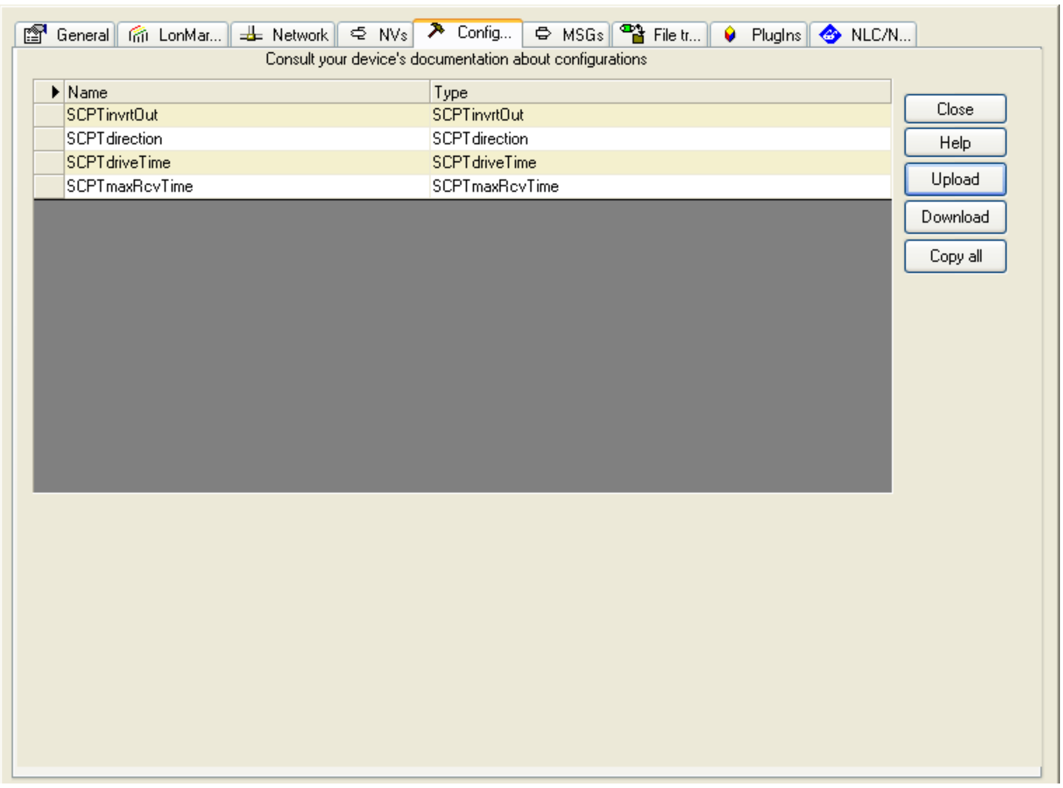
The L-Gate supports both, the LONMARK file transfer and the simpler direct memory read/write method. In both cases, however, one has to keep in mind that a file transfer incurs more overhead than a simple NV read/write. Therefore, polling CPs should be done at a much slower rate than polling NVs.

Another aspect is how CPs are handled by network management tools. Formerly, those tools were the only instance that could modify CPs in devices. Therefore, most tools do not automatically read back CPs from the devices when browsing them. This can result in inconsistencies between the actual CP contents on the device and their copy in the network management tool. It is recommended to synchronize the CPs from the device into the LNS database before editing and writing them back.

To Synchronize CPs in NL220

1. Double-click on the device object in the device tree.

2. Press the **Upload** button on the Configuration tab of the device properties (see Figure 89).



Consult your device's documentation about configurations

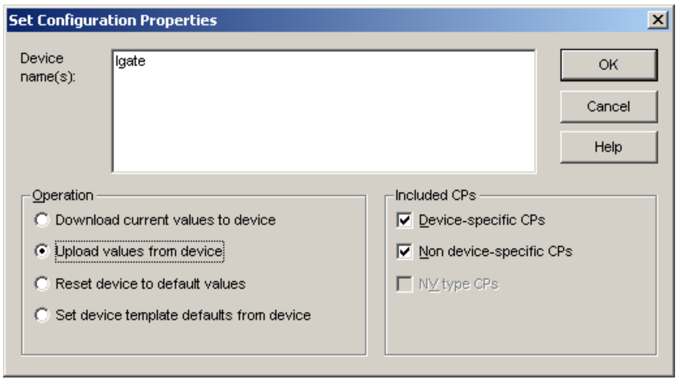
Name	Type
SCPTinvrtOut	SCPTinvrtOut
SCPTdirection	SCPTdirection
SCPTdriveTime	SCPTdriveTime
SCPTmaxRcvTime	SCPTmaxRcvTime

Figure 89: Configuration Tab for Configuration Properties in NL220.

To Synchronize CPs in LonMaker TE

1. Right-click on a device object and select **Commissioning → Resync CPs…** from the context menu.

2. This opens the dialog shown in Figure 90.



Device name(s): lgate

Operation
○ Download current values to device
● Upload values from device
○ Reset device to default values
○ Set device template defaults from device

Included CPs
☑ Device-specific CPs
☑ Non device-specific CPs
☐ NV type CPs

Figure 90: Set Configuration Properties in LonMaker TE.

3. In this dialog select the radio button **Upload values from device** in the **Operation** group box. To use the current settings of the device as default values for new devices, select **Set device template defaults from device**.

4. Execute the operation by clicking the **OK** button.

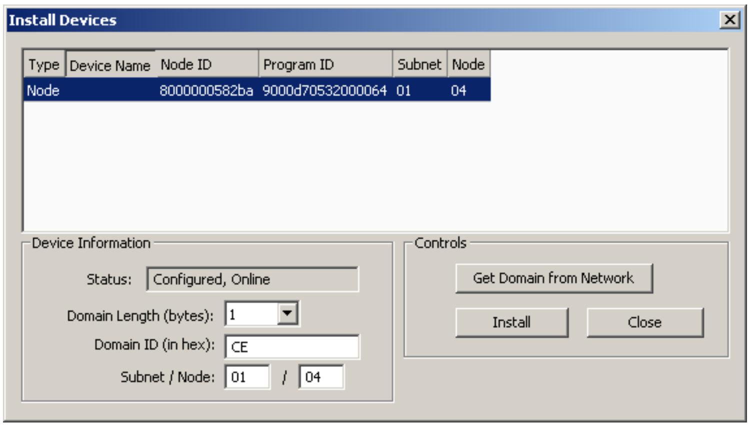
6.8.2 Install Unconfigured Devices

CEA-709 devices must be installed by a network management tool (e.g., LNS-based tool) to be available for communication. To install a device, its domain information must be written and the device must be set configured, online. If no network management tool is available, the CEA-709 network scan can be used to install a small number of unconfigured devices.

To Install Devices

1. Open the CEA-709 network scan dialog and scan for devices as described in Section 6.7.6.

2. Click the **Install** button. This opens the **Install Devices** dialog as shown in Figure 91.



Type	Device Name	Node ID	Program ID	Subnet	Node
Node		8000000582ba	9000d70532000064	01	04

Device Information

Status: Configured, Online

Domain Length (bytes): 1

Domain ID (in hex): CE

Subnet / Node: 01 / 04

Figure 91: Install devices dialog.

3. Select the device to be installed.

4. Enter the domain information or click **Get Domain from Network** and press a service pin.

5. Enter a subnet and node address and click **Install**.

6. Repeat this step for other unconfigured devices on the network.

6.8.3 Using Feedback Data Points

Feedback data points allow reading back the value written out over an output data point. In LONMARK systems getting a feedback value is normally accomplished by creating a dedicated feedback NV on the device, which can be bound back to the devices that are interested in the currently active value on an output.

Some nodes, however, do not possess such feedback NVs for certain functions. To support getting feedback values on such nodes, the Configurator can create feedback data points based on existing output data points. This is especially interesting for bound output NVs (static and dynamic alike). The corresponding feedback data point is an input, which uses the original output NV for polling the target NV. Once the binding is changed the new target is polled. No additional input NV needs to be created for the feedback value, if the feedback data point feature is used.

To Create a Feedback Data Point

1. Select an output data point in the data point list of the CEA-709 port folder, e.g. ‘nvoHumid101’.

2. Right-click and choose Create Feedback-Point from the context menu.

3. A new input data point is created, having '_fb' appended to the original name, e.g., 'nvoHumid101_fb'. Note, that the feedback data point maps to the same NV index as the original output data point.

4. Choose an appropriate poll cycle in the data point properties for the feedback data point.

6.8.4 Working with UNVTs, UCPTs

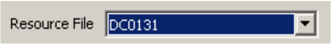
This device supports user-defined type, including user-defined network variable types (UNVTs) and user-defined configuration property types (UCPTs). In order to interpret the contents of user-defined types, the *device resource files* supplied by the vendor must be added to the resource catalog on your PC.

Once the resource files are installed, the CEA-709 network scan and the LNS scan will display the user-defined types from the resource files. Those data points can be used on the device like regular, standard-type data points. Also manual creation of UNVTs can be performed.

To Manually Create a Static UNVT

1. Perform the steps to manually create a static NV as described in Section 6.7.9.

2. When the **Create New NV** dialog appears, change the resource file from 'STANDARD' in the **Resource File** drop-down box to the desired, user-defined resource file


Resource File DC0131

3. Then select the desired UNVT from the **Type** drop-down list below. This list will display the types of the selected resource file only.

4. Click **Create Static NV** to create the UNVT on the device.

6.9 Connections

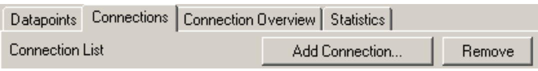
6.9.1 Create a New Connection

After having configured the device's network ports with data points, internal connections between those data points can be created. Usually, the manual method to create a connection is used to create n-way connections or connections for data points, where the generate-and-auto-connect method cannot be applied.

A connection is an internal mapping in the device between input and output data points. A connection always consists of *one* hub data point and *one or multiple* target data points. Hub data points can be input or output. If the hub data point is an input, then the target data points must be output and vice versa. All data points in the connection must be of a compatible type.

To manually create a new connection

1. Click on the **Connections** tab



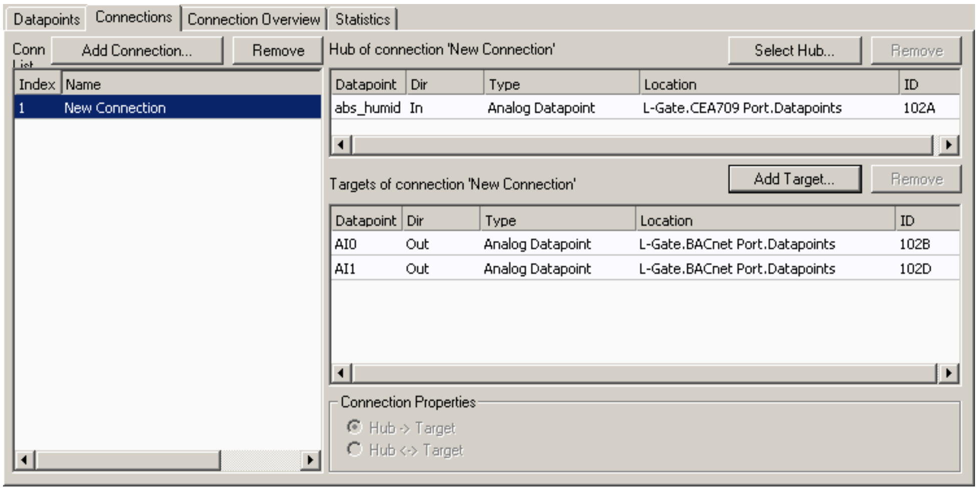
in the tool bar of the main connections window and press **Add Connection…**. A new connection is added to the connection list. Rename the connection if you want to do so.

2. Click on **Select Hub…** to select the hub point. This opens a list of all available data points. Select one and press **OK**.

3. Then click on **Add Target…** Similar to 2) select all target data points. You may use multi-select to select more than one data point at a time.

Note: *By default only compatible data points are displayed. Sometimes compatible data points are available as member points (e.g., a SNVT structure member). Click on* ⊞ *to expand the data point and select the desired member point.*

4. Now the connection display contains a hub and two target data point as shown in Figure 92.



Index	Name
1	New Connection

Hub of connection 'New Connection'

Datapoint	Dir	Type	Location	ID
abs_humid	In	Analog Datapoint	L-Gate.CEA709 Port.Datapoints	102A

Targets of connection 'New Connection'

Datapoint	Dir	Type	Location	ID
AI0	Out	Analog Datapoint	L-Gate.BACnet Port.Datapoints	102B
AI1	Out	Analog Datapoint	L-Gate.BACnet Port.Datapoints	102D

Figure 92: Connection dialog with hub and target points.

6.9.2 Create Connections from a CSV File

A quick way to perform batch edit on connections is to export and import connections from the connections CSV file. Each line in the connections CSV file identifies a connection. The first column is the connection name. The second column specifies the hub data point. The full path to the data point must be specified using the dot '.' as the folder separator. The third and following columns specify the target data points.

To Create Connection from a CSV File

1. Select the menu **Tools → Export Connections …**

2. Select an appropriate file name and export.

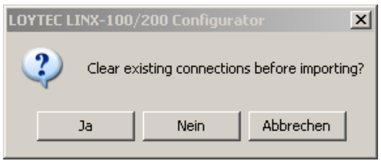
3. Edit the connections CSV file. An example is shown in Figure 93.

```
#connection_csv_ver,1
#ConnectionName,HubDPName,TargetDPName
nvoAbs_humid1,L-Gate.CEA709 Port.abs_humid1,L-Gate.BACnet Port.AO101
nvoAbs_humid2,L-Gate.CEA709 Port.abs_humid2,L-Gate.BACnet Port.AO102
nvoAbs_humid3,L-Gate.CEA709 Port.abs_humid3,L-Gate.BACnet Port.AO103
nvoAbs_humid4,L-Gate.CEA709 Port.abs_humid4,L-Gate.BACnet Port.AO104
```

Figure 93: Example Connection CSV File.

4. Select the menu **Tools → Import Connections …**

5. If connections that are not part of the connection CSV file shall be deleted, click **Yes** when prompted. Click **No** if the other connections shall be left as is.



LOYTEC LINX-100/200 Configurator

Clear existing connections before importing?

6. Choose the file to import and click **Ok**.

7. When the import has completed, optionally view the log to check, which connections have been added, modified, and deleted.

6.9.3 Modify Connections

Connections can be edited and deleted. This is also done in the **Connections** tab of the main window. Editing connections does not influence the data point configuration. This means, when deleting a connection or adding/removing data points to/from a connection, the data points are not deleted.

To Edit a Connection

1. Change to the **Connections** tab of the main window.

2. Select the connection to edit. Then follow the steps as applied when creating a connection.

3. To delete a target, select the target and click on **Remove Target(s)**.

To Delete a Connection

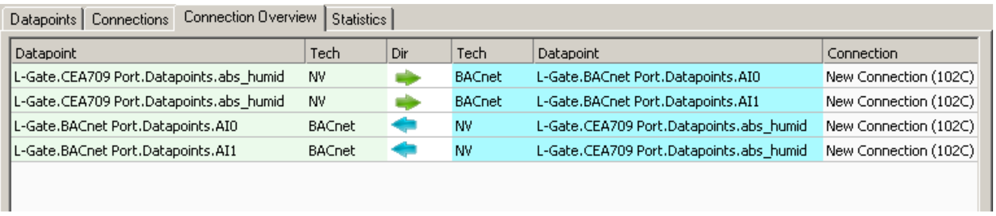
1. Change to the **Connections** tab of the main window.

2. Select the connection for removal. Use multi-select to select more than one connection.

3. Click **Remove**.

6.9.4 Connection Overview

Select the **Connection Summary** tab to get a graphical representation of all connections. It represents the two connected data points, their technology they are based on and the direction of the connection. An example for the overview is shown in Figure 94.



Datapoint	Tech	Dir	Tech	Datapoint	Connection
L-Gate.CEA709 Port.Datapoints.abs_humid	NV	→	BACnet	L-Gate.BACnet Port.Datapoints.AI0	New Connection (102C)
L-Gate.CEA709 Port.Datapoints.abs_humid	NV	→	BACnet	L-Gate.BACnet Port.Datapoints.AI1	New Connection (102C)
L-Gate.BACnet Port.Datapoints.AI0	BACnet	←	NV	L-Gate.CEA709 Port.Datapoints.abs_humid	New Connection (102C)
L-Gate.BACnet Port.Datapoints.AI1	BACnet	←	NV	L-Gate.CEA709 Port.Datapoints.abs_humid	New Connection (102C)

Figure 94: Connections Summary.

6.10 BACnet Configuration

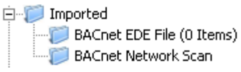
6.10.1 Scan for BACnet Objects

LOYTEC devices also support an online network scan on the BACnet network. In this scan the device searches for other devices on the BACnet network and pulls in the BACnet object information of these devices. These BACnet objects can then be used on the device as the basis for client mapping.

To Scan for BACnet Objects

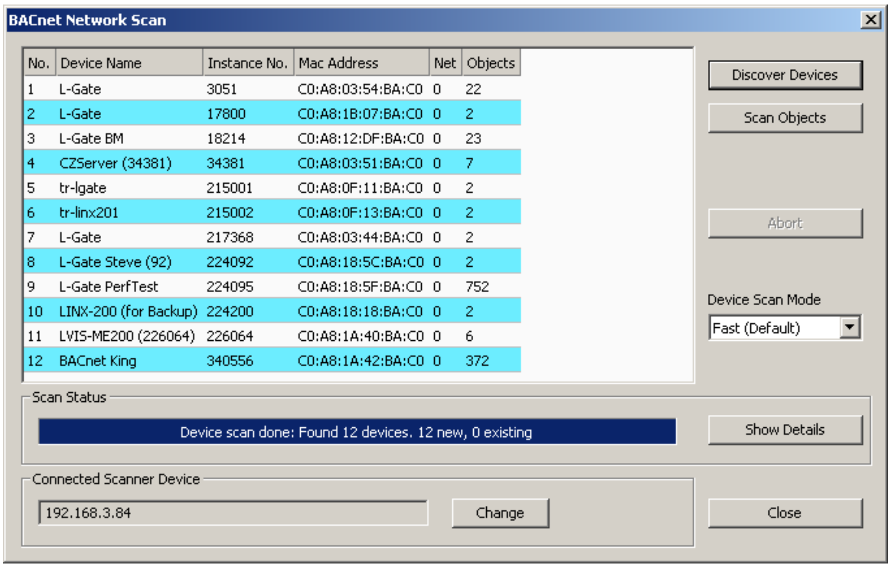
1. Go to the **Datapoints** tab.

2. Select the folder **BACnet Network Scan**



Imported
- BACnet EDE File (0 Items)
- BACnet Network Scan

3. Right-click on that folder and select **Scan BACnet Network…**. This opens the BACnet Network Scan dialog as shown in Figure 95.



