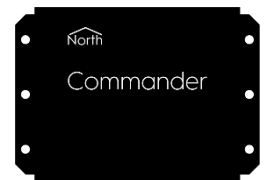




Commander Manual



Commander is the smaller of North's building controllers. Commander contains North's interface technology, block-based programming language, and easy-to-use information services. Commander can work as a stand-alone controller; linked with Commander Hub for easy remote monitoring; or alongside other North controllers and display systems to create a larger control or monitoring solution.

This document relates to Commander Version 2.0, with firmware dated 01/06/26 and after.

Please read the *Commander Tutorial* alongside this document, available from www.northbt.com/cmdr

Contents

What is Commander?	6
Interface Technology	6
Programmable Control	6
Information Services	6
Typical Use	7
Quick Start	8
Mount Commander	8
Set Switches	8
Apply Power	8
Insert the Battery	8
Install North Engineering software	8
Connect PC to Commander	8
Hardware	9
Dimensions	9
Installation	10
Connectors	11
LEDs	11
Power	12
LAN Port	12
RS232 Ports	12
Internal Battery	13
Internal Switches	14
Memory	14
Interface Licences	14
Firmware	15
Main Firmware	15
Interface Driver Firmware	15
Secure by Default	16
Functional Organisation	17
Functions	17
Settings	17
Organisation of this Manual	17
Platform Information	18
Switch Settings	18
Battery Health	18
Default Configuration	18
Reset/Restart Information	18
Software Versions	18
Software Cloud Update	18
Debug Recording	19
LAN Port Setup	20
Default IP Addressing	20
Static IP Addressing	20
Dynamic DHCP Addressing	20
DNS Server Address	20
Time Server Address	20
Real-time Clock and Time Zone	21
Coordinated Universal Time	21
Local Time	21
Daylight Saving Time	21

Interfacing Commander to other Systems	22
Started Interfaces	22
Installed Drivers	22
Interface Licences	22
Transferring Values	23
Reading the Value	23
Writing the Value	23
Transfer Tasks	23
Essential Data	24
Structure	24
Pages	24
Objects	24
Value Reading and Writing	25
Adjustability	25
Alarm Monitoring	25
Value Logging	25
Commander Hub	25
Controlling using Time and Date	26
Calendar	26
Timers	26
Profilers	26
ObVerse	26
ObVerse Cause-and-Effect Strategy	27
Properties	27
Modules	27
Editing ObVerse	27
Alarm Basics	28
Format	28
Alarm Delivery	28
History of Alarms	28
Emailing Alarms	29
Alternative Alarm Destinations	29
Communicating with other North IP Devices	30
Securing North IP Device Access	30
Checking Communications	31
DEFAULTIP Switch	31
Web Server	32
Overview Page	32
Values Page	33
Events Page	33
Device Information Page	33
Security Settings	33
DEFAULTIP Switch	33
Commander Hub	34
Data Collection	34
Keeping it Secure	34
High Availability Servers	34
Easy to Connect	34
My Hub	35

Security Server	36
User Information.....	36
Groups	36
Use by other Tasks.....	36
Updating Commander's Firmware.....	38
Cloud Update	38
TFTP Update	39
Removing all Data from Commander	41
Object Specifications.....	42
Example Object Reference	42
Device Top-Level Objects	42
Configuration	44
Platform Information.....	45
Default Configuration	46
Last Restart	46
Software Versions	47
Software Version Detail	47
Software Cloud Update	48
Recording Configuration	49
LAN Port Configuration.....	50
DHCP Server	51
DHCP Server Lease	51
UTC & Daylight Savings Configuration.....	52
Interfaces Configuration.....	53
Installed Drivers	53
Interface Licences	53
Commander Hub	54
Web Server Configuration	55
Web Server Content	55
Web Server Security.....	56
Web Server Default Access Security	56
Web Server Information	57
Essential Data Configuration.....	58
Essential Data Page Configuration.....	59
Essential Data Object Configuration	61
Essential Data Task Control.....	63
Time Control Configuration	64
ObVerse Processor Configuration	65
ObVerse Object Modules	66
Security Server Configuration	67
Data Transfer Configuration.....	68
Data Transfer Task.....	68
Alarm Delivery Configuration	69
Alarm History Configuration.....	70
Alarm Email Configuration	71
Alarm Email Destination Configuration	73
Email Address Setup.....	74
North IP Devices Configuration	75
North IP Device Configuration.....	76
Essential Values	77
Essential Values Page	77
Time Control	78
Calendar.....	79
Calendar Exception Date	80
Timer	81
Profiler.....	82
ObVerse	83

Security Server	84
Security Server Group.....	84
Security Server User	85
Data Transfer	86
Transfer	86
Alarm Delivery.....	87
Alarm Delivery Destination.....	87
Alarm History	89
Alarm Emailer	90
Alarm Emailer Destination	90
North IP Devices.....	91
North IP Secure Device	91
Platform Information.....	93
LAN Port	94
Web Server Configuration	95
Web Server Configuration	95
Web Server Template	96
Web Server Home Page	97
Web Server Security.....	97
North IP Devices Configuration	98
North IP Device Configuration.....	98
Telnet Setup.....	99
 Appendix A - Ethernet/IP Protocols.....	 101
 Appendix B – Factory Installed Drivers	 103
 Appendix C – Internal Switch Features	 104
PROGRAM switch	104
DEFAULTIP switch.....	104
 Warranty, Safety, Environmental, and Regulatory Information	 105
Warranty.....	105
Support Period.....	105
Security	105
Declaration of Conformity	105
UK PSTI Statement of Compliance.....	105
Recycling information	106
Battery Disposal.....	106
 Commander Versions	 107

What is Commander?

Commander is the smaller of North's building controllers, which also includes ObServer. The controllers contain North's interface technology, block-based programming language, and easy-to-use information services. Commander can work as a stand-alone controller; linked with Commander Hub for easy remote monitoring; or alongside other North controllers and display systems to create a larger control or monitoring solution.

Interface Technology

Commander includes North's interface technology. Commander can access values from thousands of different third-party systems in a common way, using North drivers. This ability allows Commander to pass data between different systems and enables different sub-systems within a building to be fused together to form a single, coherent system.



Programmable Control

ObVerse is North's block-based programming language. It is available in all North controllers. Although it is easy to use, it provides real flexibility during engineering, allowing the engineer to incorporate design changes with minimal effort. Date and timer functions are standard, along with feedback control and logic.

Information Services

Commander supports North's standard protocol, allowing secure communications with other North products, including powerful engineering tools and display software. Commander also generates and serves standard web pages automatically – these provide a consistent user display on all browsers, including those on mobile devices. Commander can also monitor and inform users about alarm conditions using email or SMS, for example.

Commander can link to Commander Hub, the cloud-based meeting place for Commanders, their owners, their installers, and their service providers. These people can then access Commander's data from anywhere, viewing historical data and adjusting values. Events can be emailed to the relevant people.

The engineer can extend information services, if necessary, by using North's driver technology: values from within Commander can be made available to, say, BACnet and Modbus devices.

Typical Use

Commander's powerful feature list means it can perform a wide range of tasks. The following are typical applications...

Single-device Integration of Systems

Creating an interface between two or more systems is easy with Commander (Fig. 1). Interlocking an air-conditioning system with an underfloor heating system is a common problem, although the possibilities are endless.

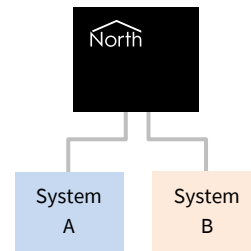


Fig. 1 Integration

Building-wide Management System

Connecting different systems, in different locations, to a common LAN (usually an intranet or VPN) allows users to manage these systems using a common interface from anywhere on the LAN and adjust settings as necessary.

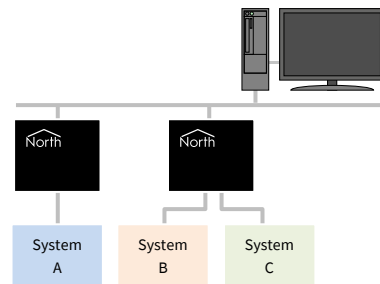


Fig. 2 Building management

Remote Management System

Commander can be part of a remote management system that connects different systems in different buildings and provides information back to a central display. The central display can be North's Commander Hub service, or ObSys management software.

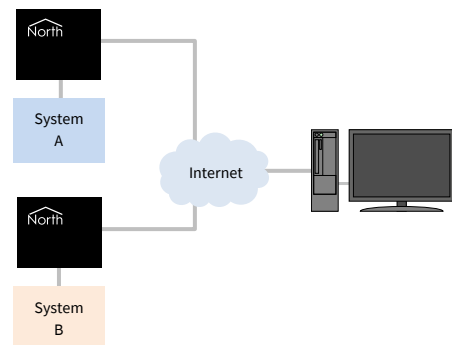


Fig. 3 Remote management

Quick Start

Mount Commander

Locate Commander so it is accessible to remove the lid and set the internal switches when required. Leave a clearance of at least 20mm around the device, with 80mm minimum at the cable connection edge (see [Dimensions](#)). Choose a safe location away from vibration, shock, and electrical noise; in an area where there is no excessive moisture.

If you are mounting Commander directly on to a wall or within a panel, use the chassis as a template to mark and drill four 4mm holes. Screw the Commander securely to the surface using the mounting holes.

If using the optional DIN-rail mounting kit, order code MISC/DINKIT, attach the two clips to the back of Commander using the bolts provided. Clip on to standard 35 mm DIN-rail, 'top hat' compatible.

Set Switches

Detach Commander's lid by removing the two screws, and sliding it off.

Set **DEFAULTIP** switch ON to force the Commander to use the default IP address of 192.168.192.167. Refer to the [Internal Switches](#) section for more details.

Apply Power

Commander's power connector (PWR) is polarity independent. Use a 12 to 24V, either AC or DC, power supply rated at 3VA. We recommend using a good quality regulated DC power supply, for example 12V DC providing 500mA per Commander. Refer to the [Power](#) section for more details.

Connect and apply power. The Commander MODE LED illuminates green to indicate a healthy power, and will blink in Default IP or Program mode. Refer to the [LEDs](#) section for more details.

Insert the Battery

Insert the supplied 3.6V battery into the holder in the direction indicated, with + symbol, and secure with the supplied clip. Refer to the [Internal Battery](#) section for more details.

Install North Engineering software

If necessary, Install North Engineering software onto your Windows PC. Download ObSys Setup from the www.northbt.com website. If you are new to using Commander or need a refresher, the *Commander Tutorial* is a better place to start – follow the steps to learn how to use the main features.

Connect PC to Commander

Connect your PC to Commander's LAN port using Cat 5 or better Ethernet cable. Commander will detect whether a patch or cross-over cable is used and work with either. Refer to the [LAN Port](#) section for more details.

If your PC's Ethernet port is set to Automatic (DHCP mode) IP assignment, it can use Commander DHCP server to get a valid address. Otherwise, set IP assignment to manual with an IPv4 address 192.168.192.1 and subnet mask 255.255.255.0

Run the **Start Engineering** application and select **Commander at default IP address**. You may need to press **Scan** to manually scan Commander's contents. The Commander contents should appear in the list with a label that includes its serial number.

Hardware

Commander's black steel case contains a two-board device. The upper board contains the main processor, memory, LAN port, battery and switches. The lower board contains the power regulation and the isolated RS232 ports.