BACnet Network Scan

No.	Device Name	Instance No.	Mac Address	Net	Objects
1	L-Gate	3051	C0:A8:03:54:BA:C0	0	22
2	L-Gate	17800	C0:A8:1B:07:BA:C0	0	2
3	L-Gate BM	18214	C0:A8:12:DF:BA:C0	0	23
4	CZServer (34381)	34381	C0:A8:03:51:BA:C0	0	7
5	tr-lgate	215001	C0:A8:0F:11:BA:C0	0	2
6	tr-linx201	215002	C0:A8:0F:13:BA:C0	0	2
7	L-Gate	217368	C0:A8:03:44:BA:C0	0	2
8	L-Gate Steve (92)	224092	C0:A8:18:5C:BA:C0	0	2
9	L-Gate PerfTest	224095	C0:A8:18:5F:BA:C0	0	752
10	LINX-200 (for Backup)	224200	C0:A8:18:18:BA:C0	0	2
11	LVIS-ME200 (226064)	226064	C0:A8:1A:40:BA:C0	0	6
12	BACnet King	340556	C0:A8:1A:42:BA:C0	0	372

Device Scan Mode: Fast (Default)

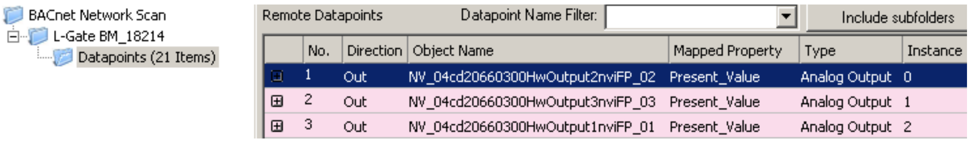
Scan Status: Device scan done: Found 12 devices. 12 new, 0 existing

Connected Scanner Device: 192.168.3.84

Figure 95: BACnet network scan dialog.

4. Click on the button **Discover Devices**. This starts a network scan. The results are put in the device list box. A progress bar below indicates how many devices are being scanned.

5. Select a device in the device list and click the button **Scan Objects**. This scans the BACnet objects on the selected device and adds them to the **BACnet Network Scan** folder as a separate sub-folder for the device as shown in Figure 96.



- BACnet Network Scan
  - L-Gate BM_18214
    - Datapoints (21 Items)

Remote Datapoints   Datapoint Name Filter: Include subfolders

	No.	Direction	Object Name	Mapped Property	Type	Instance
⊟	1	Out	NV_04cd20660300HwOutput2nviFP_02	Present_Value	Analog Output	0
⊞	2	Out	NV_04cd20660300HwOutput3nviFP_03	Present_Value	Analog Output	1
⊞	3	Out	NV_04cd20660300HwOutput1nviFP_01	Present_Value	Analog Output	2

Figure 96: BACnet network scan results.

6. Click **Close** when all devices needed have been scanned.

6.10.2 Import from EDE File

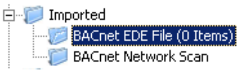
If the device is engineered offline or some of the required BACnet devices are not yet online in the network, the engineering process can be done by importing a device and object list from a set of EDE files. These objects also appear in the import folder and can be later used on the device.

There are a set of EDE files. Select the main EDE file, e.g. *device.csv*. The EDE import will also search for the other components, which must be named *device-states.csv*. Which components are expected, please refer to Section 7.3.3. Example EDE files can be found in the 'examples' directory of the LOYTEC Gateway Configuration software installation directory.

To Import BACnet Objects from an EDE File

1. Go to the **Datapoints** tab.

2. Select the folder **BACnet EDE File**



- Imported
  - BACnet EDE File (0 Items)
  - BACnet Network Scan

3. Right-click and select **Import File**. In the following file selector dialog, choose the EDE import file and click **Ok**.

4. Now the **BACnet EDE File** folder is populated with the imported BACnet objects.

6.10.3 Use Imported BACnet Objects

After BACnet objects have been imported (with a network scan or by importing from an EDE file) the user can select the BACnet objects that the L-Gate shall access. When executing the **Use on device** the configuration software allocates client mappings on the device. These client mappings will read or write values from the BACnet objects in the network.

In an additional step, there can be also server objects allocated on the device. These server objects can be created automatically from converting a client mapping to a server object. This is usually done, if the imported BACnet objects shall also be directly modified over the BACnet network on the device itself.

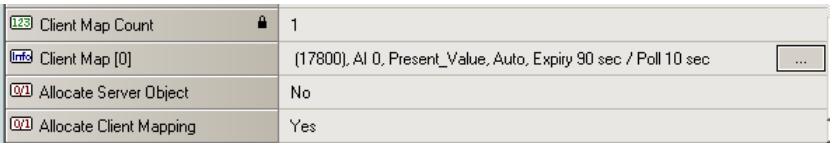
To Use Imported BACnet Objects on the Device

1. Go to the **Datapoints** tab and select the desired BACnet objects in one of the import folders.

2. Use the multi-select feature by holding the *Shift* or *Ctrl* keys pressed.

3. Click on the button **Use on Device** in the tool bar.

4. This creates data points in the BACnet Port/Datapoints folder. All data points in that folder will be created as client mappings. No server object is created automatically in this case.



Client Map Count	1
Client Map [0]	(17800), AI 0, Present_Value, Auto, Expiry 90 sec / Poll 10 sec ...
Allocate Server Object	No
Allocate Client Mapping	Yes

5. To also create server objects select the data points in question using the multi-select feature. Then edit the property Allocate Server Object and set it to Yes.

Allocate Server Object	Yes

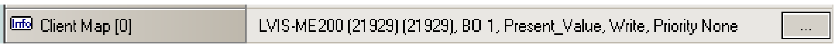
6.10.4 Edit a Client Mapping

The client mapping information in BACnet data points can be edited after they have been created. Usually, this is done to correct the remote BACnet object instance number.

To Edit a Client Mapping

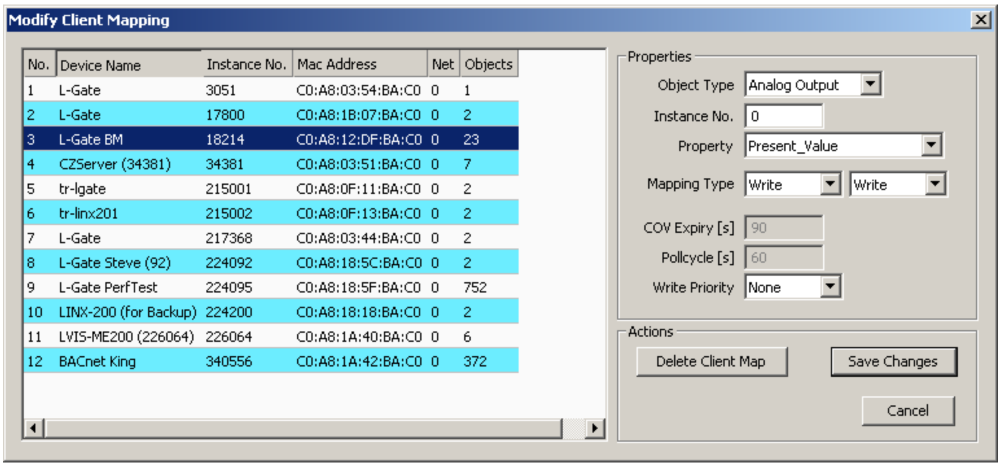
1. Select the BACnet data point that has the client mapping to be edited.

2. On the **Client Map** property click the **…** button



Client Map [0]	LVIS-ME200 (21929) (21929), BO 1, Present_Value, Write, Priority None ...

3. This opens the **Modify Client Mapping** dialog as shown in Figure 97.



Modify Client Mapping

No.	Device Name	Instance No.	Mac Address	Net	Objects
1	L-Gate	3051	C0:A8:03:54:BA:C0	0	1
2	L-Gate	17800	C0:A8:1B:07:BA:C0	0	2
3	L-Gate BM	18214	C0:A8:12:DF:BA:C0	0	23
4	CZServer (34381)	34381	C0:A8:03:51:BA:C0	0	7
5	tr-lgate	215001	C0:A8:0F:11:BA:C0	0	2
6	tr-linx201	215002	C0:A8:0F:13:BA:C0	0	2
7	L-Gate	217368	C0:A8:03:44:BA:C0	0	2
8	L-Gate Steve (92)	224092	C0:A8:18:5C:BA:C0	0	2
9	L-Gate PerfTest	224095	C0:A8:18:5F:BA:C0	0	752
10	LINX-200 (for Backup)	224200	C0:A8:18:18:BA:C0	0	2
11	LVIS-ME200 (226064)	226064	C0:A8:1A:40:BA:C0	0	6
12	BACnet King	340556	C0:A8:1A:42:BA:C0	0	372

Properties

Object Type: Analog Output
Instance No.: 0
Property: Present_Value
Mapping Type: Write / Write
COV Expiry [s]: 90
Pollcycle [s]: 60
Write Priority: None

Figure 97: Modify Client Mapping Dialog.

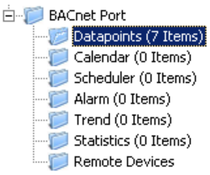
4. Edit the target device by selecting a different device in the **Mapped Device** list. Edit the target object instance number. For read client mappings edit the **COV expiry** or **Pollcycle** setting. For write client maps edit the **Write Priority**. When finished click **Save Changes**.

6.10.5 Create Server Object

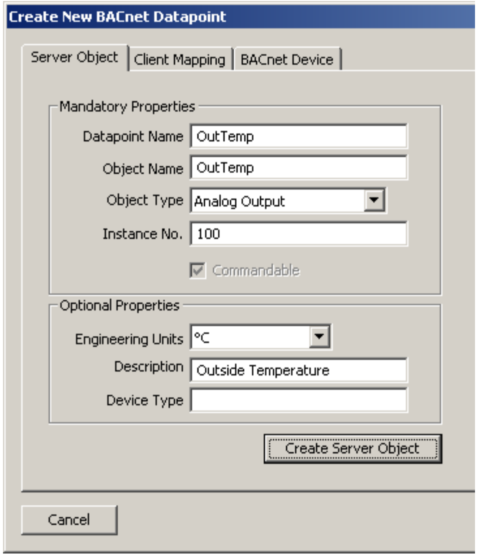
On the BACnet port server objects can also be created manually. These BACnet objects are visible on the BACnet network and can be modified by other devices. They appear as data points in the BACnet/Datapoints folder.

To Create Server Objects Manually

1. Select the BACnet Port/Datapoints folder



2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the **Create New BACnet Point** dialog as shown in Figure 98.



Datapoint Name: OutTemp
Object Name: OutTemp
Object Type: Analog Output
Instance No.: 100
☑ Commandable
Engineering Units: °C
Description: Outside Temperature
Device Type:

Figure 98: Create a Server Object manually.

3. In the **Mandatory Properties** enter a **Datapoint Name** and an **Object Type**. Optionally, update the **Instance No** and select the **Commandable** check box for value objects, if the value object shall be commandable from the network.

4. In the **Optional Properties** you may select **Engineering Units** for analog objects. For all object types you can enter the **Description**. The **Device Type** can be left empty.

5. Click **Create Server Object**. The BACnet data point is created and appears in the data point list.

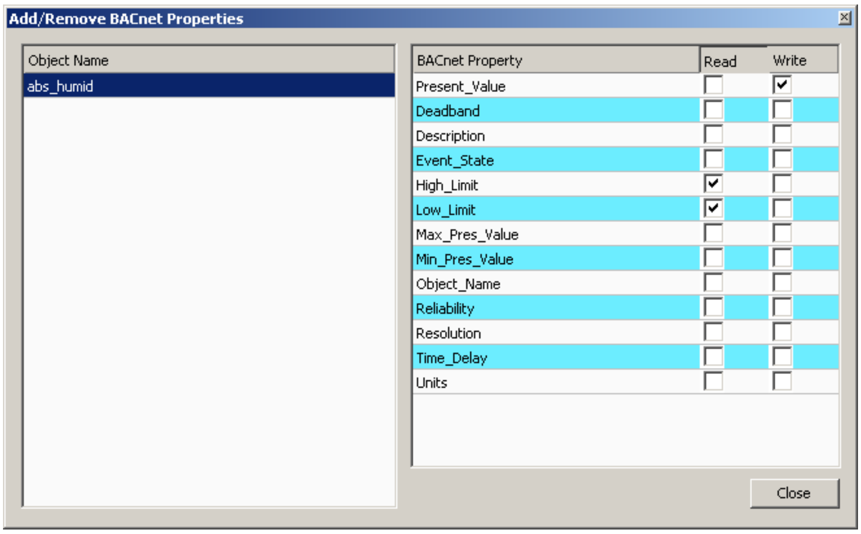
6.10.6 Map other Properties than Present_Value

When creating a BACnet server object, the Present_Value property is mapped by the created data point. That means writing and reading on the data point reads or writes the Present_Value. If other properties shall be accessed, they must be added to the BACnet server object's data point.

To Add other Properties

1. Select the BACnet server object for adding properties.

2. Right-click on the data point and select Add/Remove BACnet properties … . The dialog appears as shown in Figure 99.



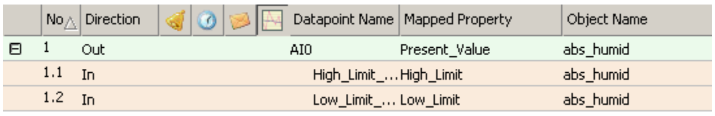
Object Name
abs_humid

BACnet Property	Read	Write
Present_Value	☐	☑
Deadband	☐	☐
Description	☐	☐
Event_State	☐	☐
High_Limit	☑	☐
Low_Limit	☑	☐
Max_Pres_Value	☐	☐
Min_Pres_Value	☐	☐
Object_Name	☐	☐
Reliability	☐	☐
Resolution	☐	☐
Time_Delay	☐	☐
Units	☐	☐

Figure 99: Dialog for adding/removing BACnet properties.

3. Check the additional properties. Checking the **Read** box will add an input data point, checking the **Write** box will add an output data point.

4. Click **Close**. The selected data point can now be expanded with the plus icon and show its additional properties as sub-data points.



	No	Direction	Datapoint Name	Mapped Property	Object Name
⊟	1	Out	AI0	Present_Value	abs_humid
	1.1	In	High_Limit_…	High_Limit	abs_humid
	1.2	In	Low_Limit_…	Low_Limit	abs_humid

5. To remove properties perform the same steps and uncheck the corresponding check-boxes. Alternatively, select the property (or more) and press the *Delete* key.

6.10.7 Enable International Character Support

By default BACnet objects on the device contain ASCII strings in properties such as object name, description, active/inactive text, state texts. This is the setting most third-party tools are interoperable with. To support international character sets, the device can be configured to expose strings as ISO-8895-1 (for most Western European languages) or UCS-2 (for Unicode character sets such as Japanese).

To Enable International Character Support

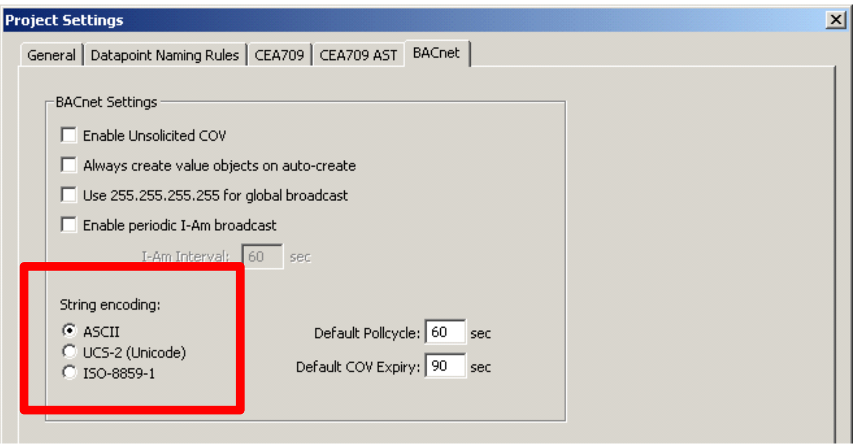
1. In the Configurator software menu go to **Settings → Project settings …**. This opens the **Project Settings** dialog.

2. Click on the tab **BACnet**.

3. Put a check mark either on ASCII (default), UCS-2 (Unicode, e.g., for Japanese), or ISO-8859-1 (for Western European languages), as indicated by the red rectangle in Figure 100.

4. Click **Ok.**

5. Download the configuration to activate the change.



BACnet Settings

□ Enable Unsolicited COV

□ Always create value objects on auto-create

□ Use 255.255.255.255 for global broadcast

□ Enable periodic I-Am broadcast

I-Am Interval: 60 sec

String encoding:

● ASCII

○ UCS-2 (Unicode)

○ ISO-8859-1

Default Pollcycle: 60 sec

Default COV Expiry: 90 sec

Figure 100: BACnet Project settings dialog.

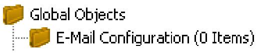
6.11 E-Mail Templates

6.11.1 Create an E-Mail Template

E-Mail templates are used to assemble and transmit E-Mails when certain trigger conditions occur. The E-Mail template contains the destination E-Mail address, the subject, and text. Variable parameters can be added to the text by using data point sources. The transmission of an E-Mail is triggered by one or more trigger data points. For setting up E-Mails, the E-Mail account information has to be configured on the device, e.g. on the Web UI (see Section 4.2.11).

To Create an E-Mail Template

1. Under the **Global Objects** folder, select the **E-Mail Configuration** sub-folder.

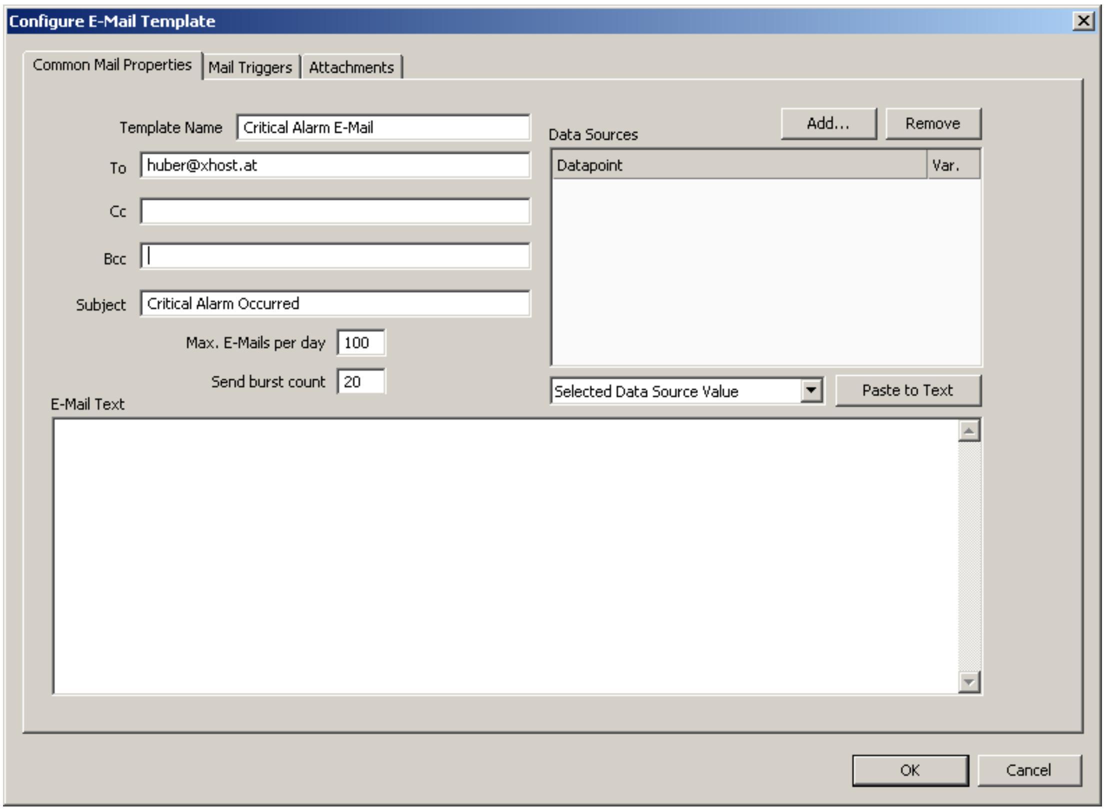


Global Objects

E-Mail Configuration (0 Items)

2. Right-click and select **New E-Mail Template …** from the context menu.

3. In the **Configure E-Mail Template** dialog, which is shown in Figure 101 enter the **To** address and the **Subject**. Optionally, **Cc** and **Bcc** addresses can be specified.



Template Name: Critical Alarm E-Mail

To: huber@xhost.at

Cc:

Bcc:

Subject: Critical Alarm Occurred

Max. E-Mails per day: 100

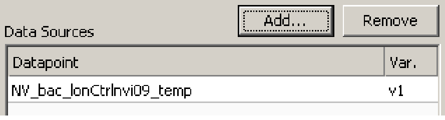
Send burst count: 20

Figure 101: Configure E-Mail Template Dialog.

4. Enter text in the **E-Mail Text** multi-line field.

5. If the E-Mail text shall contain values of data points, add data points to the **Data Sources** list by clicking the **Add…** button.

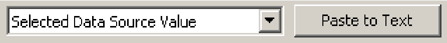
6. A data point selector dialog opens. Select one or more data points and click **Ok**. The selected data point appears in the **Data Sources** list.



Datapoint	Var.
NV_bac_lonCtrlnvi09_temp	v1

7. A data point selector dialog opens. Select one or more data points and click **Ok**. The selected data point appears in the **Data Sources** list.

8. Select the data point in the **Data Sources** list. In the drop-down box underneath select **Selected Data Source Value** and click the **Paste to Text** button.



9. A place holder `%{v1}` for the data point value appears now in the E-Mail text.

6.11.2 Trigger E-Mails

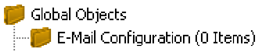
E-Mail templates are used to assemble and transmit E-Mails when certain trigger conditions occur. For an E-Mail template, one or more trigger conditions can be defined. The E-Mail will be sent, when one of the trigger conditions is activated. Depending of the trigger data point type, the trigger conditions can be refined.

Note, that the behavior of the trigger data point is influenced by the COV properties of the data point. If the **Only notify on COV** property is checked, the data point triggers only if its value changes to the value of the trigger condition. If that property is not checked, the data point triggers on every write with a value that matches the trigger condition.

The trigger for sending an E-Mail can be enabled or disabled altogether by using an *enable* data point. This data point must be of type *binary*. If the value of that enable data point is TRUE, the trigger conditions are evaluated. If the value of the enable is FALSE, no E-Mails are be triggered.

To Create an E-Mail Trigger

1. Under the **Global Objects** folder, select the **E-Mail Configuration** sub-folder.



Global Objects
E-Mail Configuration (0 Items)

2. Right-click and select **Configure E-Mail Template …** from the context menu.

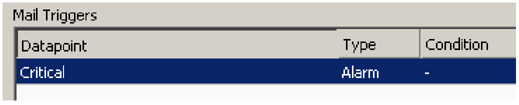
3. Change to the **Mail Triggers** tab.

Note: *Of course, you can also change directly to the **Mail Triggers** tab when creating an E-Mail template.*

4. Click the **Add…** button. A data point selection dialog opens.

5. Select one or more data point and click **Ok**.

6. The triggers appear now in the **Mail Triggers** list. The data points that server as E-Mail triggers also appear with the E-Mail icon ✉ in the data point list.

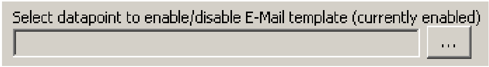


Mail Triggers

Datapoint	Type	Condition
Critical	Alarm	-

7. In the **Manage Trigger Conditions** you can refine the trigger condition depending on the trigger data point class.

8. If the trigger condition is depending on the value of an enabling data point, you can add an enable data point by clicking on the **…** button.



Select datapoint to enable/disable E-Mail template (currently enabled)

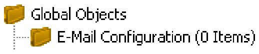
9. To remove such a trigger enable, click the **Remove Enable Trigger** button.

6.11.3 Attachments

E-Mail templates can be configured to have file attachments. Basically, any file of the device can be specified as an attachment.

To Configure Attachments

1. Under the **Global Objects** folder, select the **E-Mail Configuration** sub-folder.



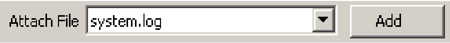
Global Objects
E-Mail Configuration (0 Items)

2. Right-click and select **Configure E-Mail Template …** from the context menu.

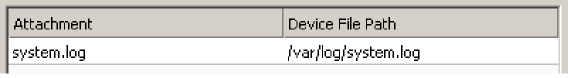
3. Change to the **Attachments** tab.

Note: *Of course, you can also change directly to the* ***Attachments*** *tab when creating an E-Mail template.*

4. Select an available file from the **Attach File** drop-down box.


Attach File: system.log

5. Click the **Add** button. The file appears in the **Attachments** list.



Attachment	Device File Path
system.log	/var/log/system.log

6. To remove an attachment, select the attachment file in the **Attachments** list and click the button **Remove**.

6.11.4 Limit E-Mail Send Rate

The transmission of E-Mails is triggered by the configured trigger conditions. It is not predictable, how often the trigger condition will cause the transmission of an E-Mail. The E-Mail template can be configured to limit the number of transmitted E-Mails. This is done in the Configure E-Mail Template dialog.

To configure an E-Mail Rate Limit, configure the settings:

- **Max. E-Mails per day**: This setting defines how many e-mails can be sent on average per day. The actual number of transmitted e-mails on a specific day may be slightly higher than this setting, depending on burst rates. The default is 100 e-mails per day. This results in an average interval of one e-mail per 14 minutes.
- **Send burst count**: This setting defines how many e-mails may be transmitted shortly after each other not limited by the above average interval. After the burst count, the average mails per day limit takes effect. The default is a maximum of 20 e-mails in a row.

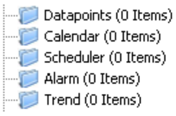
6.12 Local Schedule and Calendar

6.12.1 Create a Calendar

As the first step, the required data points must be created. A calendar must be created, if the schedules shall work with exception days, such as “Holidays”. If it suffices for schedules to define daily schedules for normal weekdays only, no calendar needs to be created. On each port, one calendar can be created.

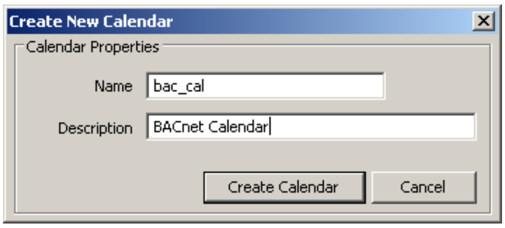
To Create a Calendar

1. Under the port folder, select the **Calendar** sub-folder.



2. Right-click in the data point list view and select **New local Calendar …**.

3. In the Create New Calendar dialog box (as shown in Figure 102) enter Name and Description of the calendar.



Create New Calendar

Calendar Properties

Name: bac_cal

Description: BACnet Calendar

Figure 102: Create New Calendar dialog box.

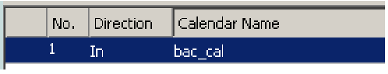
4. Click **Ok**. The calendar appears now in the data point list view.

6.12.2 Create Calendar Pattern

When a local calendar is used, it needs to be configured with calendar patterns. A cleandar pattern represents a class of days such as “Holidays”. The calendar patterns can then be used in a schedule to define daily schedules for exception days. The available calendar patterns should be created when the system configuration is engineered. The actually dates in the calendar patterns can be modified later at run-time.

To Create a Calendar Pattern

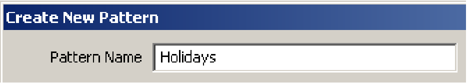
1. Select an existing calendar data point.



No.	Direction	Calendar Name
1	In	bac_cal

2. Right-click and select **Create Calendar Pattern…**

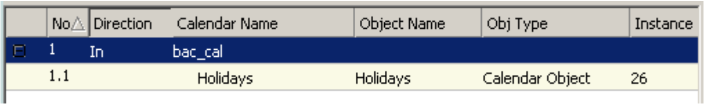
3. Enter a Pattern Name in the **Create Calendar Pattern** dialog



Create New Pattern

Pattern Name: Holidays

4. Click **Create Pattern**. The dialog closes and the calendar pattern appears beneath the calendar data point.



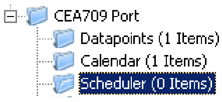
No	Direction	Calendar Name	Object Name	Obj Type	Instance
1	In	bac_cal			
1.1		Holidays	Holidays	Calendar Object	26

6.12.3 Create a Local Scheduler

For scheduling data points, a scheduler object must be created. On each port, multiple local scheduler objects can be created. These local schedulers can then be configured to schedule data points.

To Create a Local Scheduler

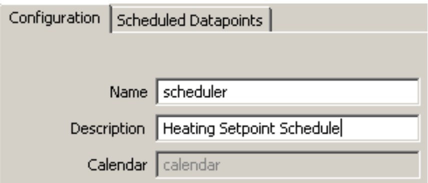
1. Under the port folder, select the **Scheduler** sub-folder.



CEA709 Port
- Datapoints (1 Items)
- Calendar (1 Items)
- Scheduler (0 Items)

2. Right-click in the data point list view and select **New Local Scheduler ….**

3. Enter a name for the schedule and a description. Note, that the schedule automatically detects a calendar, if it has previously been created.



Name: scheduler
Description: Heating Setpoint Schedule
Calendar: calendar

4. Click **Create Schedule**. The new schedule appears in the data point list of the Scheduler sub-folder.

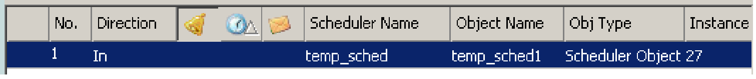
6.12.4 Configure Scheduled Data Points

When a local scheduler has been created, it needs to be configured, which data points it shall schedule. This is done by attaching data points to the scheduler. Note, that there may be limits, how many and which data points may be attached (see Section 5.5.3).

This configuration must be done as an initial setup. Which data points are scheduled cannot be changed at run-time. The daily schedules, however, can be changed later in the Web UI or over the network.

To Attach Data Points to a Scheduler

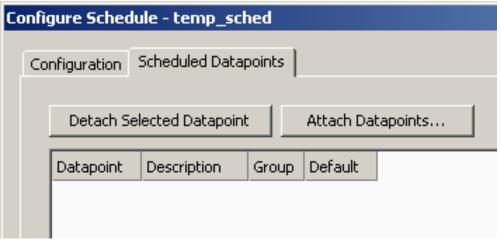
1. Select the scheduler data point in the Scheduler sub-folder.



No.	Direction				Scheduler Name	Object Name	Obj Type	Instance
1	In				temp_sched	temp_sched1	Scheduler Object 27	

2. Right-click and select Configure Schedule from the context menu. The same dialog which appears when a new scheduler is created is shown and allows to configure the scheduler. Of course, this step can also be done directly when the point is created.

3. Select the tab Scheduled Datapoints.



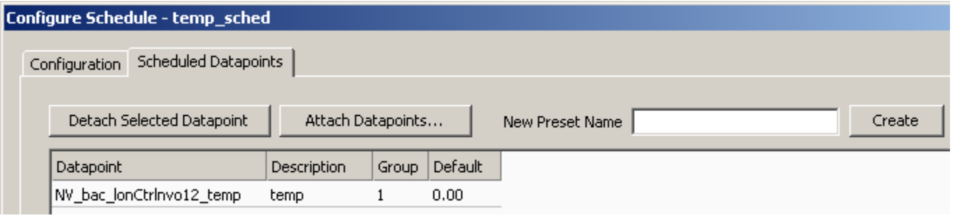
Datapoint	Description	Group	Default

4. Click the button Attach Datapoints . This opens another data point selector window.

5. Select the data points to attach and click Ok. For each of the attached data points, one or more lines appear in the list below the attach button. If the attached point is a structure, there will be one line for each element of the structure.

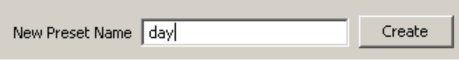
Tip! *Data points can also be attached to a scheduler by selecting a data point in the data point manager, drag it onto a scheduler data point and drop it on the scheduler data point.*

6. Enter a Description text in the second column of each line. This text will be shown when the user changes a value set on the device later on.



Datapoint	Description	Group	Default
NV_bac_lonCtrlnvo12_temp	temp	1	0.00

7. Add new value presets by entering a name and pressing the Create button next to the input field.

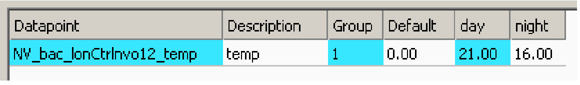


New Preset Name day

Tip! *To generate presets automatically for multi-state data points, click the* ***Auto-Create*** *button. This button is available, if no other presets have been defined yet.*

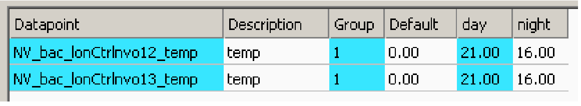
---

8. For each new preset, a new column will appear in the list. In this column, enter the desired value for each of the attached points, which will be set when this value template is scheduled. The user may later edit the values for each preset on the device but cannot add new value presets unless there is only one line (one value) in the list.



Datapoint	Description	Group	Default	day	night
NV_bac_lonCtrlnvo12_temp	temp	1	0.00	21.00	16.00

9. If there are multiple output values which belong together, they can be grouped in order to save space on the device. For each group, the entered value is stored only once, even if there are more data points in the same group.



Datapoint	Description	Group	Default	day	night
NV_bac_lonCtrlnvo12_temp	temp	1	0.00	21.00	16.00
NV_bac_lonCtrlnvo13_temp	temp	1	0.00	21.00	16.00

10. When done with the point and value setup, switch back to the Configuration tab or click Save Changes to leave the dialog.

Tip! *A shortcut to creating a scheduler object and attaching a data point is to select a data point in the data point manager, right-click on it and choose* ***Schedule Datapoint*** *from the context menu. This generates a scheduler and links that data point to it.*

6.12.5 Configure Daily Schedules

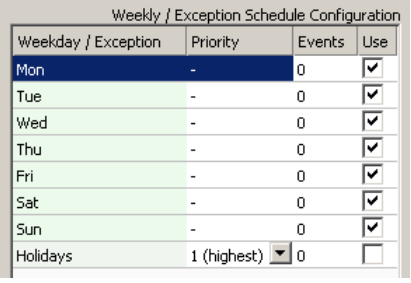
Once a scheduler is configured with attached data points and value presets, the daily schedules can be defined. This can be done on the device or over the network at run-time, or also in the configuration software. A daily schedule defines the time and value sequences in a 24-hour period starting at 00:00 and ending at 23:59 hours. For each weekday its own daily schedule can be configured.

In addition, daily schedules can be configured for exception days from a calendar, such as “Holidays”. An exception day always overrides a normal weekday. If more than one exception day is used, a priority must be assigned. This is necessary so that the system knows which schedule to follow on a day which is part of more than one calendar pattern.

To Configure a Daily Schedule

1. Open the Configure Schedule dialog and click on the Configuration tab (see Section 6.12.4).

2. Select the day for which to configure a daily schedule.

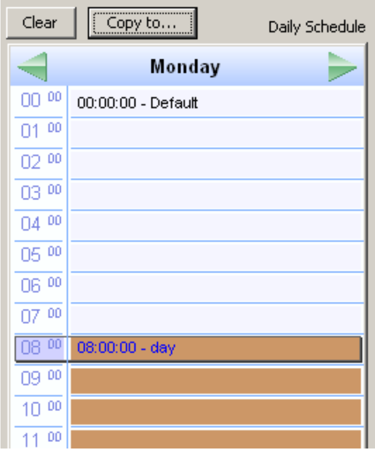


Weekly / Exception Schedule Configuration

Weekday / Exception	Priority	Events	Use
Mon	-	0	☑
Tue	-	0	☑
Wed	-	0	☑
Thu	-	0	☑
Fri	-	0	☑
Sat	-	0	☑
Sun	-	0	☑
Holidays	1 (highest)	0	□

3. Select a value preset in the **Available Data Presets** box on the upper right-hand side.

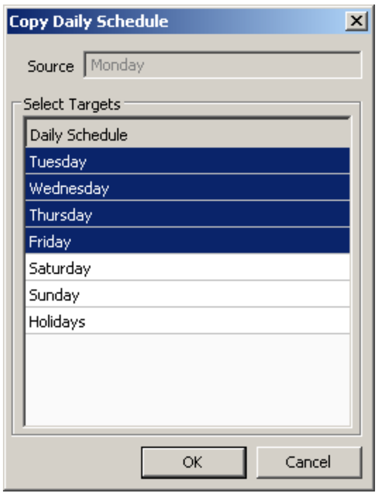
4. Drag and drop the preset from this list into the time table area to define the desired output values on the day schedule.



00:00:00 - Default

08:00:00 - day

5. Completed daily schedules may be copied to other days using the **Copy to** button. For example, the Monday may serve as the template for a regular work day and be copied to Tuesday till Friday. Then click **Ok**.



Copy Daily Schedule

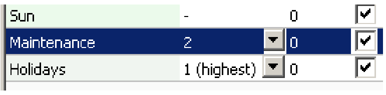
Source: Monday

Select Targets

Daily Schedule
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
- Holidays

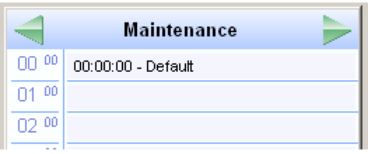
To Use Exception Days

1. Select a calendar pattern, which shall be used as an exception day and place a checkmark on it.



Sun	-	0	☑
Maintenance	2	0	☑
Holidays	1 (highest)	0	☑

2. Edit the daily schedule.



00:00:00 - Default

3. If more than one calendar pattern is used, edit the priorities. For example, if a given calendar day falls in both categories, “Holidays” and “Maintenance”, the exception day with the higher priority becomes effective on that day. The highest available priority is marked **highest**. Note, that the actual priority values depend on the technology (see Section 5.5.3).