Dimensions

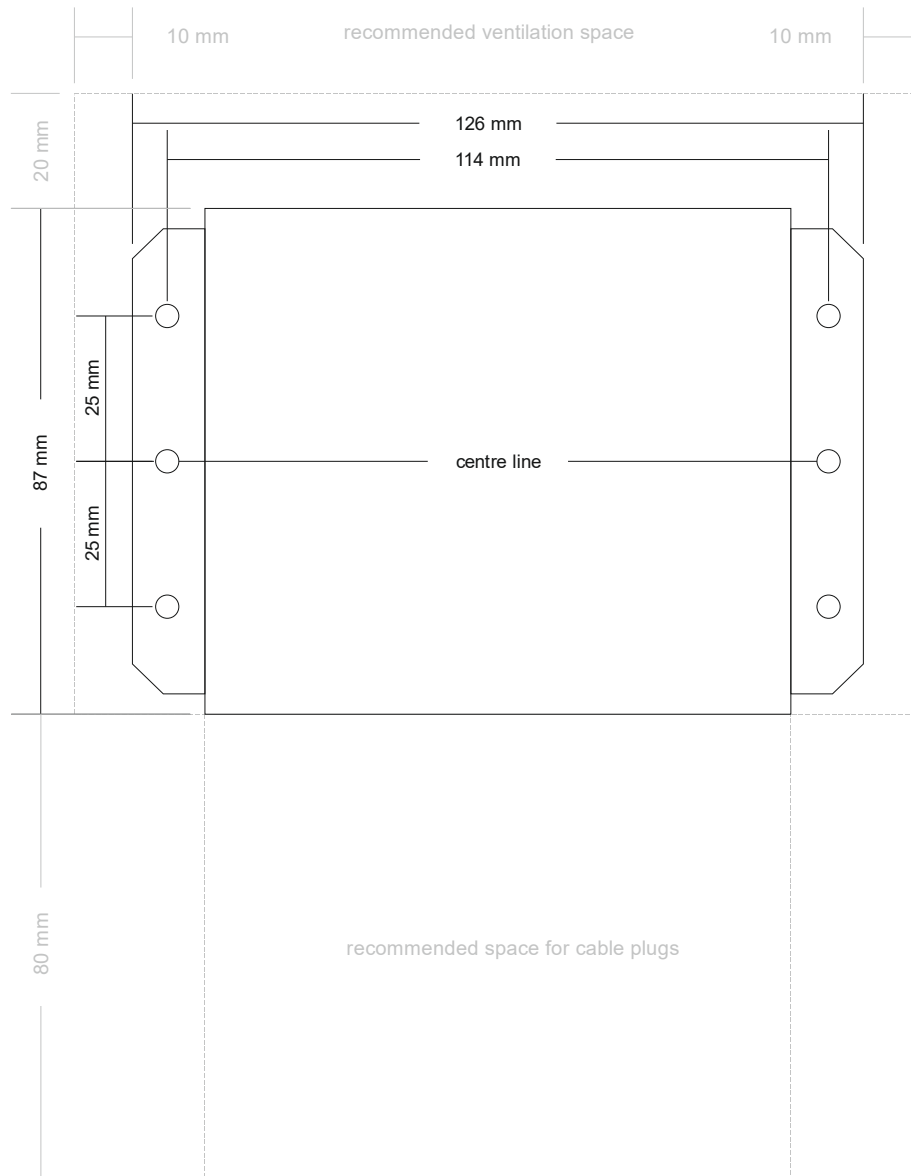


Fig. 4 Dimensions of Commander

Width	126 mm
Height	87 mm
Depth	45 mm

Installation

Leave a clearance of at least 20mm around the device, with 80mm minimum at the cable connection edge (see Fig. 4). It should be accessible to remove the lid and set the internal switches when required.

Choose a safe location for installing Commander, in a secure place based on its use.

DO NOT install Commander:

- In an area with excessive moisture, temperature, corrosive fumes, or explosive vapours
- Where vibration or shock is likely to occur
- In a location near a source of electrical noise.

Installation on an even surface

Six 4mm mounting holes are available (Fig. 4), suitable for M4 bolts. Use the chassis as a template to mark and drill four holes. Screw the Commander securely either directly on to a wall or within a panel using the mounting holes.

Installation on DIN-rail

An optional DIN-rail mounting kit is available, order code MISC/DINKIT. Attach the two clips to the back of Commander using the bolts provided. Tighten the bolts as much as necessary so the clip retains its shape. Clip on to standard 35 mm DIN-rail, 'top hat' compatible.

Connectors

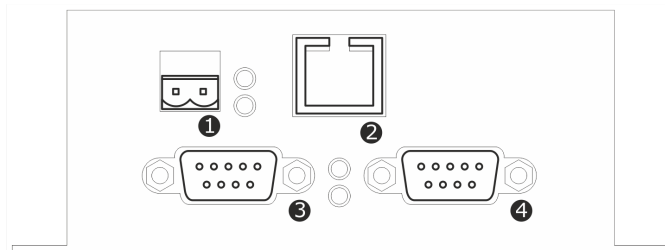


Fig. 5 Connectors on Commander

- | | |
|--------|--------------------------|
| ❶ PWR | 12-24V AC/DC at 3W |
| ❷ LAN | Isolated 10/100 LAN port |
| ❸ COM1 | Isolated RS232 port |
| ❹ COM2 | Isolated RS232 port |

LEDs

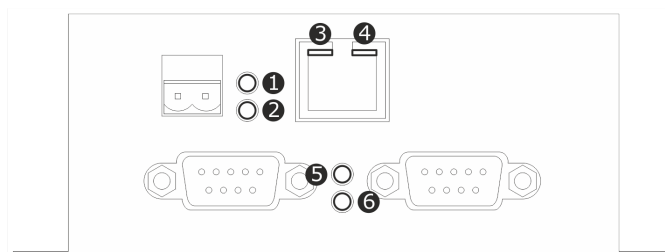


Fig. 6 LEDs on Commander

- | | | |
|---------------|--------|--|
| ❶ MODE | Green | Off=No power, On=Run, Blink=Default IP or Program mode |
| ❷ SAVE | Green | On=Writing to flash memory |
| ❸ LAN SPEED | Yellow | Off=10 Mbps, On=100 Mbps |
| ❹ LAN LNK/ACT | Green | Off=No link, On=Link up, Flash=LAN port activity |
| ❺ COM1 ACT | Red | On=COM1 port activity |
| ❻ COM2 ACT | Red | On=COM2 port activity |

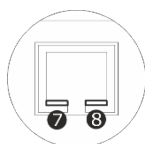


Fig 7 LAN port LEDs on previous hardware versions

Commander hardware version 1 and 2 has a different LAN port (Fig 7). It can be identified with its cable clip at the bottom.

- | | | |
|-----------|--------|-------------------------|
| ❷ LAN LNK | Green | Off=No link, On=Link up |
| ❸ LAN ACT | Yellow | On=LAN port activity |

Power

Commander requires a 12V to 24V ($\pm 10\%$), AC or DC, power supply rated at 3VA. The power connector, PWR, is polarity independent.

North recommend you use 6VA supplies. We recommend using a good quality regulated DC power supply, for example 12V DC providing 500mA per Commander.

The Commander MODE LED will illuminate green to indicate a healthy power, and blink to show Commander is in Default IP or Program mode.

LAN Port

Commander has a single isolated LAN port, with the following specification:

- RJ-45 10Base-T/100Base-TX
- HP Auto MDI-X™ sensing crossover cable
- 10/100 Mbps full and half duplex auto-negotiation
- Compliant with IEEE 802.3/802.3u

Earlier Commander hardware, version 1 and 2, has a different LAN port with the following specification:

- RJ45 10Base-T
- Auto MDI-X sensing crossover cable
- Full and half duplex auto-negotiation

CAUTION

DO NOT connect this product to a LAN connection that is subject to over-voltages.

RS232 Ports

Commander has two isolated RS232 ports, COM1 and COM2. These can be used to interface either directly with RS232 devices, or with devices supporting a different hardware layer (e.g. RS485) using a converter.

Each of the 9-way DTE ports use the following pins:

- 1 Not connected
- 2 RXD – data from external system
- 3 TXD – data from Commander
- 4 DTR – held high by Commander
- 5 GND – the signal ground
- 6 Not connected
- 7 RTS – control from Commander, use varies depending on Interface
- 8 CTS – control from external system, use varies depending on Interface
- 9 Not connected

An optional North RS232-RS485 serial converter is available, order code CONV/232/485.

Internal Battery

Remove the lid to access Commander's battery (Fig. 8).

Commander requires a battery to retain its engineered settings during a power-down. Secure the battery in position using the supplied clip.

To load the *default configuration*, turn-off power supply and remove the battery. Wait 60 seconds, then turn-on power supply before re-inserting the battery.

The lithium-ion battery is non-rechargeable, but retains its charge for a long time.

Commander measures the voltage supplied from its battery and can send alarm events when this becomes too low. You may wish to replace the battery after 10 years, regardless of whether battery has become low or not.

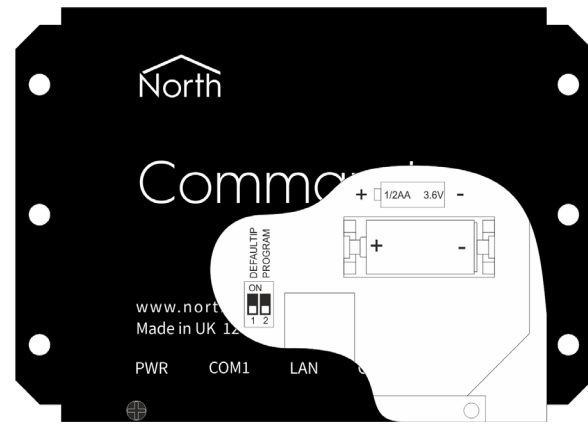


Fig. 8 Internal battery and switches

Replacing the battery

When replacing a low battery, keep Commander powered-on or you will inadvertently load the default configuration.