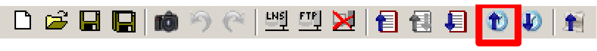
Important! ***Choose different priorities for different exceptions. If two exceptions are valid for a given day and their priorities are equal, it is not determined, which exception is in effect.***

6.12.6 Configure Exception Days

When a local calendar is used, its calendar patterns need to be configured with exception days (pattern entries). The calendar patterns can be configured in the L-Gateway configuration software or be modified at run-time over the Web UI or over the network. When configuring in the software, the current exception days should be uploaded from the device, to work on the current configuration.

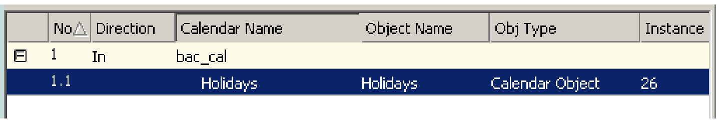
To Configure a Calendar Pattern

1. Click on the Upload calendar/scheduler configuration button



in the tool bar of the main connections window. Click **Ok** when the upload is finished.

2. Select the **Calendar** sub-folder and select the calendar pattern, which shall be configured

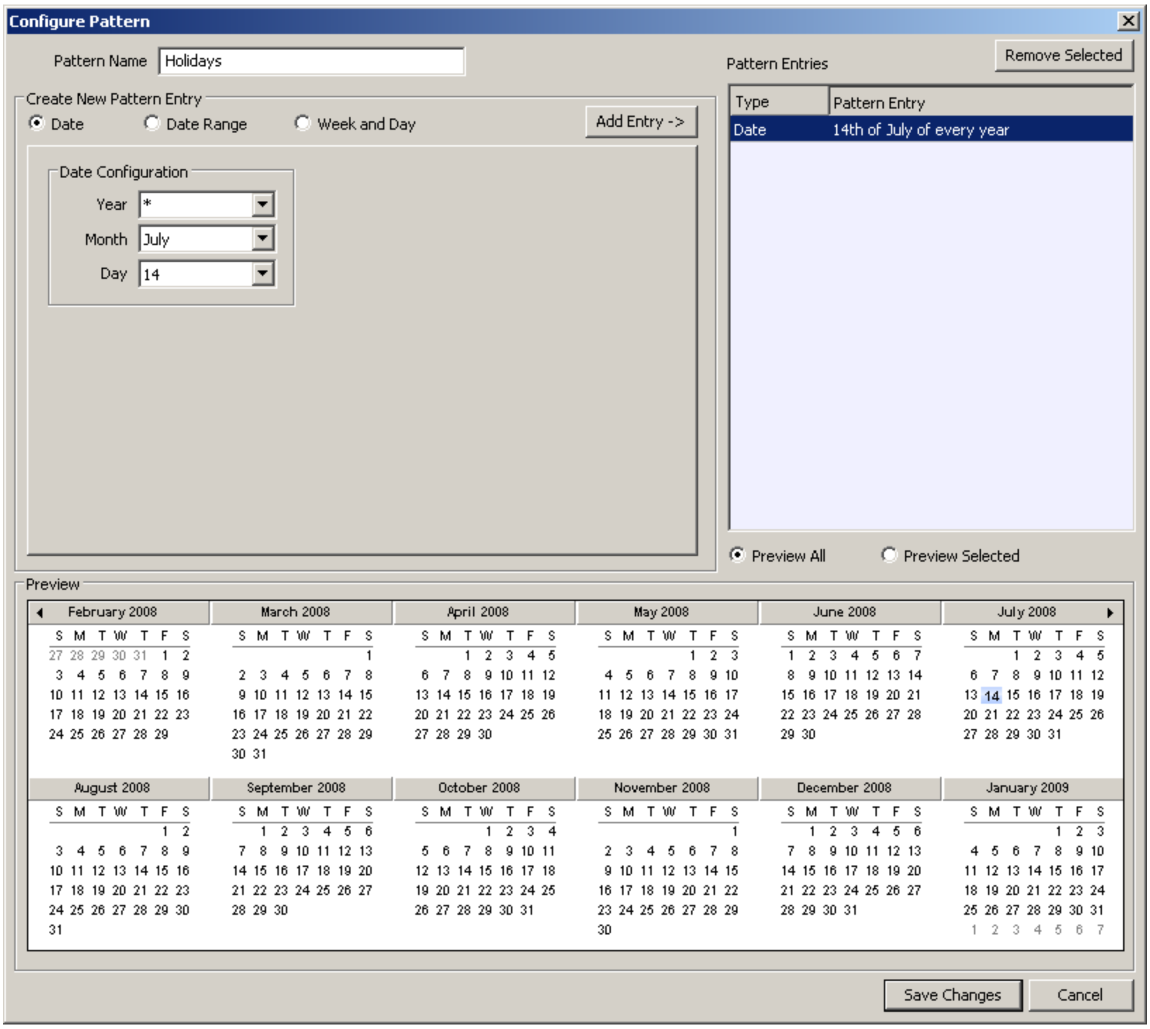


	No	Direction	Calendar Name	Object Name	Obj Type	Instance
⊟	1	In	bac_cal			
	1.1		Holidays	Holidays	Calendar Object	26

3. Right-click and select **Configure Pattern …** in the context menu.

4. The **Configure Pattern** dialog appears as shown in Figure 103. Add dates to the calendar pattern by entering a Date Configuration. Then click **Add Entry**. The date appears in the **Pattern Entries** list on the right-hand side.

5. Edit an exception by selecting the pattern entry in the **Pattern Entries** list. Then modify the date configuration in the **Date Configuration** group box.



Pattern Name: Holidays

● Date ○ Date Range ○ Week and Day

Year: *
Month: July
Day: 14

Pattern Entries

Type	Pattern Entry
Date	14th of July of every year

● Preview All ○ Preview Selected

```
February 2008          March 2008             April 2008
 S  M  T  W  T  F  S    S  M  T  W  T  F  S    S  M  T  W  T  F  S
27 28 29 30 31  1  2                      1          1  2  3  4  5
 3  4  5  6  7  8  9    2  3  4  5  6  7  8    6  7  8  9 10 11 12
10 11 12 13 14 15 16    9 10 11 12 13 14 15   13 14 15 16 17 18 19
17 18 19 20 21 22 23   16 17 18 19 20 21 22   20 21 22 23 24 25 26
24 25 26 27 28 29      23 24 25 26 27 28 29   27 28 29 30
                       30 31

May 2008               June 2008              July 2008
 S  M  T  W  T  F  S    S  M  T  W  T  F  S    S  M  T  W  T  F  S
             1  2  3    1  2  3  4  5  6  7          1  2  3  4  5
 4  5  6  7  8  9 10    8  9 10 11 12 13 14    6  7  8  9 10 11 12
11 12 13 14 15 16 17   15 16 17 18 19 20 21   13 14 15 16 17 18 19
18 19 20 21 22 23 24   22 23 24 25 26 27 28   20 21 22 23 24 25 26
25 26 27 28 29 30 31   29 30                  27 28 29 30 31

August 2008            September 2008         October 2008
 S  M  T  W  T  F  S    S  M  T  W  T  F  S    S  M  T  W  T  F  S
                1  2       1  2  3  4  5  6             1  2  3  4
 3  4  5  6  7  8  9    7  8  9 10 11 12 13    5  6  7  8  9 10 11
10 11 12 13 14 15 16   14 15 16 17 18 19 20   12 13 14 15 16 17 18
17 18 19 20 21 22 23   21 22 23 24 25 26 27   19 20 21 22 23 24 25
24 25 26 27 28 29 30   28 29 30               26 27 28 29 30 31
31

November 2008          December 2008          January 2009
 S  M  T  W  T  F  S    S  M  T  W  T  F  S    S  M  T  W  T  F  S
                   1       1  2  3  4  5  6                1  2  3
 2  3  4  5  6  7  8    7  8  9 10 11 12 13    4  5  6  7  8  9 10
 9 10 11 12 13 14 15   14 15 16 17 18 19 20   11 12 13 14 15 16 17
16 17 18 19 20 21 22   21 22 23 24 25 26 27   18 19 20 21 22 23 24
23 24 25 26 27 28 29   28 29 30 31            25 26 27 28 29 30 31
30                                             1  2  3  4  5  6  7
```

Figure 103: Configure Calendar Pattern Dialog.

6. Click **Save Changes** when all exception days have been entered.

Tip! *When not sure, how a date configuration affects the calendar days, click on a pattern in the* ***Pattern Entries*** *list and the affected days will be highlighted in the* ***Preview****.*

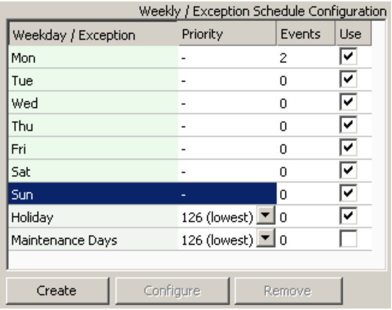
6.12.7 Configure Embedded Exceptions

Besides exception days of the calendar, special exception days can be embedded into the scheduler. These embedded exception days are not visible or accessible in other scheduler objects.

To Configure an Embedded Exception

1. Open the **Configure Schedule** dialog to configure daily schedules as described in Section 6.12.4.

2. Click on the **Create** button below the **Weekly/Exception Schedule Configuration** list

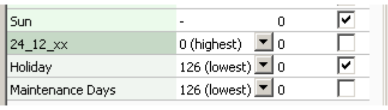


Weekly / Exception Schedule Configuration

Weekday / Exception	Priority	Events	Use
Mon	-	2	☑
Tue	-	0	☑
Wed	-	0	☑
Thu	-	0	☑
Fri	-	0	☑
Sat	-	0	☑
Sun	-	0	☑
Holiday	126 (lowest)	0	☑
Maintenance Days	126 (lowest)	0	□

3. The **Create Pattern** dialog opens. You can enter exactly one pattern entry for the embedded exception. It is recommended to choose a descriptive name for the day, e.g. ‘24_12’xx’ for every 24th of December.

4. Click **Create Pattern**. The embedded exception is now available.



Sun	-	0	☑
24_12_xx	0 (highest)	0	□
Holiday	126 (lowest)	0	☑
Maintenance Days	126 (lowest)	0	□

6.12.8 Configure Control Data Points

A scheduler object can be configured to use special control data points. An *enable/disable* data point can be configured, which enables or disables the scheduler depending on its Boolean value. An *enable/disable feedback* data point is updated with the current enabled state of the scheduler. This also reflects and an enable from the network. The *Preset Name* data point can be attached to be updated with the name of the currently active preset.

To Configure Control Data Points

1. Open the **Configure Schedule** dialog to configure daily schedules as described in Section 6.12.4.

2. Go to the **Scheduled Datapoints** tab.

3. In the Control Datapoints group box, click the ... button to add the desired control data point. A data point selection dialog opens.

4. Select a matching data point and click **OK**. For the preset name a string data point must be selected.

5. To remove an undesired control data point, click on the **Remove** button.

6.12.9 Using the SNVT_tod_event

The SNVT_tod_event can be used in a schedule for implementing the next-state feature. The parts of this network variable contain:

- Current state: This is the currently scheduled occupancy state.

- Next state: This is the next, future occupancy state in the schedule.

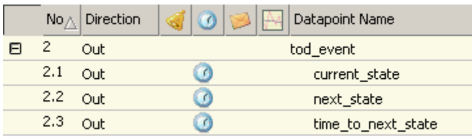
- Time to next state: This part reflects the time in minutes until the next state becomes active.

To Use a SNVT_tod_event

1. Create a SNVT_tod_event in the data point configuration.

2. Add the SNVT_tod_event to the scheduled data points of a scheduler as described in Section 6.12.4.

3. All three parts of the SNVT_tod_event are scheduled.



	No	Direction					Datapoint Name
⊟	2	Out					tod_event
	2.1	Out		🕒			current_state
	2.2	Out		🕒			next_state
	2.3	Out		🕒			time_to_next_state

6.12.10 Using the Local Scheduler

Once the setup of the local scheduler is done, it is basically operational. It will immediately start to work based on the configuration data downloaded through the configuration software. You can verify the daily schedules and values of scheduled data points on the Web UI (see Section 4.2.14). The local schedule can be altered over the Web UI or using the network technology of the port, where the scheduler has been created.

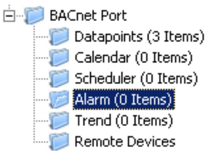
6.13 Local Alarming

6.13.1 Create an Alarm Server

To generate local alarms, an alarm server needs to be created at first. The local alarm sources will report alarms to that alarm server. The alarm server is the interface to access local alarms. This can be done over the network or the Web UI.

To Create an Alarm Server

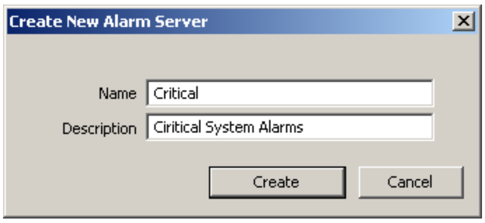
1. Under the port folder, select the **Alarm** sub-folder.



BACnet Port
- Datapoints (3 Items)
- Calendar (0 Items)
- Scheduler (0 Items)
- Alarm (0 Items)
- Trend (0 Items)
- Remote Devices

2. Right-click in the data point list view and select **New Alarm Server ….**

3. In the **Create New Alarm Server** dialog box (as shown in Figure 104) enter **Name** and **Description** of the alarm server.



Create New Alarm Server

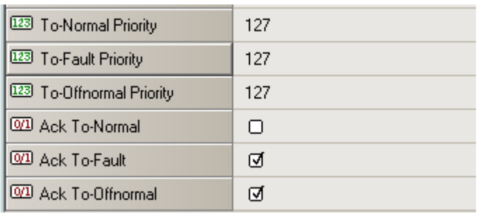
Name: Critical

Description: Ciritical System Alarms

Figure 104: Create New Alarm Server dialog box.

4. Click **Ok**. The alarm server appears now in the data point list view.

5. For a BACnet alarm server, select the created object and edit the properties for transition priorities (To-Normal, To-Fault, To-Offnormal) and the corresponding check boxes, which define whether acknowledgements are required. These are the standard BACnet settings in a Notification Class object.



To-Normal Priority	127
To-Fault Priority	127
To-Offnormal Priority	127
Ack To-Normal	☐
Ack To-Fault	☑
Ack To-Offnormal	☑

6.13.2 Create an Alarm Condition

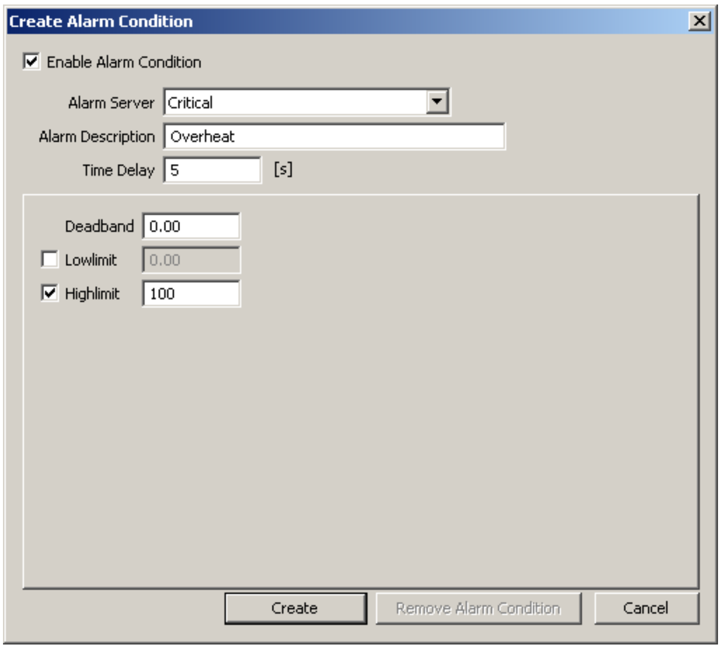
To generate alarms from data points, intrinsic reporting is used. For each data point an alarm condition must be defined. This condition employs an intrinsic algorithm to generate alarms based on the data point’s value. Depending on the data point type (analog, binary, multi-state), different conditions are defined. The alarm is reported to the attached alarm server. Currently, only BACnet data points can be configured with intrinsic alarm conditions.

To Create an Intrinsic Alarm Condition

1. Select a data point.

2. Right-click and select **Create Alarm Condition…** from the context menu.

3. For an analog data point the dialog as shown in Figure 105 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select **Low Limit** and **High Limit** and put check marks, if they shall be employed. Enter a **Deadband**, to account for hysteresis.



Create Alarm Condition

☑ Enable Alarm Condition

Alarm Server: Critical

Alarm Description: Overheat

Time Delay: 5 [s]

Deadband: 0.00

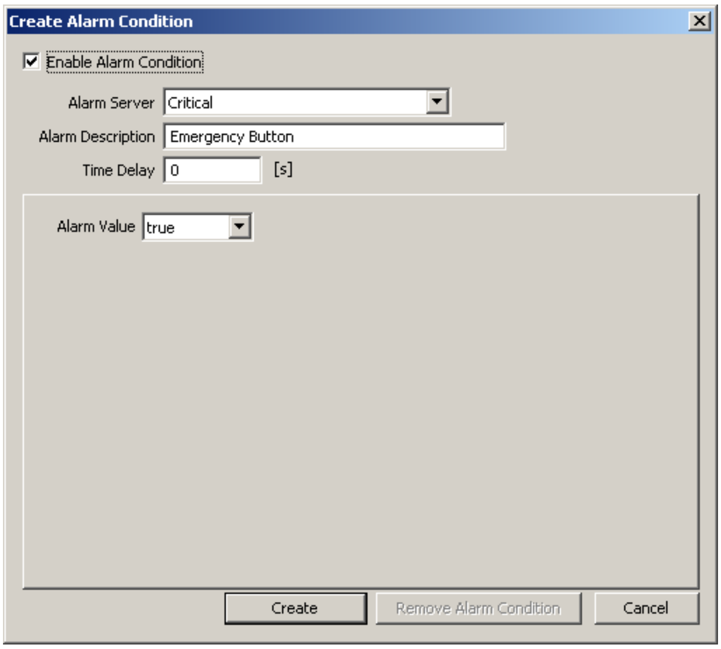
☐ Lowlimit: 0.00

☑ Highlimit: 100

Figure 105: Alarm Condition for an Analog Data Point.

4. For a binary data point the dialog as shown in Figure 106 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the

data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select the **Alarm Value** which triggers the alarm.