Remove the clip by inserting a slotted screwdriver (max 4mm tip) at either end of the battery holder to release. Insert new battery in the direction indicated, with a + symbol, then replace clip.

Battery type: 1/2 AA size, 3.6V, 1.2Ah, Lithium Thionyl Chloride (Li-SOCl₂)

Compatible batteries: EVE ER14250, Saft LS14250, Tadiran SL-350/S.

Visit northbt.link/battery to search for compatible batteries.

Battery safety

CAUTION

Risk of fire, explosion or severe burn hazard:

DO NOT recharge.

DO NOT dispose of battery into fire or a hot oven, mechanically crush, disassemble, short-circuit, or expose contents to water.

DO NOT store the battery in a high temperature environment.

IMPORTANT

Replace with compatible lithium-ion battery in the direction indicated with + symbol

Risk of fire or explosion if the battery is replaced by an incorrect type.

Lithium battery material safety data sheet available at www.northbt.com/cmdr.

Internal Switches

Remove the lid to access Commander's switches (Fig. 8).

The **DEFAULTIP** switch selects whether Commander uses the default or an assigned IP address. When the switch is changed, Commander restarts.

When set ON, Commander is set to use the default IP address of 192.168.192.167. This is useful if you do not know the assigned IP address of Commander. It also unlocks the device – pausing security and enabling a DHCP server and Web Server. Refer to [Appendix C](#) for a full list of services enabled.

When set OFF, Commander uses the engineer assigned IP address and security settings. Refer to the [LAN Port Setup](#) section on how to assign an IP address.

When the **PROGRAM** switch is set ON (and Commander restarted), it enables the installing of new firmware into Commander's flash memory.

Previous hardware versions have a **FACTORY** switch. This should always be set OFF.

Memory

Commander has 8MB of flash memory, which holds its main operating firmware and driver firmware, along with a default configuration. Refer to the [Firmware](#) and [Default Configuration](#) sections for details on how this is utilised.

The main operating and driver firmware can be updated to the latest version, and new drivers added. Follow the guide in the [Updating Commander's Firmware](#) section.

Commander also has 4MB of RAM, which it uses to hold all configurable settings – this is battery-backed to maintain the memory over a power-failure. A fresh battery will maintain the memory contents for several years.

Interface Licences

North supply Commander with a certain number of interface licences, which control the number of interfaces that can be used at a time. Each interface usually requires one interface licence before it will start, although certain drivers require zero licences.

It is possible to upgrade the number of interface licences available within a Commander. Simply call North support while you are on site to activate a new licence.

Refer to the [Interfacing Commander to other Systems](#) section for more details.

Firmware

Commander's operation, and all of its power and flexibility, is controlled by firmware stored in its flash memory.

Main Firmware

The main operating features are provided in firmware. This firmware is loaded into Commander during production and can be updated if required.

The main operating features evolve over time as newer ideas are incorporated, but contain the following areas:

- General platform information, such as firmware versions
- LAN port setup, including IP addressing and time synchronisation
- Real-time clock and time zone, including daylight saving
- Interfacing to other systems
- Link to Commander Hub
- Web server
- Database of essential values
- Controlling using time and date
- ObVerse cause-and-effect strategy
- Transferring values between systems
- Alarm handling, including filtering, delivery, and audit trails
- Communicating with other North IP devices
- Security server

Interface Driver Firmware

Interface drivers are provided in individual firmware files, to simplify updating. The most popular interface drivers are loaded into Commander during production (see [Appendix B](#)). Less-used interface driver firmware can be downloaded as required. Interface drivers can be updated as newer versions are produced.

Popular interface drivers include:

- Zip – to communicate and control a North Zip network
- Modbus – including Modbus over TCP/IP and serial line protocols
- BACnet – providing BACnet/IP as both a client and a server
- JSON – an API for third-party software and web services
- KNX – for accessing equipment supporting the KNX standard
- Advanced – one of many available fire panel interfaces
- Mitsubishi – one of many air-conditioning interfaces
- DALI – one of many lighting interfaces.

For the latest list of drivers available for Commander, visit northbt.link/drivers.

Secure by Default

Commander is built for communications and supports many different protocols on Ethernet. Each of these is both a strength and a weakness – a strength when building a powerful integrated systems; a weakness because each protocol could provide a point of attack by malicious actors.



Commander is manufactured with a secure by default configuration, which means network based features are either secured or turned off. Look for the secure by default logo in this manual.

Features that can affect the security of Commander include:

- Internal switch settings
- Driver interfaces – consider the benefits and reduce any risks of starting an interface and making a protocol available
- North IP Device access – before connecting to a network, secure by setting the authentication key and selecting required network access
- If using the Web Server, turn on by selecting required network access and user security settings
- Enabling Commander Hub
- Keeping Commander's firmware up to date
- Removing all data from Commander at end of life.

Functional Organisation

The different areas of function within Commander (or any other North product) are organised, and therefore engineered, in the same way using objects.

This object system, which North have used in products for many years, is extremely simple to understand, and yet gives a flexible, extendable system.

The object system has two simple rules:

- Each device appears as an **object**
- Each object can either **contain** other sub-objects, or have a **value** that can read (and usually set)

Commander appears on the LAN as an object; it contains sub-objects that represent the sub-functions within Commander; each of these contains sub-objects representing sub-functions; and so on until we get to sub-objects that have values, which can be viewed and possibly adjusted.

Functions

Functions within Commander are represented by container objects. A container object can either have a pre-determined list of sub-objects (called a fixed container object), or can have a variable list of sub-objects (called a variable container object).

North's object engineering software shows the contents of an object, and allows the engineer to navigate up, down and across these container objects. It also allows the engineer to scan and find the sub-objects within any variable container object.

For example, Commander is a variable container object with its contents changing as interfaces are started and stopped.

Settings

Settings within Commander are represented using value objects. The value of an object can be viewed by engineering software or by other devices; some value objects can also have their value adjusted.

North's object engineering software shows the current values of these objects, and allows the engineer to make changes to objects that are adjustable.

For example, Commander's label is a value object that can be viewed and adjusted.

Organisation of this Manual

The following chapters in this manual describe the functional areas within Commander. These areas appear as sub-objects of Commander within the object engineering software, ObView.

Refer to the *Commander Tutorial* for more help on using the object engineering software to engineer Commander, including full examples.

The final chapter, *Object Specifications*, details the contents to each of Commander's container objects. It lists each of the fixed and variable container objects and describes the type and attributes of each value object.

Platform Information

The *Platform Information* area provides general information about Commander.

Switch Settings

It is possible to view the mode specified by Commander's switches, although objects are read-only. Because the values are available as objects, they can be used by the engineer to affect other things, such as enabling cause-and-effect strategy, or enabling security for certain users.