☑ Enable Alarm Condition

Alarm Server: Critical

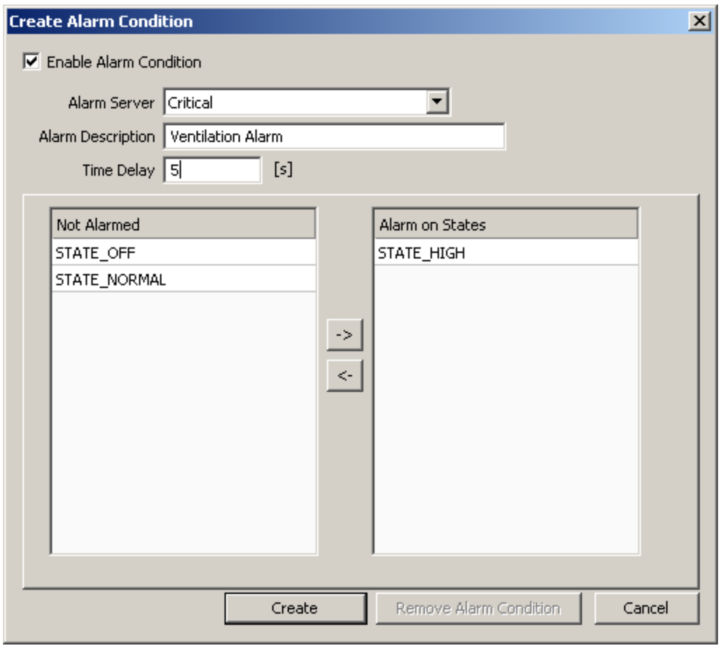
Alarm Description: Emergency Button

Time Delay: 0 [s]

Alarm Value: true

Figure 106: Alarm Condition for a Binary Data Point.

5. For a multi-state data point the dialog as shown in Figure 107 appears. Select the **Alarm** Server. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select the **Alarm States**, which triggers the alarm, by clicking the arrow buttons.



☑ Enable Alarm Condition

Alarm Server: Critical

Alarm Description: Ventilation Alarm

Time Delay: 5 [s]

Not Alarmed	Alarm on States
STATE_OFF	STATE_HIGH
STATE_NORMAL	

Figure 107: Alarm Condition for a Multi-State Data Point.

6. Click on **Create**. In the alarm column, the alarm sign 🔔 will be added for those data points, that have an alarm condition.

6.13.3 Deliver Alarms via E-Mail

Updates in the alarm summary of an alarm object can be used as a trigger to send e-mail. For setting up e-mails, the account information has to be configured on the device, e.g. on the Web UI (see Section 4.2.11). Then an e-mail template can be created and the alarm point attached as a trigger.

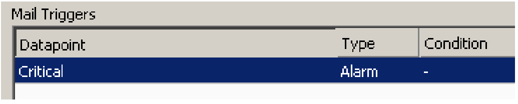
To Create an E-Mail Template for Alarms

1. Create or configure an E-Mail template as described in Section 6.11.1.

2. Change to the **Mail Triggers** tab.

3. Click the **Add…** button and select an alarm data point.

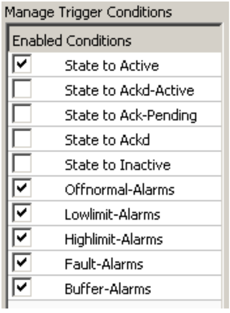
4. In the Mail Triggers list select the added trigger data point.



Mail Triggers

Datapoint	Type	Condition
Critical	Alarm	-

5. In the **Manage Trigger Conditions** list put a check mark on alarm conditions that shall invoke the transmission of the e-mail.



Manage Trigger Conditions

Enabled Conditions
- ☑ State to Active
- ☐ State to Ackd-Active
- ☐ State to Ack-Pending
- ☐ State to Ackd
- ☐ State to Inactive
- ☑ Offnormal-Alarms
- ☑ Lowlimit-Alarms
- ☑ Highlimit-Alarms
- ☑ Fault-Alarms
- ☑ Buffer-Alarms

6. Change to the **Common E-Mail Properties** tab.

7. Add the alarm data point as a data source and insert the place holder into the e-mail text as described in Section 6.11.1.

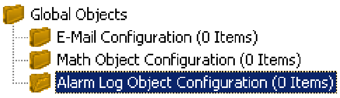
6.13.4 Create an Alarm Log

The alarm objects on the device contain an alarm summary (live list) of currently active and acknowledge-pending alarms. As soon as an alarm becomes inactive and has been acknowledged, it disappears from the alarm summary. To store a historical log of alarm transitions an *alarm log* needs to be created.

An alarm log can log transitions of one or more alarm objects. Its size is configurable. The alarm log is a ring buffer. As soon as its size limit is reached, the oldest alarm log records are overwritten by new alarm transitions.

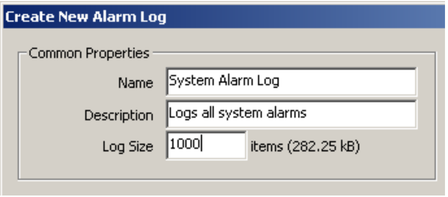
To Create an Alarm Log

1. Under the **Global Objects** folder, select the **Alarm Log Object Configuration** sub-folder.



Global Objects
E-Mail Configuration (0 Items)
Math Object Configuration (0 Items)
Alarm Log Object Configuration (0 Items)

2. In the data point list right-click and select **New Alarm Log …** from the context menu.



Create New Alarm Log

Common Properties

Name: System Alarm Log

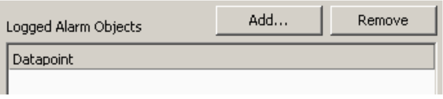
Description: Logs all system alarms

Log Size: 1000 items (282.25 kB)

3. In the **Create New Alarm Log** dialog enter a **Name** for the alarm log. Optionally enter a **Description**.

4. Enter a **Log Size**, which defines how many transitions are resident in the alarm log.

5. Click on the button **Add…** on top of the **Logged Alarm Objects** list.



6. A data point selector dialog opens. Select one or more alarm objects that shall be logged and click **OK**. The alarm objects appear in the list.

7. Click **Create** to create the alarm log object.

6.14 Local Trending

6.14.1 Create a Local Trend

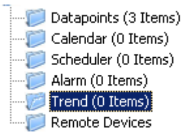
The value of a data point can be logged over time. This is referred to as trend data. To generate trend data a trend object has to be created. The trend data is stored in a data logger file. This file can be downloaded via FTP in binary or CSV format (see Section 7.1.2).

Trend objects can generate trend logs for multiple data points and can be operated in one of three basic modes:

- **Interval Mode**: In this mode a snapshot of all trended data points is logged into the data logger file.
- **COV Mode**: In this mode, each of the trended data points is logged separately, if and only if its value changes. For analog data points, a specific COV increment can be configured in the data point configuration properties of the trended data point.
- **Trigger Mode**: In this mode a snapshot of all trended data points is logged each time a trigger condition fires. The trigger condition is applied to a trigger data point.

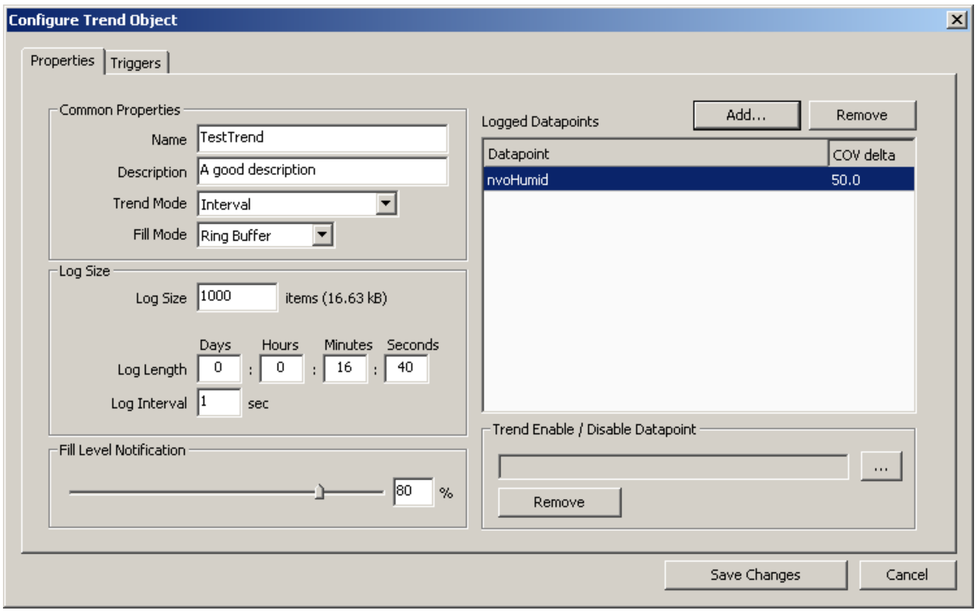
To Create a Trend Object

1. Under the port folder, select the **Trend** sub-folder to create a trend log object.



2. Right-click and select **New Trend …** from the context menu.

3. In the **Create New Trend Object** dialog (shown in Figure 108) enter a name and optionally a description for the trend log object.



Name: TestTrend
Description: A good description
Trend Mode: Interval
Fill Mode: Ring Buffer
Log Size: 1000 items (16.63 kB)
Log Length: Days 0 : Hours 0 : Minutes 16 : Seconds 40
Log Interval: 1 sec
Fill Level Notification: 80 %

Datapoint	COV delta
nvoHumid	50.0

Figure 108: Basic Trend Object Configuration.

4. Select the desired **Trend Mode**.

5. Select the **Log Size**. The display in the dialog will adapt the estimations for needed data logger file size in KB and duration of the trend log. Alternatively, for interval trends, the estimated log duration and log interval can be edited.

6. Select a **Fill Level Notification** percentage. This will decide at which fill-level trigger will fire. A fill-level trigger can be used to trigger the transmission of an e-mail (see Section 6.14.5).

7. Click **Save Changes** to store the basic configuration of the trend object. The new trend log object appears in the data point list of the Trend folder.

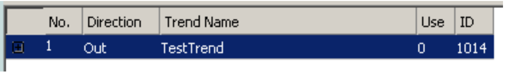
6.14.2 Configure Trended Data Points

When a local trend object has been created, it needs to be configured, which data points it shall log. This is done by attaching data points to the trend object. Only simple data points can be attached for trending, i.e., of class analog, binary, or multi-state. For trend log objects in the CEA-709 technology, multiple data points can be attached for trending.

The trending can be enabled/disabled on behalf of an *enable* data point. This data point should be of type *binary*. If the value of that enable data point is TRUE, the trend object logs data as defined by the trend mode. If the value of the enable is FALSE, trending is disabled. If no enable data point is configured, the trend log is always enabled.

To Attach Data Points for Trending

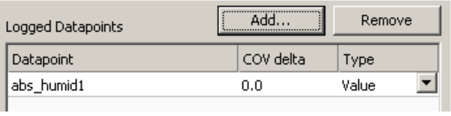
1. Select the trend object in the Trend sub-folder.



No.	Direction	Trend Name	Use	ID
1	Out	TestTrend	0	1014

2. Right-click and select **Configure Trend** from the context menu. The same dialog which appears when a new trend object is created is shown and allows configuring the trend object. Of course, this step can also be done directly when the object is created.

3. Add data points to be trended. Click on **Add …** which opens a data point selector window.



Logged Datapoints

Datapoint	COV delta	Type
abs_humid1	0.0	Value

4. Select the data points and click **OK**. For each of the attached data points, a line appears in the list below the add button. The trended data points will also appear with the trend icon in the data point manager.

Tip! *Data points can also be attached to a trend by selecting a data point in the data point tab, drag it onto a trend object and drop it on the trend object.*

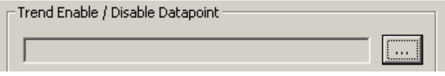
5. Data points can be removed from the trend by clicking **Remove**.

6. If COV mode was selected, the COV increment is displayed in the **COV delta** column. This value can be increased to produce less trend data. Note, that it cannot be lowered under the trended data point's own COV increment. Go to the data point configuration to change the COV increment in this case.

7. If the trended value of the data point shall be aggregated over the log interval, select the desired aggregation in the **Type** column. Available options are **Min**, **Max**, **Avg**.

Tip! *For creating multiple curves with min, average, and maximum values, add the same data point three times and select the different aggregation types.*

8. In addition, a special **Trend Enable** data point can be selected. If configured, the trend log will only log data, if the value of this data point evaluates **true**, i.e., is not zero. Click the **…** button to select a data point.



9. To remove the enable data point, click the **Remove** button.

10. When done with the data point setup, click **Save Changes** to leave the dialog.

Tip! *A shortcut to creating a trend log object and attaching a data point is to select a data point in the data point manager, right-click on it and choose **Trend Datapoint** from the context menu. This generates a trend log and links that data point to it.*

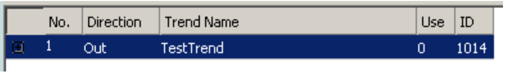
6.14.3 Trend Triggers

Local trend objects in CEA-709 can be operated in *trigger mode*. In this mode, one or more trigger data points cause the generation of a snapshot containing the values of the trended data points at the time instant the trigger is activated. For a trend object, one or more trigger conditions can be defined. Depending on the trigger data point type, the trigger conditions can be refined.

Note, that the behavior of the trigger data point is influenced by the COV properties of the data point. If the **Only notify on COV** property is checked, the data point triggers only if its value changes to the value of the trigger condition. If that property is not checked, the data point triggers on every write with a value that matches the trigger condition.

To Configure Trigger Data Points for Trending

1. Select the trend object in the **Trend** sub-folder.



No.	Direction	Trend Name	Use	ID
1	Out	TestTrend	0	1014

2. Right-click and select **Configure Trend** from the context menu.

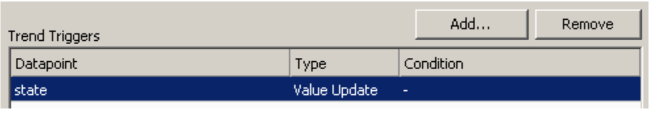
3. Change to the **Triggers** tab.

Note: *Of course, you can also change directly to the **Triggers** tab when creating a trend object.*

4. Click the **Add…** button. A data point selection dialog opens.

5. Select one or more data points and click **OK**.

6. The triggers appear now in the **Trend Triggers** list.



Datapoint	Type	Condition
state	Value Update	-

7. In the **Manage Trigger Conditions** you can refine the trigger condition depending on the trigger data point class.

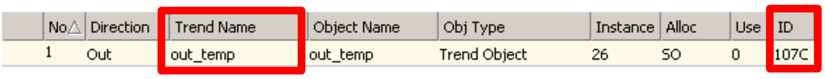
When done with the data point setup, click **Save Changes** to leave the dialog

6.14.4 Download Trend Data in CSV Format

Trend logs can be downloaded from the device via FTP in CSV format (see Section 7.1.2). The CSV contents are generated on-the-fly from the internal binary storage when accessing the file. Each trend log point has one CSV file. The files are located in

`/data/trend/`*TrendLogName_UID*`.csv`

Where *TrendLogName* is the data point name of the trend (Trend Name). The *UID* is the unique ID of the trend log object. The UID can be obtained from the ID column in the data point list of trend log data points as shown in Figure 109. This would result in the trend CSV file '`/data/trend/out_temp_107C.csv`'.



No△	Direction	Trend Name	Object Name	Obj Type	Instance	Alloc	Use	ID
1	Out	out_temp	out_temp	Trend Object	26	SO	0	107C

Figure 109: UID of data points.

Because the contents are generated on-the-fly, the file size in the FTP client will appear as 0 Bytes. The decimal point and CSV column separator can be configured over in the system configuration of the Web UI (see Section 4.2.1) of the L-Gate. Note, that for a comma "," as the separator, the decimal point is a point. This is useful for English/U.S. applications. For countries that use the comma as the decimal point, select the semicolon as the CSV separator.

6.14.5 Deliver Trend Data via E-Mail

Trend logs can be downloaded from the device via FTP. This requires an active action by the user. Alternatively, trend data can be sent as an e-mail attachment. For doing that, an e-mail template has to be setup for the trend log to be transmitted. The fill-level condition in the trend object can be used as a trigger to send an e-mail with the trend's data logger CSV file as an attachment.

For setting up e-mails, the account information has to be configured on the device, e.g., on the Web UI (see Section 4.2.11). Then an e-mail template can be created and the trend object attached as a trigger.

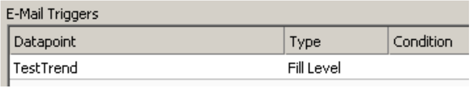
To Create an E-mail Template for Trends

1. Create or configure an e-mail template as described in Section 6.11.1.

2. Change to the **Mail Triggers** tab.

3. Click the **Add…** button and select a trend object.

4. In the **Mail Triggers** list, the added trigger data point appears with the **Fill Level** condition.

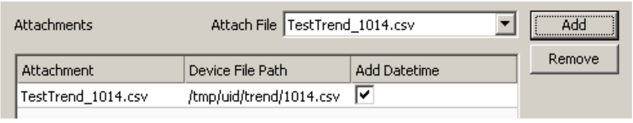


Datapoint	Type	Condition
TestTrend	Fill Level	

5. Change to the **Attachments** tab.

6. Select the trend log CSV file of the trend object in the **Attach File** drop-down box and click **Add**.

Note: *ZIP versions of the CSV files are also available. Select those to save transmission bandwidth and mailbox space.*



Attach File: TestTrend_1014.csv

Attachment	Device File Path	Add Datetime
TestTrend_1014.csv	/tmp/uid/trend/1014.csv	☑

7. Click **OK** to complete the e-mail template configuration.

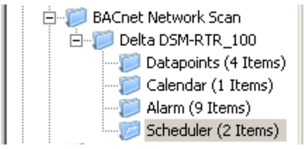
6.15 Remote AST Objects

6.15.1 Remote Scheduler and Calendar

Adding remote access to the configuration of a scheduler and calendar, which is located on another device, is done by creating remote scheduler and calendar objects. These objects can be created from data obtained by a network scan or LNS scan.

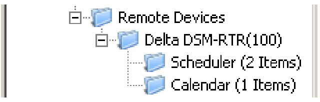
To Create a Remote Scheduler

1. Execute a network scan, as described earlier in this document. The scan folder is filled with available schedulers.



2. From the data points in the import folder, select the scheduler objects you are interested in and click the **Use on Device** speed button. This creates suitable

remote scheduler and the corresponding calendar objects in the **Remote Devices** folder.



3. Adjust the basic settings for the newly created objects, such as the object name and description. The object name will be used as the name for the scheduler, as seen on the Web UI.

4. For BACnet, also adjust the poll cycle, which will be used to periodically fetch the current configuration in case the remote device does not support COV subscriptions.

5. For CEA709, a static NV is created to receive information from the remote device about changes to the scheduler configuration, so that the local device does not need to poll the remote device. Set a name for this NV (default is nviSchedLink<number>) and assign it to a suitable function block.

On BACnet devices, the new data points can be used right away to exchange configuration data with the scheduler on the remote device. Just connect the new scheduler data point to a schedule control to view and edit the configuration of the remote devices scheduler.

On CEA709 devices, there is one extra step to take before the new data points will be operational: The new input NV representing the remote calendar on the local device (this NV is normally called *nviCalLink*) needs to be bound to the output NV called *nvoCalLink* located in the Calendar functional block of the remote device and the new static *nviSchedLink* NVs which were created for each remote scheduler point need to be bound to the respective *nvoSchedLink* variable located in the Scheduler functional block of the remote device. The binding between the *nvoSchedLink* variable on the remote device to the *nviSchedLink* variable on the local device defines which of the scheduler data points on the local device connect to which scheduler unit on the remote device. All required information is transmitted over the link NVs, so it is possible to later change the binding to any other remote scheduler without rescanning the network.

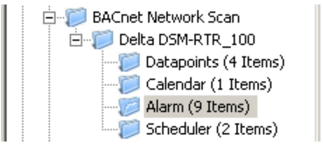
Note: *If connected via LNS, the bindings to the nvoCalLink and nvoSchedLink NVs are made automatically by the configuration software in the download process.*

6.15.2 Alarm Clients

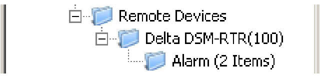
Accessing alarm server objects on remote devices is done by creating remote alarm data points. These points may be created from data obtained by a network scan. The local device is configured as an alarm client and subscribes to alarm updates from the remote alarm server. The alarm client can also be used to acknowledge alarms on the remote alarm server. Any updates are synchronized back to the alarm client.

To Create an Alarm Client

1. Execute a network scan, as described earlier in this document. The scan folder is filled with available remote alarm servers.



2. From the points in the import folder, select the alarm server points you are interested in and click the Use on Device speed button. This creates the corresponding alarm client points in your project.



Remote Devices
Delta DSM-RTR(100)
Alarm (2 Items)

3. For CEA709, select the new alarm client point and adjust the name of the local NV (default name is nviAlarm_2). This NV is located in the Clients functional block.

On BACnet devices, the new data points can be used right away to exchange alarm information with the alarm server on the remote device. Just connect the new alarm client data point to an alarm list control to view and acknowledge alarms reported by the associated alarm server.

On CEA-709 devices, there is one extra step to take before the new data points will be operational: The new static input NVs representing the alarm clients on the local device need to be bound to the alarm outputs of the remote device. A CEA709 device normally delivers alarms through an output NV of type *SNVT_alarm_2* located in the node object of the device, therefore the new input NV on the local device must be bound to the alarm output NV of the remote devices node object. All required information is transmitted over the alarm input NV, so it is possible to later bind the alarm client to any other alarm server without rescanning the network.

Note: *If connected via LNS, the binding to the nvoAlarm2 NV is made automatically by the configuration software in the download process.*

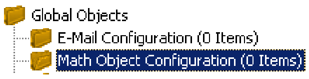
6.16 Math Objects

6.16.1 Create a Math Object

Math objects are advanced application objects that can execute mathematical operations on data points. A math object takes a number of input data points (variables v_1, v_2, …, v_n) and calculates a result value according to a specified formula. When configuring a math object, the input data points, output data points and the formula must be configured by the user. Input data points can be configured with a change-of-value condition, to trigger the math calculation only if the value changes more than a certain delta.

To Create a Math Object

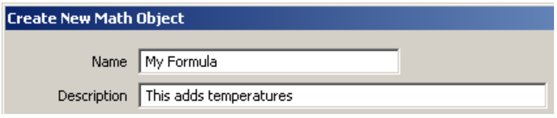
1. Under the **Global Objects** folder, select the **Math Object** sub-folder.



Global Objects
E-Mail Configuration (0 Items)
Math Object Configuration (0 Items)

2. Right-click and select **New Math Object …** from the context menu.

3. In the **Create New Math Object** dialog, enter a name and optionally a description for the math object.

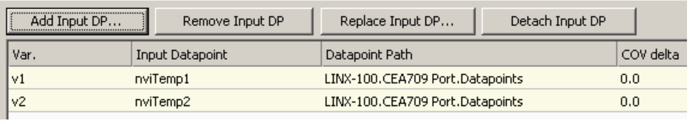


Create New Math Object

Name: My Formula

Description: This adds temperatures

4. Attach input data points by clicking the **Add Input DP** button.

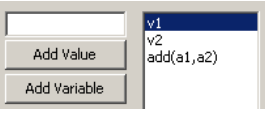


Var.	Input Datapoint	Datapoint Path	COV delta
v1	nviTemp1	LINX-100.CEA709 Port.Datapoints	0.0
v2	nviTemp2	LINX-100.CEA709 Port.Datapoints	0.0

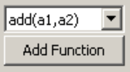
5. In the data point selector dialog, select the input data points and click **OK**. The data points appear as v1, v2, etc.

6. If the data point shall trigger the math calculation only after a certain change-of-value, enter a value into the **COV delta** column.

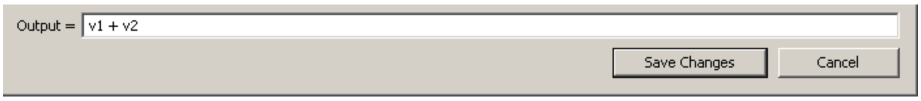
7. Select the input data point and click **Add Variable** to push the variable on the evaluation stack.



8. Select a function to be applied on the variables and click the **Add Function** button.

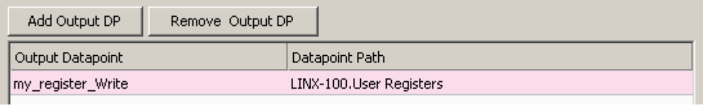


9. The resulting formula is displayed at the bottom of the dialog. Alternatively, the formula can be entered there.



Output = v1 + v2

10. Add output data points by clicking the **Add Output DP button**.



Output Datapoint	Datapoint Path
my_register_Write	LINX-100.User Registers

11. In the data point selector dialog select the output data points and click **OK**.

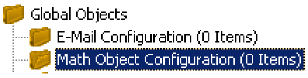
12. To create the math object click **Create**.

6.16.2 Editing a Math Object

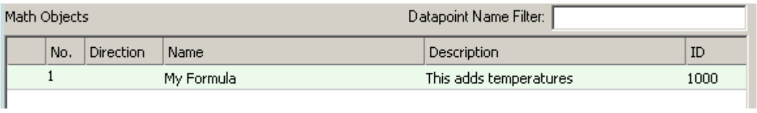
Math objects can be edited once created. The formula can be changed, new variables added, or additional output data points added.

To Edit a Math Object

1. Under the **Global Objects** folder, select the **Math Object** sub-folder.


Global Objects
E-Mail Configuration (0 Items)
Math Object Configuration (0 Items)

2. Select the math object in the data point list.



No.	Direction	Name	Description	ID
1		My Formula	This adds temperatures	1000

3. Right-click and select **Configure Math Object …** from the context menu.

4. Edit the math object as described in Section 6.16.1.

5. To replace an input data point by another input data point without re-writing the entire formula, click the **Replace Input DP …** button. This opens a data point selector dialog. Select the replacement data point there.

6. To detach an input data point click the **Detach Input DP** button. This leaves the respective variable slot empty.

7. To finalize the edit click on **Save Changes**

6.17 Mapping CEA-709 and BACnet Schedules

6.17.1 Mapping and Limitations

Mapping schedulers and calendars is realized by creating connections between schedulers, and connections between corresponding calendars. The information in a scheduler connection is synchronized between its participants. When starting up, however, it is important to define where the source of the information is located, i.e., the actual execution of the schedule takes place. If the schedules and calendars are out-of-sync when the system starts, the information from the source schedule/calendar is distributed in the system. The hub of a connection is always the source of the information. The targets receive the initial schedules/calendars.

In the configuration software, only local schedulers and calendars that are hub in a connection can be configured. The target schedules are synchronized automatically on the device. Changing schedules or calendars on the Web UI or over the network automatically synchronize the change with all members of the connection.

Since schedules and calendars in the two technologies have their own restrictions, the mapping underlies a number of restrictions as well:

- Only schedules that schedule a single value can be mapped. In practice, all schedules can be mapped where one only value can be defined per value preset, e.g., one analog value.
- The target schedule, which is used to expose the actual scheduler to a different technology, must not itself have data points attached, that are scheduled. The target scheduler only acts as a shell that stores the daily schedules.
- CEA-709 schedulers, which schedule only one NV, but that NV is a structure (e.g., SNVT_switch) cannot be mapped to a BACnet scheduler. This is because the value preset on the CEA-709 scheduler has two values to configure. This violates the one-value rule.
- All calendars referred to by mapped schedulers must be added to a calendar connection.
- On one port, only one calendar can exist. Therefore, all exposed calendars must be added to a single connection. As a consequence all calendars are synchronized in the system. There can exist only one calendar connection on a device, that contains all exposed calendars.

- Once a scheduler is in a connection, do not change its scheduled data points. Doing so after creating may violate the connection rules and result in a non-functioning connection.

Figure 110 shows an example, how two remote CEA-709 schedulers are exposed to BACnet schedulers. There are three connections involved. One connection *sched_1_conn* is created for *lon_sched_1* and *bac_sched_1*. A second connection *sched_2_conn* is created for *lon_sched_2* and *bac_sched_2*. Since there is only one BACnet calendar, all calendar objects must be put into a single connection *cal_conn*, containing *lon_cal_1*, *lon_cal_2*, and *bac_cal*.

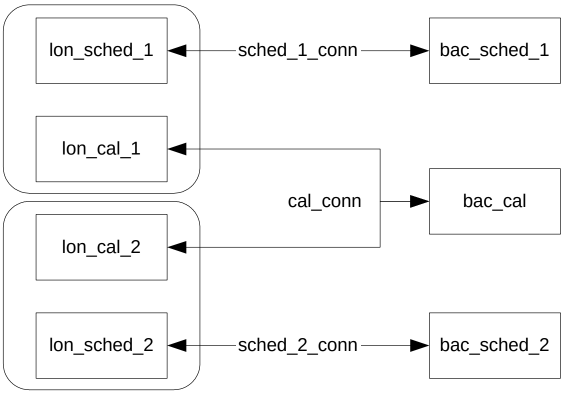


Figure 110: Example for schedule and calendar connections.

6.17.2 Map from CEA-709 to BACnet

This section describes how to expose a CEA-709 scheduler and calendar to a BACnet operator workstation (OWS). It is assumed that the CEA-709 scheduler is either a local or a remote scheduler on the L-Gate and schedules only one value. That CEA-709 scheduler must be the hub.

To Expose a CEA-709 Schedule to BACnet

1. Prepare a CEA-709 schedule object to be exposed (local as in Section 6.12 or a remote scheduler as in Section 6.15.1 from the Remote Devices folder)

2. Create a local BACnet scheduler as in Section 6.12. Do not attach data points to that scheduler.

3. Create a new connection (see Section 6.9.1). Give it a descriptive name, e.g. sched_conn.

4. Select the CEA-709 schedule object as the hub.

5. Select the BACnet scheduler as the target.

6. Click **Save**. Now a scheduler connection appears in the connections list.

Important: ***Once a scheduler is in a connection, do not change the scheduled data points!***

7. Create a local BACnet calendar object, if not existing yet. Add the required number of calendar patterns, i.e., the number of calendar patterns used in the CEA-709 calendar. It is recommended to allocate a number of spare calendar patterns, too. This can be handy, because BACnet calendars cannot dynamically add calendar patterns at run-time, while CEA-709 calendars can. Do not specify names for the calendar patterns.

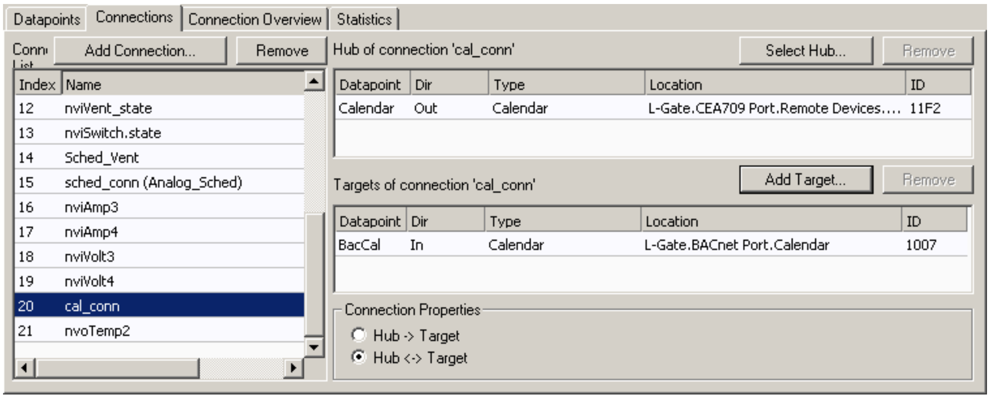
8. Create a second new connection. Give it a descriptive name, e.g., cal_conn.

Important: ***If there already exists a calendar connection, don't create a new connection and add the exposed calendar as a target to the existing connection! There can only be one calendar connection that contains all exposed calendars.***

9. Select the CEA-709 calendar as the hub. When exposing a remote schedule, select the calendar from the same remote device folder where the schedule was selected from.

10. Select the created BACnet calendar as the target.

11. Click **Save**. Now a calendar connection appears in the connections list as shown in Figure 111.



Index	Name
12	nviVent_state
13	nviSwitch.state
14	Sched_Vent
15	sched_conn (Analog_Sched)
16	nviAmp3
17	nviAmp4
18	nviVolt3
19	nviVolt4
20	cal_conn
21	nvoTemp2

Hub of connection 'cal_conn'

Datapoint	Dir	Type	Location	ID
Calendar	Out	Calendar	L-Gate.CEA709 Port.Remote Devices....	11F2

Targets of connection 'cal_conn'

Datapoint	Dir	Type	Location	ID
BacCal	In	Calendar	L-Gate.BACnet Port.Calendar	1007

Connection Properties

○ Hub -> Target

● Hub <-> Target

Figure 111: Calendar connection CEA-709 to BACnet.

6.17.3 Map from BACnet to CEA-709

This section describes how to expose a BACnet scheduler and calendar to a CEA-709 network. It is assumed that the BACnet scheduler is either local or remote. That BACnet scheduler must be the hub.

To Expose a BACnet Schedule to CEA-709

1. Prepare a BACnet schedule object to be exposed (local as in Section 6.12 or a remote scheduler as in Section 6.15.1 from the Remote Devices folder)

2. Create a local CEA-709 scheduler as in Section 6.12. Do not attach data points to that scheduler.

3. Create a new connection (see Section 6.9.1). Give it a descriptive name, e.g. sched_conn.

4. Select the BACnet schedule object as the hub.

5. Select the CEA-709 scheduler as the target.

6. Click **Save**. Now a scheduler connection appears in the connections list.

Important: ***Once a scheduler is in a connection, do not change the scheduled data points!***

7. Create a local CEA-709 calendar object, if not existing yet. Do not add any calendar patterns.

Important: ***If there already exists a calendar connection, don't create a new connection and add the exposed calendar as a target to the existing connection! There can only be one calendar connection that contains all exposed calendars.***

8. Create a second new connection. Give it a descriptive name, e.g., cal_conn.

9. Select the BACnet calendar as the hub. When exposing a remote schedule, select the calendar from the same remote device folder where the schedule was selected from.

10. Select the created CEA-709 calendar as the target.

11. Click **Save**. Now a calendar connection appears in the connections list.

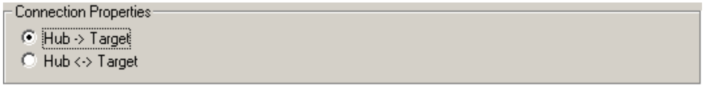
6.17.4 Create One-Way Mappings

A one-way mapping lets schedules and calendar patterns be updated in one direction only: From the hub to the target(s). If a schedule in the hub is updated, the targets receive the new schedule. If a target schedule is updated, however, the change remains local to this scheduler. The local change is overwritten the next time the hub schedule is updated again. This feature is convenient to distribute calendar patterns and schedules from a central location (e.g., the BACnet OWS) but allow temporary, local modifications at the same time.

To Create a One-Way Mapping

1. Create a schedule and/or calendar mapping.

2. Select the created connection and select the radio button hub → target in the **Connection Properties**.



Connection Properties

● Hub -> Target

○ Hub <-> Target

7 Operating Interfaces

7.1 Common Interface

7.1.1 Schedule and Calendar XML Files

The daily schedule and calendar pattern configuration can be changes at run-time over the Web UI or the network. An alternate way to change that configuration is to download a schedule and calendar XML file via FTP onto the device. After the file has been downloaded, the new configuration becomes effective immediately. The device does not need to be rebooted. The files are located in

```
/tmp/uid/sched/UID.xml
/tmp/uid/cal/UID.xml
```

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in Figure 109. A schedule data point with UID 107C would result in the schedule XML file '`/tmp/uid/sched/107C.xml`'. The UID remains constant for the life time of the data point even when the name or description is changed.

The content of the XML file must be compliant to the scheduleCfg schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace 'http://www.loytec.com/xsd/scheduleCfg/1.0/'.

7.1.2 Trend Log CSV File

The CSV file format for a trend log and the location of those files are defined in this section. The trend log CSV files are accessible either via their UID only, or in combination with contents of the trend log object name. The files are located in

```
/tmp/uid/trend/UID.csv
/data/trend/Datapointname_UID.csv
```

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in Figure 109. For a more user-friendly listing of the files, the *Datapointname* contains the trend log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the trend object 'trend0' and the UID '107C' would result in the CSV file '`/data/trend/trend0_107C.csv`'. The UID remains constant for the life time of the object even when the name is changed.

The CSV file format for a trend log is defined in this section. The CSV file starts with a header, containing at least the first line, which specifies the CSV format (log_csv_ver). The current version is 2. The next line contains the field log_device. It has trailing fields that specify the vendor, product code, firmware version and device ID string. The Device ID String can be one of the following: (IP) 192.168.24.100, (BACnet Device) 224100, (CEA-709 NID) NID.

The log_info line specifies the fields UID and name of the trend log object. The line log_create has two fields specifying the date and time when this CSV log was generated. The line log_capacity has two fields: the current number of log entries in the file and the log capacity.