Battery Health

The state of *Commander's battery* is available as an object. Commander will also send a battery status alarm when the battery voltage reduces to a low level (3V) or very low level (2V). If necessary, the battery state can be transferred to other external devices, such as lamps and sounders.

Default Configuration

Commander's engineered settings are held in battery-backed memory. If the battery has expired when the external power is lost, this configuration is lost.

Commander's current configuration can be saved to permanent flash memory, so that if the settings are lost, the default configuration can be loaded.

This feature can be used in several ways:

- As a failsafe, if the battery and power fail simultaneously
- As a pre-configuration mechanism, enabling a user to load a standard configuration.

Reset/Restart Information

Commander holds information about the last restart to occur, including the assumed cause. This information is sometimes useful when solving problems.

Software Versions

Commander's firmware is made up from a collection of different modules. The software version and build date for each module is available, again to help when solving problems.

Software Cloud Update

If Commander has access to the Internet (and therefore to North's cloud services) it can be instructed to check it is running the latest firmware. It will check the installed system and driver software against the latest available versions, and update them if necessary.

See *Updating Commander's Firmware* for more details.

Debug Recording

Commander can send information to an unused COM port to assist with debugging. The North support team may request that this information is captured.

A set of flags specify which debug information is recorded:

- Information – general start-up information
- Objects – request/reply messages between modules
- COMs – bytes being sent and received on COM ports
- Network – IP events, including ARP and DHCP
- Internal Comms – fast request/reply messages between internal modules

An ASCII terminal, or PC running terminal software, is needed to receive the debug information. The terminal needs to be set to 38400 baud, no parity, 8 data-bits, 1 stop-bit, and no hardware flow control.

An RS232 null-modem cable is required to connect the terminal software to Commander.

LAN Port Setup

The LAN Port area allows the set-up of Commander's LAN port. The most important value is Commander's IP address, which allows other devices, including engineering software, to access Commander from elsewhere on the LAN.

There are three ways of assigning Commander with an IP address to use:

- Default – a predetermined IP address, controlled by a hardware switch within Commander
- Static – set to an engineer-assigned fixed IP address
- Dynamic – set to an address assigned dynamically by a DHCP server [Factory setting].

Whichever way is used, Commander's current IP address is available within a read-only object.

Default IP Addressing

Setting the **DEFAULTIP** internal switch to ON, restarts Commander to work at the default IP address of 192.168.192.167 with a subnet mask of 255.255.255.0, and no gateway address. This is used for initial set-up, quick engineering, or if the Commander's IP address is unknown.

Default IP mode pauses security and enables the DHCP server, useful for connecting your engineering PC directly to Commander. This mode is not usually compatible with a working LAN.

Static IP Addressing

Configuring an IP address and subnet mask assigns Commander to use that IP address – you can also configure a gateway, DNS server, and time server addresses. This is the usual way of configuring the IP address, as users and other devices usually need to know where Commander is.

Dynamic DHCP Addressing

Configuring an IP address of '0.0.0.0' instructs Commander to request its IP settings from the network's DHCP server – the server normally also supplies DNS and NTP server addresses. Dynamic addressing is simpler than static addressing, but the IP address given by the DHCP server to Commander may change after a period. Ask your network administrator to create a DHCP reservation using the MAC address.

The Commander Label is passed to the DHCP server, after filtering invalid DNS characters. The filter changes any uppercase letters to lower case, and any non-alphanumeric characters (including spaces) are changed to the hyphen '-' character.

This is the default setting.

DNS Server Address

Commander sometimes needs access to a DNS server to resolve fully qualified domain names (FQDN). It is usual for the DHCP server to provide the server's IP address, but otherwise the engineer can configure it using this object.

If no DNS address is specified, 1.1.1.1 is used if possible.

Time Server Address

Commander can request time information from an NTP server, but again needs to know the server's address. It is usual for the DHCP server to provide this, but otherwise the engineer can configure it.

If no NTP server address is supplied, Commander will try to contact 'pool.ntp.org' for a valid NTP server if possible.

Real-time Clock and Time Zone

Commander contains a real-time clock, time-zone information, as well as daylight saving offsets. Commander can use all of these to determine local time.

Coordinated Universal Time

Commander contains a hardware real-time clock (RTC). The internal battery retains settings when the Commander is powered-off. This clock holds Coordinated Universal Time (UTC).

If the Commander has access to an NTP time server, it will automatically correct its clock. Commander requests the time from the NTP server every 4 hours, and if the response is acceptable, the real-time clock is adjusted (if out by more than 2 seconds).

Local Time

Commander calculates local time by applying a local time offset to UTC time (as well as any daylight-saving offset). By default, Commander's local time offset is zero, which is correct for the United Kingdom and Ireland. In mainland Europe, the local time offset should be set to +1 hour.

If the local time is adjusted manually, Commander will automatically convert the value to UTC before writing to the real-time clock.

Daylight Saving Time

Commander's daylight-saving table is set during production with 10 years of dates and offsets suitable for use within the European Union. If used outside of this area, the dates and offsets within the table should be set as necessary.

Interfacing Commander to other Systems

One of Commander's strengths is its ability to interface to several systems, including those from other manufacturers. Drivers are the software convertors that allow interfaces to work.

The driver required for a particular interface is selected from those installed in Commander. Commander starts these interfaces when they are specified, and whenever Commander is restarted. Drivers can be stopped, if they are no longer needed.



Commander supports many different protocols on Ethernet. Each of these is both a strength and a weakness – a strength when building a powerful integrated systems; a weakness because each protocol could provide a point of attack by malicious actors. Therefore we must consider the benefits and reduce any risks of starting an interface and making a protocol available.

Started Interfaces

Commander allows up to four interfaces to be started and used at the same time, although interface licences may limit this.

Installed Drivers

The list of drivers currently installed within the Commander can be viewed – and the names copied to the current interface list to start an interface using a particular driver. The same driver can be used on several interfaces concurrently. For example, Commander can start interfaces to two separate Zip systems, each with 16 Zip modules.

Commander has certain drivers pre-installed in the factory. For a list of these, see [Appendix B – Factory Installed Drivers](#).

Other drivers can be installed at any time. For details on how to do this, see [Updating Commander's Firmware](#).

Each driver is documented with details of the equipment it can connect to, how the driver is used, and what objects are available. You will find driver manuals in the North Product Documentation app.

Interface Licences

Each Commander is supplied with a certain number of interface licences. It is possible to add more licences on site, although a phone call is required to check/verify settings.

Call North support on +44 (0) 1273 694422 for more help with adding more licences.

Order Codes for Commander are as follows:

North Order Code	Interface Licences
CMDR/0	0
CMDR/1	1
CMDR/2	2
CMDR/3	3
CMDR/4	4

Order Code for an additional interface licence

North Order Code	Interface Licences
UPGD/1	1

Transferring Values

Transferring values from one place to another is the simplest form of integration. Commander supports this with Data Transfers – where each transfer reads from one place and then writes to another.

Commander supports up to 500 Data Transfers.

Transfers are processed sequentially. Each transfer contains a source object reference, a source read rate, the last value read, a destination object reference, and a destination write rate.

Commander's object system means that any value available from Commander, including configuration objects and other attached systems, can be used with transfers.

Reading the Value

The source read rate should be configured to suit the type of value being transferred. For example, room temperatures are typically read every minute or so, and operating set points read every 15 minutes.

Setting the source read rate to 'as soon as possible' (ASAP) instructs Commander to read the value every time the transfer is processed – if all transfers have a read rate set to ASAP, the reading occurs sequentially.

Remember to consider the time needed to read values, because they do not occur instantaneously. If it takes 1 second to read a value from an external system, then it will take 100 seconds to read 100 values. Even if you specify the 100 values read every minute, the best that could occur would be every 100 seconds.

Writing the Value

Rather than read-then-write continuously, each transfer will usually only write the value to the destination object when the value changes – called change-of-value (COV) writing. This eases the workload within the destination system and saves time and effort within Commander.

It is also possible, to have the transfer perform a background write periodically. Occasionally it is useful to have the last value re-written in this way – for instance, if a system forgets values after a power failure, or if a local adjustment needs to be reset after a certain time.

Remember COV writes always happen, so consider if a background write is needed and how frequently it needs to occur. Writing the value takes precedence over reading, so set the write rate to a longer time than the read rate. A background write only usually needs to occur every few hours.

Transfer Tasks

By default, Commander works through the list of transfers sequentially – after finishing transfer 1, it starts transfer 2, and so on, until it reaches the last transfer, after which it starts work on transfer 1 again.

This is simple to understand but can be quite slow. If values are from several different systems, it is possible to allow the Data Transfer system to try to perform two or more transfers simultaneously. However, this feature should be used with care, and should be fully tested before handover, because if several tasks are reading from or writing to the same system, overloading of the system's communications can occur.

Essential Data

Several different modules within Commander need access to a database of values – called Essential Data.

Essential Data allows the engineer to configure a list of values that other Commander modules can then distribute – as web pages, as BACnet points, as Modbus points, on Zip displays...

Structure

Essential Data consists of a list of configurable pages, each of which has a list of configurable objects. In total, 640 database objects are available. The engineer may choose from a mix of page and object counts: 40 pages of 16 objects (default), 64 pages of 10 objects, 20 pages of 32 objects, or 10 pages of 64 objects. Older versions of Commander only support 30 pages of 16 objects (total 480 objects).

An Extra Data driver is also available to extend the number of database values available within Commander.

Pages

The engineer configures a label for each page. Other Commander modules use the label when displaying the value from within the database – if a page has no label, then the page does not appear in label-based hierarchical views, such as those available as web pages.

Each page has a remote object prefix. This allows objects within the page to reference remote data relative to this prefix. When in use, if any object in the page fails to read its remote object, Essential Data assumes all the objects will fail, and therefore saves time and effort. It also allows easier copying of pages when several devices of one type are used.

Objects

For each object within a page, the engineer configures a label. The label determines whether the object appears – if an object has no label, the object does not appear in label-based hierarchical views.

The engineer configures the value type for an object. The type determines whether a value is made available via a particular protocol – for example, profile objects are not made available over the Modbus protocol. The type also controls the appearance of the value on hierarchical views, including when the user adjusts the value.

Type	Use	Example
Text	Text string of ASCII characters	Kingston Lane
NoYes	Binary state: 0 or 1 meaning No or Yes	1 (<i>means Yes</i>)
OffOn	Binary state: 0 or 1 meaning Off or On	0 (<i>means Off</i>)
Number	Integer, positive or negative	-12300
Float	Floating-point value, with decimal places	21.54
Times	List of on-off times	08:30-12:00,13:00-17:30
DateTime	A moment in time	25/12/15 12:30
Date	A particular day	01/01/19
Enum	A number representing something	3 (<i>means Automatic</i>)
Profile	List of time-value changes	09:00=21,12:00=20,18:00=19

Value Reading and Writing

The engineer can configure the database object to read periodically from, or write periodically to, any object accessible to Commander. This allows slow-access data to be collected and ready for speedy delivery when needed.

As a new value is read, the object also recalculates the alarms state, sends alarm messages if necessary, and logs the value.

Commander considers each object in a linear fashion, beginning with the first object on the first page. If it is time to read (or write) the value, this is started; if not, the object is passed over. When the final object has been checked, Commander starts from the first object again.

If all objects are set to read ASAP (as soon as possible), Commander performs each in turn. If it takes one second to read an object, and there are five hundred objects to be read, the whole process will take five hundred seconds. Please consider the read rate of objects, allowing time for the object to perform its remote action.

If an object is set to read periodically, and is set to adjustable, then an adjustment will cause three attempts at writing the new value to the object, before reading is resumed.

Adjustability

By enabling adjustability, along with configuring value high and low limits, the engineer can control whether the user can modify the value of an item – and if this occurs, the value will be written to the associated object.

Alarm Monitoring

When a value is updated, it is compared against the value high and low limits, and an alarm message generated as necessary if its alarm state changes.

Value Logging

If necessary, Essential Data can log the value periodically, to create a short history of the value over time. Other devices can access the data log. More recently, logging by Commander Hub is preferred.

Essential Data uses the configured log rate to sample the value – if the log rate is set to 15 minutes, one day will use 96 readings.

A total of 40 objects can have logging enabled.

If the value has not changed from the last sample, then rather than waste sample space, the log records start-and-end sample times to save space. Using this method, 15 minute sampling will use a maximum of 96 readings per day, but could be considerably less if, for example, the value is an alarm state.

Commander Hub

If the link to [Commander Hub](#) is enabled, values from Essential Data are sent to Commander Hub, where all values are recorded. Historical data can be viewed, and adjustable objects may be changed via the Commander Hub web pages at www.cmdrhub.com.

Controlling using Time and Date

Timers and profilers allow users to control when things happen in the day, and when they do not. Using timers can save energy, while keeping the occupants happy. Commander supports time control using the calendar, timers and profilers within its Time Control area.

Commander's single calendar determines today's day-type. Today's day-type is used by 20 timers to determine which of their on-off time-lists to use, and by 20 profilers to determine which of their time-value profiles to use.

Calendar

Commander supports 10 different day-types: one of them is an off day-type, leaving nine to configure. They are numbered 0 (off), and 1-9.

If you have a centralised calendar elsewhere on the system, Commander can request the day-type from this – in which case you need to specify the object reference of the current day-type in the central calendar.

If you are calculating the day-type in Commander, it works in the following way. The calendar determines whether today's date is an exception date – if it is, then that exception day-type is used; otherwise the day-type of the standard day-of-week is used.

The calendar re-calculates the day-type every minute, based on the day-types and the exception dates.

Any North device that can access Commander's objects can also access the calendar objects.

Timers

Commander uses timers to control off/on processes. Each timer produces an off or an on state, which can be accessed by other tasks (Fig. 9).

Each timer has a time-list for each of the possible day-types and uses that time-list on days that have that day-type. A time-list is a list of on-off time-periods. The timer re-calculates the state of the timer every minute.

Any North IP device can access the Timers.