Following are one or more lines of log_item. Each line specifies a trended data point. The first field is the index, the second the ID of the logged data point, the third the data point name. The data point name can be augmented by engineering units in square brackets. Log entries in the CSV refer to the item index to identify the data point, for which the entry was logged.

```
#log_csv_ver;2
#log_device;LOYTEC;Product Code;Firmware Version;Device ID String; Serial No
#log_info;Log-ID;Log Name
#log_create;YYY-MM-DD;HH:MM:SS
#log_capacity;filled;capacity
#log_item;index;UID;data point name [units]
```

After those lines any number of comment lines starting with a hash character '#' are allowed. One line contains the column headings. Lines that are not comments specify one log record per line, using the column information as described below. The columns are separated by commas ',' or semi-colons ';'. If commas are used as a separator, the decimal point must be a point '.'. If semi-colons are used, the decimal point must be a comma ','.

There are as many value columns as value sources specified in the header. If at a given date/time more values are logged, all of them appear in the same line. If at that given time some sources did not log values, those columns are left empty.

Column	Field	Example	Description
A	Sequence Number	50	The log record sequence number. This is the monotonously increasing sequence number, which is unique for each log record.
B	Source	0	Data point source identifier. Indexes into logger_entry header. For value lines in a multi-column CSV, this field indexes the first column, which has a value. For the ERROR record type, the field indexes the data source that caused the error. For LOGSTATE, TIMECHANGE records this field is not applicable and can be left at zero.
C	Record Type	2	The record type: LOGSTATE (0), BOOL (1), REAL (2), ENUM (3), UNSIGNED (4), SIGNED (5), NULL (7), ERROR (8), TIMECHANGE (9)
D	Error/Time Change/Log Status	1	This field is valid for records of type ERROR, TIMECHANGE, and LOGSTATUS.
E	Date/Time	2007-11-02 15:34:22	The date/time of the log record. This is in the format YYYY-MM-DD HH:MM:SS.
F	Value 0	24,5	Logged value from source 0 or empty
G	Value 1	200	Logged value from source 1 or empty
…	…		
…	Value *n* – 1	5000	Logged value from source *n* – 1 or empty

Table 8: Columns of the Trend Log CSV File

There are as many value columns as value sources specified in the header. If at a given date/time more values are logged, all of them appear in the same line. If at that given time some sources did not log values, those columns are left empty. The "Source" column in a multi-value CSV refers to the first data source that supplied a value in a given line.

7.1.3 Alarm Log CSV File

The historical alarm logs are also accessible as CSV-formatted files. The alarm log CSV files are accessible either via their UID only, or in combination with contents of the alarm log object name. The files are located in

```
/tmp/uid/allog/UID.csv
/data/allog/Alarmlogname_UID.csv
```

The *UID* is the unique ID of the alarm log object. The UID can be obtained from the ID column in the data point list of the alarm log folder, similar to obtaining the UID of trend log objects. For a more user-friendly listing of the files, the *Alarmlogname* contains the alarm log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the alarm log object 'alarmlog0' and the UID '100C' would result in the CSV file '`/data/allog/alarmlog0_100C.csv`'. The UID remains constant for the life time of the object even when the name is changed.

The CSV format of the alarm log CSV file is identical to the trend log CSV format as described in Section 7.1.2.

7.2 CEA-709 Interface

7.2.1 NV Import File

Network variables can be imported to the Gateway configuration software in a CSV file. The format of this file is described in this section.

The first line of the file must contain a comment, starting with a hash character '#' specifying the format version and import technology:

```
#dpal_csv_config;Version=1;Technology=CEA709
```

After that line any number of comment lines starting with a hash character '#' are allowed. Lines that are not comments specify one NV per line, using the column information as described in Table 9. The columns are separated by commas ',' or semi-colons ';'. Which separator is used can be configured in the Web UI (see Section 4.2.1).

Column	Field	Example	Description
A	SNVT	39	A numeric value of the SNVT (as defined in the SNVT master list). The example value 39 represents a SNVT_temp.
B	NV index	0	The NV index in decimal of the NV on the network node. Indices start at 0.
C	NV selector	1	The NV selector in decimal of the NV on the network node.
D	NV name	nvoTemp	The NV programmatic name of the NV on the network node.
E	is output	1	Defines if this NV is an output on the network node. ‘1’ means the NV is an output on the network node.
F	flag auth cfg	1	‘1’ defines that authentication can be configured for this NV on the network node.
G	flag auth	0	‘1’ defines that the NV is authenticated.
H	flag priority cfg	1	‘1’ defines that the priority can be configured for this NV on the network node.
I	flag priority	0	‘1’ defines that the NV is using priority.
J	flag servicetype cfg	1	‘1’ defines that the service type can be configured for this NV on the network node.
K	flag service ack	1	‘1’ defines that the NV is using acknowledged service.
L	flag polled	0	‘1’ defines that the NV is using the polled attribute
M	flag sync	0	‘1’ defines that the NV is a synchronous NV.
N	deviceref	1	This field is a numeric reference to a device description. If it is the first occurrence of this reference in the file, the columns defined below must be filled in. Otherwise, they can be left out.
O	programID	9000A44850060402	The program ID string of the network device.
P	neuronID	80000000C8C8	The NID of the network device.
Q	subnet	2	The subnet address of the network device. Use ‘0’ if the device has no subnet address information.
R	node	3	The node address of the network device. Use ‘0’ if the device has no node address information.
S	location str	0	The location string of the network device. Use ‘0’ if no information is available.
T	devicename	DDC	The device name of the network device. Leave this field blank if this information is not available.
U	node self-doc	&3.2@0,2	Self-documentation string of the device (special characters are escaped)
V	NV length	2	NV length in bytes
W	NV self-doc	@0|4	NV self-documentation string (special characters are escaped)
X	allocation	1	Define, how this NV shall be allocated: external=1 (default) /static=2/file=3

Table 9: CSV Columns of the NV Import File

7.2.2 Node Object

The L-Gate provides a node object conforming to the LONMARK guidelines. A diagram of the node object is depicted in Figure 112.

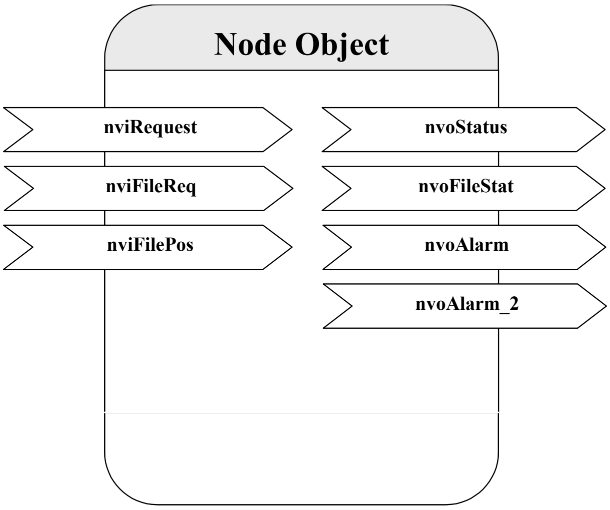


Figure 112: Node Object

- The Node Object accepts the following commands via *nviRequest*:
  - RQ_NORMAL
  - RQ_UPDATE_STATUS
  - RQ_REPORT_MASK
  - RQ_ENABLE
  - RQ_DISABLE
  - RQ_UPDATE_ALARM
  - RQ_CLEAR_ALARM
  - RQ_RESET
  - RQ_CLEAR_RESET
- LONMARK alarming is supported via *nvoAlarm* (SNVT_alarm) and *nvoAlarm_2* (SNVT_alarm_2). This allows devices supporting the LONMARK alarm notifier profile to receive alarms generated by the L-Gate and react with a defined action (e.g. send an email). By supporting both alarm SNVTs, SNVT_alarm and SNVT_alarm_2, legacy and state-of-the-art alarm handling is supported.

7.2.3 Extended Node Object Interface

When any of the AST features is enabled in the project settings, the node object contains some extensions.

- nviDateEvent (*SNVT_time_stamp*), nvoDateResync (*SNVT_switch*): These NVs are part of the standard LONMARK node object, if schedulers are used. If not bound, the local calendar is used. If a global calendar shall be used, both of these NVs must be bound to the respective NVs of the global calendar object.
- nviTimeSet (*SNVT_time_stamp*): When writing to this NV, the system is set. The time value is interpreted as local time.
- nvoSystemTemp (*SNVT_temp*): This NV can be used to poll the system temperature of the L-Gate. It does not send updates and must be polled.
- nvoSupplyVolt (*SNVT_volt*): This NV can be used to poll the supply voltage of the L-Gate. It does not send updates and must be polled.
- nvoIpAddress (*SNVT_str_asc*): This NV can be used to poll the IP address of the L-Gate. It does not send updates.

- nciEarthPos (*SNVT_earth_pos*): This configuration property can be used to set the earth position of the L-Gate. It has been implemented as an NV to make other devices send that configuration to the L-Gate over the network (e.g., from a GPS device).

7.2.4 Real-Time Keeper Object

When the scheduler objects are enabled in the project settings, the L-Gate includes the standard LONMARK real-time keeper object. The Real-Time Keeper Object is used to synchronize the system time of multiple LonMark compliant devices.

The object has the following network variables:

- nvoTimeDate (*SNVT_time_stamp*): Propagates the devices current system time and date (local time). It is typically bound to the nviTimeSet input network variable of the node objects of the LonMark compliant devices, which are synchronized with the system time of the L-Gate. The update rate of the nvoTimeDate can be configured using the configuration property SCPTupdateRate (default every 60 seconds).

7.2.5 Calendar Object

When the scheduler objects are enabled in the project settings, the L-Gate includes the standard LONMARK calendar object.

7.2.6 Scheduler Object

When the scheduler objects are enabled in the project settings, the L-Gate includes the configured number of standard LONMARK scheduler objects.

7.2.7 Clients Object

When the remote AST object feature is enabled in the project settings, the L-Gate includes a proprietary object, which is a container for network variables required to implement the remote object features.

For remote schedulers and calendars, *nviSchedLink* and *nviCalLink* NVs are created. For alarm clients nviAlarm_2 NVs are created.

7.2.8 Gateway Objects

The L-Gate contains eight proprietary Gateway objects. These are containers for all NVs, which are configured on the L-Gate’s CEA-709 port. They are intended for grouping NVs. When static NVs are created, they can be assigned to any of the eight gateway blocks. When creating dynamic NVs in the LNS-based tool, the NVs should be added to the gateway blocks.

7.3 BACnet Interface

7.3.1 Device Object

The BACnet interface provides one device object as shown in Table 10.

Property Identifier	**Property Datatype**	**Conformance Code**
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
System_Status	BACnetDeviceStatus	R
Vendor_Name	CharacterString	R
Vendor_Identifier	Unsigned16	R
Model_Name	CharacterString	R
Firmware_Revision	CharacterString	R
Application_Software_Version	CharacterString	R
Location	CharacterString	R
Description	CharacterString	R
Protocol_Version	Unsigned	R
Protocol_Revision	Unsigned	R
Protocol_Services_Supported	BACnetServicesSupported	R
Protocol_Object_Types_Supported	BACnetObjectTypesSupported	R
Object_List	BACnetARRAY[N]of BACnetObjectIdentifier	R
Max_APDU_Length_Accepted	Unsigned	R
Segmentation_Supported	BACnetSegmentation	R
Max_Segments_Accepted	Unsigned	R
APDU_Segment_Timeout	Unsigned	R
APDU_Timeout	Unsigned	R
Number_Of_APDU_Retries	Unsigned	R
Max_Master	Unsigned(1..127)	R
Max_Info_Frames	Unsigned	R
Device_Address_Binding	List of BACnetAddressBinding	R
Database_Revision	Unsigned	R
Active_COV_Subscriptions	List of BACnetCOVSubscription	R
Profile_Name	CharacterString	R

Table 10: Properties of the Device Object

7.3.1.1 Object_Identifier (Read-Only)

This property, of type “BACnetObjectIdentifier”, is a numeric code that is used to identify the object. For the Device object, the object identifier is unique internetwork-wide.

The “Object Type” part of the “Object_Identifier” is 8 (=device). The “Instance” part of this property is configurable via the configuration UI (see Section 4.2.7). The default value for the “Instance” part is 17800.

7.3.1.2 Object_Name (Read-Only)

The value of this property is configurable via the configuration UI (see Section 4.2.7). The default value is “L-Gate”. Note that this name must be unique in the BACnet internetwork.

7.3.1.3 Object_Type (Read-Only)

The value of this property is DEVICE (8).

7.3.1.4 System_Status (Read-Only)

The value of this property is always OPERATIONAL.

7.3.1.5 Vendor_Name (Read-Only)

The value of this property is “LOYTEC electronics GmbH”.

7.3.1.6 Vendor_Identifier (Read-Only)

The value of this property is 178.

7.3.1.7 Model_Name (Read-Only)

The value of this property is equal to the product code of the device (“LGATE-900”).

7.3.1.8 Firmware_Revision (Read-Only)

The value of this property gives the current firmware version of the device.

7.3.1.9 Application_Software_Version (Read-Only)

The value of this property gives the build date and the version of the current firmware.

7.3.1.10 Location (Read-Only)

This property is configurable via the configuration UI (see Section 4.2.7). The default value is “unknown”.

7.3.1.11 Description (Read-Only)

This property is configurable via the configuration UI (see Section 4.2.7). The default value is “L-Gate”.

7.3.1.12 Protocol_Version (Read-Only)

The value of this property is 1.

7.3.1.13 Protocol_Revision (Read-Only)

The value of this property is 4.

7.3.1.14 Protocol_Services_Supported (Read-Only)

For the services supported please refer to the LGATE-900 PICS document.

7.3.1.15 Protocol_Object_Types_Supported (Read-Only)

For the supported object types please refer to the LGATE-900 PICS document.

7.3.1.16 Object_List (Read-Only)

This read only property is a BACnetARRAY of “Object_Identifiers”, one “Object_Identifier” for each object within the device that is accessible through BACnet services (see below).

7.3.1.17 Max_APDU_Length_Accepted (Read-Only)

The value of this property is 487 if BACnet MS/TP is used and 1473 if BACnet/IP is used.

7.3.1.18 Segmentation_Supported (Read-Only)

The value of this property is SEGMENTED_BOTH.

7.3.1.19 Max_Segments_Accepted (Read-Only)

The value of this property is 16.

7.3.1.20 APDU_Segment_Timeout (Read-Only)

The value of this property is 2000 milliseconds.

7.3.1.21 APDU_Timeout (Read-Only)

The value of this property is 3000 milliseconds.

7.3.1.22 Number_Of_APDU_Retries (Read-Only)

The value of this property is 3.

7.3.1.23 Max_Master (Read/Write)

This property is only present in case BACnet MS/TP is used. The value of this property is configurable via the configuration UI (see Section 4.2.7). The default value of this property is 127.

7.3.1.24 Max_Info_Frames (Read/Write)

This property is only present in case BACnet MS/TP is used. The value of this property is configurable via the configuration UI (see Section 4.2.7). The default value of this property is 1.

7.3.1.25 Device_Address_Binding (Read-Only)

The “Device_Address_Binding property” is a List of “BACnetAddressBinding” each of which consists of a BACnet “Object_Identifier” of a BACnet Device object and a BACnet device address in the form of a “BACnetAddress”. Entries in the list identify the actual device addresses that will be used when the remote device must be accessed via a BACnet service request.

7.3.1.26 Database_Revision (Read-Only)

This property, of type Unsigned, is a logical revision number for the device's database. It is incremented when an object is created, an object is deleted, an object's name is changed, an object's Object_Identifier property is changed, or a restore is performed.

7.3.1.27 Active_COV_Subscriptions (Read-Only)

The Active_COV_Subscriptions property is a List of BACnetCOVSubscription, each of which consists of a Recipient, a Monitored Property Reference, an Issue Confirmed Notifications flag, a Time Remaining value and an optional COV Increment. This property provides a network-visible indication of those COV subscriptions that are active at any given time. Whenever a COV Subscription is created with the SubscribeCOV or SubscribeCOVProperty service, a new entry is added to the Active_COV_Subscriptions list. Similarly, whenever a COV Subscription is terminated, the corresponding entry is removed from the Active_COV_Subscriptions list.

7.3.1.28 Profile_Name

The value of this property is “178-LGATE”.

7.3.2 Client Mapping CSV File

Client functionality for the BACnet server objects can be defined by so-called “client mappings”. These mappings basically specify whether present value properties shall be written to or polled from the BACnet network, and what the destination address and objects are. These definitions can be downloaded as a CSV file onto the device using FTP.

The CSV file must be named “bacclnt.csv” and stored in the directory “/var/lib/bacnet” on the L-Gate. The file is read when the device boots. If any errors occur they are reported in “/tmp/bacclnt.err”.

The column format is shown in Table 11. Lines beginning with a hash (‘#’) sign are comment lines. The example values in Table 11 setup a client mapping named “Lamp Room 302”, which writes (mapping type 2) the present value of the local object AI,4 to the remote object AO,1 on the device with the instance number 17801.

Column	**Field**	**Example**	**Description**
A	Description	Lamp Room 302	User-defined description of this client mapping. Can be left empty. Don’t use commas or semi-colons in the text!
B	Local Object-Type	AI	The BACnet object type of the local server object (AI, AO, AV, BI, BO, BV, MI, MO, MV)
C	Local Object Instance Number	4	The object instance number of the above object.
D	Remote Device Instance	17801	The device object instance number of the remote BACnet device
E	Remote Object-Type	AO	The BACnet object type of the remote server object (AI, AO, AV, BI, BO, BV, MI, MO, MV)
F	Remote Object Instance Number	1	The object instance number of the above object.
G	Map Type	2	Defines the type of the mapping: 0=Poll, 1=COV, 2=Write
H	Interval/ Priority	8	Defines the poll interval in seconds for poll mappings and the COV lifetime in seconds for COV mappings. For write mappings this defines the write priority (1..16). Omit this field or set it to ‘-1’ to write w/o priority.

Table 11: CSV Columns of the BACnet Client Mappings File

7.3.3 EDE Export of BACnet Objects

The BACnet server object configuration of the L-Gate is accessible as a set of CSV files following the EDE format convention. They can be downloaded via FTP from the directory ‘/data/ede’ on the device. The files are

- lgate.csv: This is the main EDE sheet with the list of BACnet objects.
- lgate-states.csv: This is the state text sheet. For each state text reference in the main sheet, a line contains the state texts for this multi-state object.
- lgate-types.csv: This is the object types text sheet. The file contains a line for each object type number. Note, that lines for standard object types can be omitted.
- lgate-units.csv: This is the unit text sheet. The file contains a line for each engineering unit enumerator value. Note that lines for standard units can be omitted.

8 Network Media

8.1 FT

The L-Gate FT port is fully compatible to the parameters specified by LONMARK for this channel. FT ports can also be used on Link Power (LP-10) channels. However, the L-Gate does not provide the power supply for Link Power channels.

When using the Free Topology Segment feature of the FT, only one termination (Figure 113) is required and can be placed anywhere on the free topology segment. Instead of building the termination, one can order the L-Term module (LT-33) from LOYTEC, which can be used to properly terminate the bus.