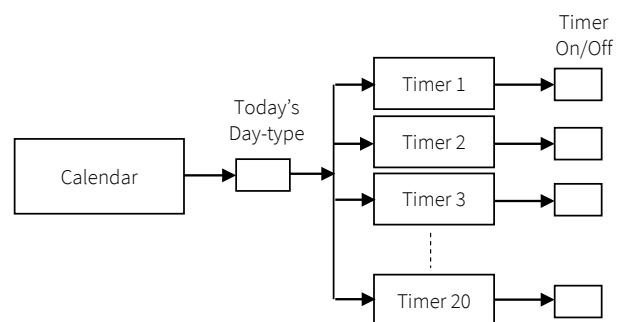


Fig. 9 Timers

Profilers

Commander uses profilers to control a variable value throughout the day.

Each profiler has a list of profiles, one for each possible day-type, and uses that profile on days that have that day-type. Each profile is a list of time-value pairs, each pair representing a change-point. When the current time matches a change-point time, the value is set to that of the change-point. The value can also be set by other tasks: the value then acts as a temporary value, until the next change-point occurs.

ObVerse

ObVerse strategy (covered in the next chapter) has timer and profiler properties that can also be used for time control.

ObVerse Cause-and-Effect Strategy

Sometimes you need to do more than simply transfer a value from one object to another – you need to calculate something, delay something, or perform a more complex function on a value. North provides this flexibility with ObVerse, a cause-and-effect programming language.

ObVerse consists of a range of modules. The engineer selects modules and links them together to perform a desired strategy.

ObVerse strategy runs in an ObVerse processor within a device.

ObVerse processors come in two types:

- Standard Processor – with logic, maths, and control modules
- Advanced Processor – with the same features found in a standard processor plus extended maths and logic, display, application execution, directory and file services, and user-defined modules.

Commander has two ObVerse standard processors.

ObVerse strategy is made up from properties, modules and comments.

Properties

ObVerse properties are containers for storing data values. They can carry a value from one module to another, or between the processor and other functions within Commander.

Properties have a data type, to define the type of value they hold – like a number or a text string.

Properties sometimes hold values passing only between modules in the same processor. In ObVerse, we call these private properties, as their value is private to the processor.

Properties sometimes hold values passing between the processor a function within Commander. In ObVerse, we call these public properties, as their value is publicly available as an object.

Modules

Modules calculate values. They take one or more inputs and calculate one or more outputs.

Different modules are available to perform different operations. The range of modules supported depends on the processor.

In Commander's ObVerse standard processor, modules perform the following types of operation: Maths, Logic, Control, Timers, System, and Object.

Editing ObVerse

You can create and edit ObVerse strategy using North's ObvEditor application, installed as part of the ObSys software. ObvEditor provides drag-and-drop graphical editing of ObVerse, uploading and downloading of ObVerse strategy, and run-time monitoring of the strategy within the processor.

For further information on ObVerse in Commander, including properties and modules, refer to the *ObVerse Manual – Standard Processor*.

Alarm Basics

As well as responding to object requests, Commander can process alarm events – messages that contain text information about events that have occurred.

Different users demand a wide variety of alarm processing – ranging from simple histories of alarms, to lists of critical events that require user acknowledgement, to sending messages to mobiles phones or by email.

Format

All North-format alarms are text-based, and have the following fields:

System and Point – identity of the system, device, and point that has changed

Condition – condition that the point has changed to

Priority – importance of the notification, between 1 (most) and 9 (least)

Date & Time – date and time that the condition changed

Refer to *Object Specifications* section for details of alarms sent by each module.

Alarm Delivery

All alarms arriving or being produced by Commander are passed into the Alarm Delivery area. Its role is to distribute copies of the alarm to other alarm processing destinations, depending on the value of the alarm fields.

Commander's alarm delivery supports up to 16 destinations.

Commander has two built-in alarm processing destinations: Alarm History and Alarm Emailer. Other destinations are available within other North devices and can appear within drivers and external systems as interfaces are started.

Filtering Delivery

Besides having a destination enable, alarms can be filtered, so that only alarms with a priority in a certain range are sent to a destination. This allows only the relevant alarms to be sent to certain destinations.

Filtering can also cover text matching and not-matching, to force alarms from particular systems to be sent only to one destination, for example, while all other alarms are sent to a different destination.

Delivery to any one of a Group of Destinations

Sometimes users may need alarms sending to any of several destinations. For example, alarms must be sent to any one of a range of on-call users (depending upon which has their PC running).

Commander supports each destination being a member of the any group, an indication that when one destination accepts the alarm, it does not send to any of the other members of the any group.

History of Alarms

Sometimes, all that is required is a list of the latest alarms. Alarm history can act as an audit trail or can be viewed more regularly to check on new alarm conditions. However, no user action is necessary, and as new alarms occur, old alarms are lost. Commander's alarm history holds the last 100 alarms.

If the link to *Commander Hub* is enabled, these alarms are sent to Commander Hub, where they are stored.

Emailing Alarms

Some users want important alarms and event messages delivered directly to their inbox. Commander has alarm emailing facilities to do this.

Commander's alarm emailer supports six destination groups. Each group has its own filtering options, so only alarms from a predetermined system are emailed to the group's recipients, and an option to send in a text-only or friendlier HTML format. A group supports up to five email address recipients.

The Alarm Emailer can connect to an SMTP relay server that supports authentication, but not to a server that requires encryption. You can typically connect to an SMTP relay server on your local network (e.g. Windows IIS SMTP Server), from your Internet service provider (e.g. BT Internet, Virgin Media), or from a paid SMTP service provider (e.g. smtp2go.com, authsmtp.com, etc.).

SMTP relay servers that require TLS encryption (e.g. Gmail, Outlook, Office 365, AWS SES, etc.) are not directly supported. To access a service requiring TLS, use an SMTP proxy such as Windows IIS SMTP Server or Stunnel.

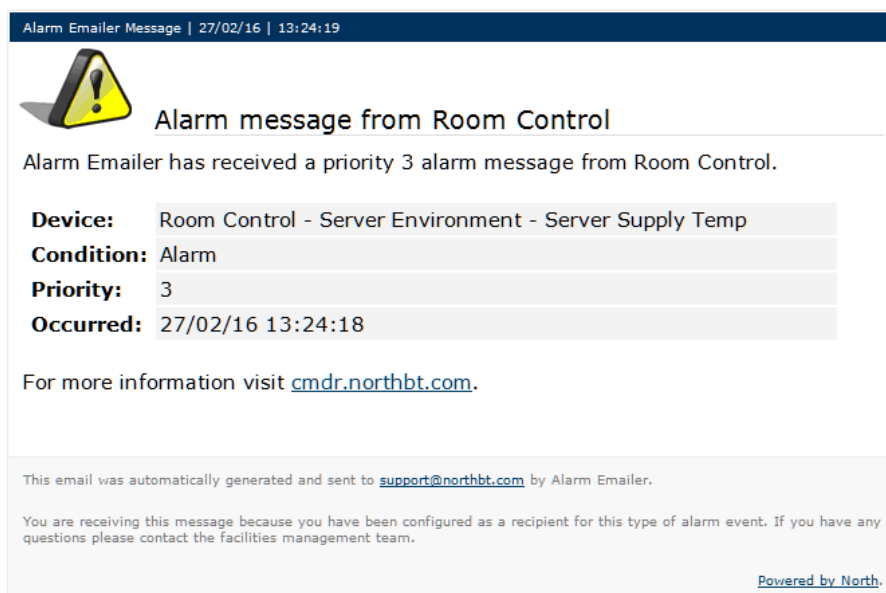


Fig. 10 Email from Commander's alarm emailer

If the link to [Commander Hub](#) is enabled, use Commander Hub to email notifications of new events.