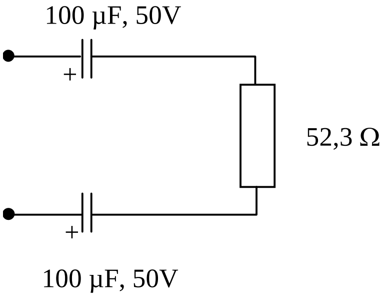


Figure 113: FT Free Topology Termination

In a double terminated bus topology, two terminations are required (Figure 114). These terminations need to be placed at each end of the bus. Here, also L-Term modules can be used at either end.

Fehler! Es ist nicht möglich, durch die Bearbeitung von Feldfunktionen Objekte zu erstellen.

Figure 114: Termination in an FT Bus Topology

9 L-Gate Firmware Update

The L-Gate firmware supports remote upgrade over the network and the serial console.

To guarantee that the L-Gate is not destroyed due to a failed firmware update, the L-Gate firmware consists of two images:

- L-Gate fallback image,
- L-Gate primary image.

The L-Gate fallback image cannot be changed. Thus, if the update of the primary image fails or the image is destroyed by some other means, the fallback image is booted and allows to reinstall a valid primary image.

When the L-Gate boots up with the fallback image, the CEA-709 port LED and the STATUS LED are flashing red.

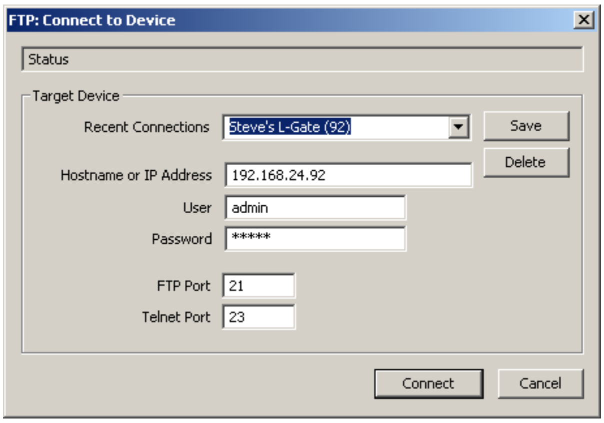
9.1 Firmware Update via the Configurator

The L-Gate primary image can be updated using the Configurator. For this purpose, the device must be connected to the Ethernet and must have a valid IP configuration (see Section 4.2.4). The L-Gate Configurator must be installed (see Section 6.1).

To Update the Firmware using the Configurator

1. Start the L-Gate Configurator from the Windows Start menu: **Start → Programs → LOYTEC L-Gate Configuratior → Configure L-Gate**.

2. Select the menu: **Connection → Connect via FTP**. This opens the FTP connection dialog as shown in Figure 115.



FTP: Connect to Device

Status

Target Device

Recent Connections: Steve's L-Gate (92)

Hostname or IP Address: 192.168.24.92

User: admin

Password: *****

FTP Port: 21

Telnet Port: 23

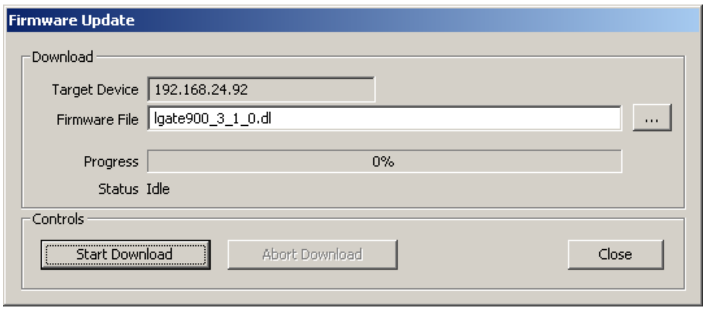
Figure 115: FTP connection dialog.

3. In the FTP connection dialog enter the IP address of the device to upgrade and the FTP user name and password. The default user name and password are ‘admin’ and ‘admin’. This can be changed via the Web interface (see Section 4.1) and reset via the console UI (see Section 10.2.2).

4. Click on **Connect**.

5. Select the menu: **Firmware → Update …**

6. This opens the Firmware Update dialog as shown in Figure 116. Click on the button “…” and select the firmware image (“lgate900_3_1_0.dl”).



Firmware Update

Download

Target Device: 192.168.24.92

Firmware File: lgate900_3_1_0.dl

Progress: 0%

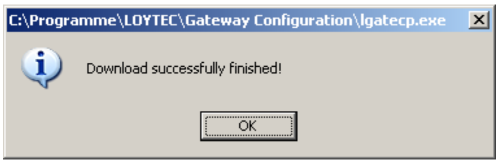
Status: Idle

Controls

Figure 116: Firmware Update dialog of the L-Gateway configuration software.

7. Click on **Start Download**.

8. Observe the download progress. When the download is complete the dialog shown in Figure 117 appears.



C:\Programme\LOYTEC\Gateway Configuration\lgatecp.exe

Download successfully finished!

Figure 117: FTP download success dialog.

9. Click **Ok**.

10. In the Firmware Update dialog click **Close**.

11. The device’s firmware has now been successfully upgraded.

9.2 Firmware Update via the Console

To download the firmware via the console interface, the L-Gate must be connected to the RS-232 port of a PC via its console interface as described in Section 10.2.1. You will need the LOYTEC serial upgrade tool (LSU Tool), which can be downloaded from our homepage at www.loytec.com.

Please make sure that the L-Gate console shows the main menu otherwise navigate to the main menu or simply reset the L-Gate.

To Upgrade via the Console

1. Double click on the *.dlc file that comes with the new firmware package. This should start the LSU Tool and load the firmware image referenced in the dlc file. Please note that the dlc file and the dl file must be stored in the same folder. The start window of the LSU tool is shown in Figure 118.

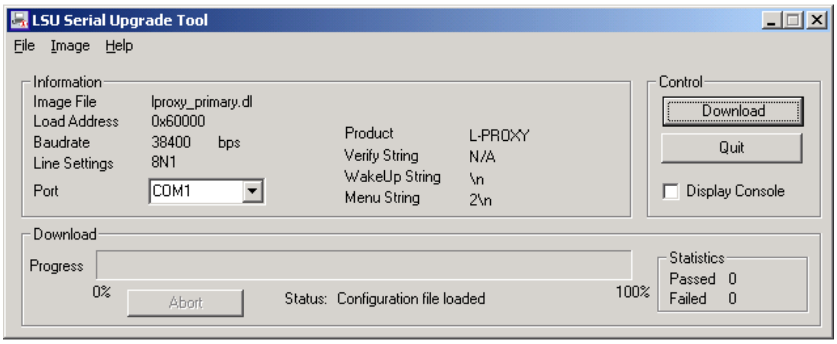


Image File lproxy_primary.dl
Load Address 0x60000
Baudrate 38400 bps
Line Settings 8N1
Port COM1
Product L-PROXY
Verify String N/A
WakeUp String \n
Menu String 2\n
Status: Configuration file loaded
Passed 0
Failed 0

Figure 118: LSU Serial Upgrade Tool in Idle Mode

2. If the L-Gate is not connected to COM1 you can change the port to COM2, COM3, or COM4. Make sure that the product shown under “Product” matches the device you are upgrading. Press **Download** to start the download. A progress bar as shown in Figure 119 can be seen.

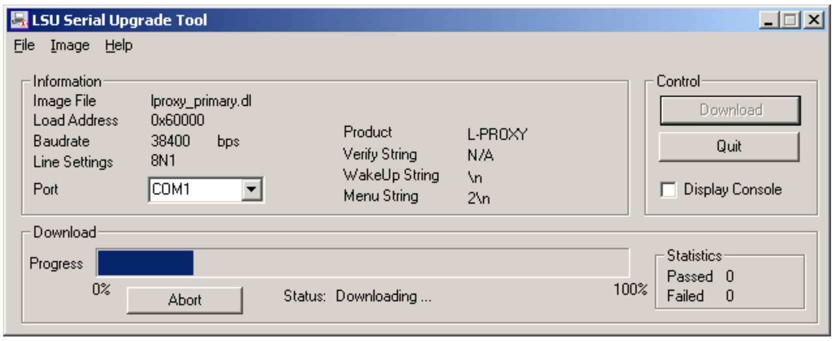
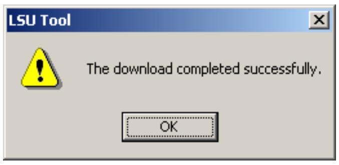


Image File lproxy_primary.dl
Load Address 0x60000
Baudrate 38400 bps
Line Settings 8N1
Port COM1
Product L-PROXY
Verify String N/A
WakeUp String \n
Menu String 2\n
Status: Downloading ...
Passed 0
Failed 0

Figure 119: Progress Bar during Firmware Download.

3. If the upgrade is successful, the following window appears (Figure 120).



The download completed successfully.

Figure 120: Successful Firmware Upgrade

4. Double check that the new firmware is executed by selecting ‘1’ and pressing **Enter** in the console window. This will bring up the device information which shows the current firmware version.

10 Troubleshooting

10.1 Technical Support

LOYTEC offers free telephone and e-mail support for our L-Gate product series. If none of the above descriptions solves your specific problem please contact us at the following address:

LOYTEC electronics GmbH
Blumengasse 35
A-1170 Vienna
Austria / Europe

email :	***support@loytec.com***
web :	***http://www.loytec.com***
tel :	***+43/1/4020805-100***
fax :	***+43/1/4020805-99***

or

LOYTEC Americas Inc.
11258 Goodnight Lane
Suite 101
Dallas, Texas 75229
USA

Email:	***support@loytec-americas.com***
web:	***http://www.loytec-americas.com***
tel:	***+1/512/402 5319***
fax:	***+1/972/243 6886***

10.2 Statistics on the Console

10.2.1 Connecting to the Console

Use a PC terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake. To connect COM1 of the PC to the Console on the device, use a standard null-modem cable with full handshaking. Power up the device or press **Return** if the device is already running. The menu shown in Figure 121 should appear on the terminal.

```
Device Main Menu
================

[1]  Show device information
[2]  Serial firmware upgrade
[3]  System configuration
[4]  CEA-709 configuration
[5]  IP configuration
[6]  CEA-852 device configuration
[7]  BACnet configuration
[8]  Reset configuration (factory defaults)
[9]  Device statistics

[a]  Data Points

[0]  Reset device

Please choose:
```

Figure 121: Console Main Menu.

10.2.2 Reset Configuration (factory defaults)

Select item ‘8’ in the console main menu. This menu item allows resetting the device into its factory default state. The menu appears as shown in Figure 122.

```
Reset Configuration Menu
========================

[1]  Reset everything to factory defaults
[3]  Reset all passwords
[4]  Clear data point configuration

[q]  Quit

Please choose:
```

Figure 122: Reset to Factory Defaults Menu.

Select option ‘1’ to reset the entire device to factory defaults (including error log, configuration files, passwords etc.). Select option ‘3’ to reset all passwords (Web interface, FTP server etc.) to factory defaults.

Select option ‘4’ to clear all configured data points, such as CEA-709 network variables or user registers. This effectively clears the entire port configuration. The device must be rebooted to let the changes take effect.

10.2.3 Device Statistics Menu

Select ‘9’ from the device main menu to get to the device statistics menu. This menu holds relevant information regarding the device statistics of the device. This section describes those statistics, which are not available on the Web UI. The device statistics menu is shown in Figure 123. Use this menu only for debugging purposes. There is no need to access this menu if the network is running smoothly.

```
Statistics Menu
===============

[4]  Show IP statistics
[8]  Show DPAL statistics
[9]  Show Reg DPAL statistics

[q]  Quit

Please choose:
```

Figure 123: Device Statistics Menu on the Console.

10.2.3.1 IP statistics

A sample console output is shown in Figure 124.

```
*********** INTERFACE STATISTICS ************
***** lo0 *****
Address:127.0.0.1
Flags: Up Loopback Running Multicast
Send queue limit:50   length:0    Dropped:0
***** eth0 *****
Address:192.168.0.2     Broadcast Address:192.168.0.255
Flags: Up Broadcast Running Simplex Multicast
Send queue limit:50   length:0    Dropped:0
Network Driver Stats for CS8900 :
        rx ready len -         50        rx loaded len -          0
          rx packets -        931           tx packets -        165
            rx bytes -      78480             tx bytes -      13627
       rx interrupts -        931        tx interrupts -        165
          rx dropped -          0           rx no mbuf -          0
       rx no custers -          0   rx oversize errors -          0
       rx crc errors -          0       rx runt errors -          0
    rx missed errors -          0                tx ok -        165
       tx collisions -          0        tx bid errors -          0
  tx wait for rdy4tx -          0            tx rdy4tx -          0
  tx underrun errors -          0           tx dropped -          2
          tx resends -          0        int swint req -       2094
       int swint res -       2094           int lockup -          0
          interrupts -       3189

************ MBUF STATISTICS ************
mbufs: 512    clusters:  64    free:  14
drops:   0       waits:   0  drains:   0
      free:461          data:51          header:0           socket:0
       pcb:0           rtable:0           htable:0           atable:0
    soname:0           soopts:0           ftable:0           rights:0
    ifaddr:0          control:0          oobdata:0

************ IP Statistics ************
             total packets received         922
 datagrams delivered to upper level         922
    total ip packets generated here         158

Destination     Gateway/Mask/Hw    Flags     Refs     Use Expire
Interface
default         192.168.0.1        UGS         6        0      0 eth0
62.178.55.77    192.168.0.1        UGH         0        1   3606 eth0
62.178.95.96    192.168.0.1        UGH         0        1   3606 eth0
81.109.145.243  192.168.0.1        UGH         0        1   3606 eth0
81.109.251.36   192.168.0.1        UGH         0        1   3606 eth0
127.0.0.1       127.0.0.1          UH          0        0      0 lo0
130.140.10.21   192.168.0.1        UGH         1        6      0 eth0
192.168.0.0     255.255.255.0      U           0        0      3 eth0
192.168.0.1     00:04:5A:26:96:1F  UHL         7        0   1722 eth0
213.18.80.166   192.168.0.1        UGH         1      148      0 eth0
************ TCP Statistics ************

************ UDP Statistics ************
                total input packets         924
               total output packets         158

************ ICMP Statistics ************
```

Figure 124: IP Statistics.

The IP statistics menu has the additional feature of displaying any IP address conflicts. If the device's IP address conflicts with another host on the network, the banner shown in Figure 125 is displayed.

```
WARNING: Conflicting IP address detected!
         IP address 10.125.123.95 also used by device with MAC address
         00 04 5A CC 10 41!

Clear IP conflict history (y/n):
```

Figure 125: IP Address Conflict.

As useful information, the MAC address of the conflicting host is shown. If the information about this conflict shall be cleared, enter 'y'. If 'n' is selected, the conflict will show up again the next time this menu is entered.

11 Application Notes

11.1 The LSD Tool

Please refer to application note “AN002E LSD Tool” for further information about the LOYTEC system diagnostics tool for the L-Gate.

11.2 Use of Static, Dynamic, and External NVs on a Device

Please refer to application note “AN009E Changing Device Interface in LNS” for more information on the static NV interface, XIF files, device templates and the use of static, dynamic, and external NVs on LOYTEC gateway products.

12 Firmware Versions

Table 12 shows the most important features available only in certain firmware versions.

Firmware Version/ Features	1.0.0	1.1.0	1.2.0	3.0.0	3.1.0	3.2.0
CEA-709/BACnet gateway	√	√	√	√	√	√
BACnet Network Scan	-	√	√	√	√	√
CEA-709 Network Scan	-	√	√	√	√	√
UNVTs, SCPTs	-	-	√	√	√	√
XML configuration	-	-	-	√	√	√
Scheduler	-	-	-	√	√	√
Trendlog	-	-	-	√	√	√
Alarming (Intrinsic Reporting)	-	-	-	√	√	√
E-Mail	-	-	-	√	√	√
L-Gate Backup/Restore configuration	-	-	-	-	√	√
Default, Persistent Values	-	-	-	-	√	√
Math Objects & Registers	-	-	-	-	√	√
Schedule/Write parts of NVs	-	-	-	-	√	√
Next state (SNVT_tod_event)	-	-	-	-	√	√
Embedded calendar	-	-	-	-	√	√
Min/max/average trends (CEA-709)	-	-	-	-	√	√
BACnet BBMD	-	-	-	-	√	√
Map all BACnet Properties	-	-	-	-	√	√
CEA-709 Self-Installation	-	-	-	-	√	√
LWEB-801 Support	-	-	-	-	-	√
Run-time Configuration	-	-	-	-	-	√

Table 12: Available Features depending on Firmware Version

13 Specifications

13.1 LGATE-900

13.1.1 Physical Specifications

Operating Voltage	12-35 VDC or 12-24 VAC ±10%
Power Consumption	typ. 3 W
In rush current	up to 950 mA @ 24 VAC
Operating Temperature (ambient)	0°C to + 50°C
Storage Temperature	10°C to +85°C
Humidity (non condensing) operating	10 to 90% RH @ 50°C
Humidity (non condensing) storage	90% RH @ 50°C
Enclosure	Installation enclosure 6 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

13.1.2 Resource Limits

Total number of data points	10000
User registers	1000
NVs (static, dynamic)	1000
External NVs	1000
Alias NVs	1000 (both in ECS and legacy mode)
Address table entries	512 (15 in legacy mode)
LONMARK calendar objects	1 (25 calendar patterns)
LONMARK scheduler objects	100

BACnet objects (analog, binary, multi-state)	750
BACnet client mappings	750
BACnet calendar objects	25
BACnet scheduler objects	100 (64 data points per object)
BACnet notification class objects	32
BACnet trend log objects	100 (total aggregated size of 130000 log records or roughly 2MB.
E-mail templates	100
Math objects	100
Alarm logs	10
Connections	1000

14 Revision History

Date	Version	Author	Description
2006-09-29	1.0	STS	Initial revision V1.0
2007-01-11	1.0.1	STS	Corrected Table 4, 7. Updated Section 2.3, 6.2, 6.3, and 6.4 for L-Gateway configuration software 2.0.
2007-03-16	1.1	STS	Updated Section 4.9.3, added Section 4.11, added Section 5.2.6 on the data point Web UI, rewrote Chapter 6 to cover more use cases, added Chapter 7 on using the L-Gateway configuration software, updated firmware update Section 10.1.
2008-02-08	3.0	STS	Major revision to cover L-Gate 3.0 and L-Gateway configuration software 3.0.
2008-08-04	3.0.1	STS	Updated Section 8.1.2 with new data logger CSV format version 2.
2009-09-22	3.1	STS	Major revision to cover L-Gate and L-Gate Configurator version 3.1.
2010-10-11	3.2	STS	Updated for L-Gate 3.2.0 release. Removed Section on Console UI and added console statistics as Section 10.2. Added Section 4.2.3 port configuration Web UI. Section 6.3 project settings: added new ASTv2 setting. Added Section 6.2.5: Managing Multistate Maps. Added Section 6.2.6 CEA-709 Properties. Added Section 6.2.7 BACnet Properties. Added Section 6.8.3 Using Feedback Data Points.