Alternative Alarm Destinations

By adding more interfaces, it is possible to add more ways of dealing with alarms, these include the following:

Driver	Use
AlarmStore	Alarm Lists needing user acknowledgement, and archiving to CSV file (ObSys only)
AlmSet	Convert alarm text to an object write
AlmXlate	Translate alarm text
ESPA444	Pager support
GSMSMS	SMS messages to mobile phones, via a GSM modem
Printer	Print alarms to a serial printer

Communicating with other North IP Devices

All the North devices that support Ethernet also support the North IP protocol. This protocol is used when North devices talk to each other: when Engineering Software talks to a Commander; when one Commander talks to another Commander; and when an ObSys display talks to a Commander.

The North IP protocol allows the devices to communicate securely and efficiently using objects.

Securing North IP Device Access

Each North device has control over what can talk to it. Access to the device, in this case Commander, is secured with these settings:

- Authentication key – encrypts messages and only allows access from devices that know the key
- Access from local network – controls whether devices on the same subnetwork can read and write values
- Access from remote networks – controls whether devices on a different subnetwork can read and write values.

These security settings are disabled while Commander is unlocked in Default IP mode.

Authentication Key

Each Commander has an authentication key (similar to a password) and encryption method that other devices must know before they can send read and write requests to Commander. The key is never actually shown, but is used to encrypt messages. The receiving Commander decrypts the message to confirm the sender knows it's key.



By default, Commander is set with a random authentication key and AES-128 encryption. In Default IP mode, before connecting Commander to a LAN, first reset the authentication key.

Remember to document any keys used. Each Commander can have a unique authentication key, or for ease, you may decide to use the same authentication key for all devices on a site. You should not use the same key for more than one site or project.

Note: Older North devices, and Commander with firmware dated before 01/06/25 do not support AES-128 encryption. For compatibility with these products, set encryption to none.

Network Access

Commander can limit access from North devices on different networks. Access from local and remote networks can be restricted: read-and-write, read-only, or none.



By default, Commander is set to allow read-and-write access from the local network and no access from any remote networks (such as via a gateway).

Note: If you wish to engineer the Commander remotely, such as using a VPN, you will need to enable remote network access.

Checking Communications

It is possible to configure Commander to check that other North IP devices are still available and communicating and generate alarm messages when they are not.

DEFAULTIP Switch

When DEFAULTIP switch is set ON, the authentication key and encryption method are temporarily disabled. This enables an engineer to access the Commander regardless of this security setting (as long as they have physical access to the Commander).

Web Server

Commander's web server builds simple responsive HTML pages which the user can view in any modern browser, including those on mobile devices (Fig. 11).

The web server creates a website, with pages in the following areas:

Overview – summary information

Values – view and adjust values from Essential Values

Events – view events from Alarm History

Device information – hardware, network, Commander Hub, and firmware information.

All pages update their information while the user is active.



Commander's web server is disabled by default, except when the DEFAULTIP switch is set ON. Access to the website can be controlled with several security settings. These settings can restrict access from either local or remote networks and enable user sign-in.

Commander's web server is ideal for local access when an Internet connection is not available. We recommend enabling the link to [Commander Hub](#), which provides remote access using North's cloud-based services.

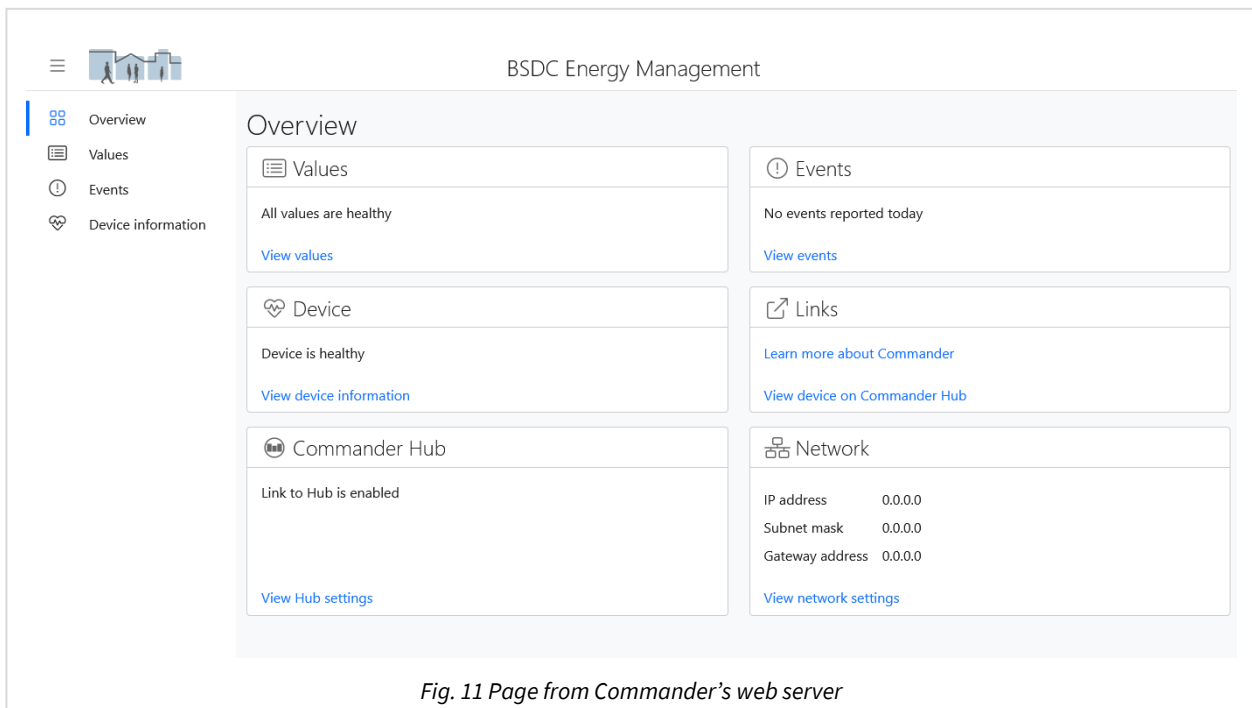


Fig. 11 Page from Commander's web server

Overview Page

Commander's overview page highlights areas within Commander that need more investigation: values, events, or the device itself.

Add links to external resources that may be useful to the end user – a web page, telephone number, or email address.

When Commander's DEFAULTIP switch is set ON, then Commander Hub and Network settings can be changed. This is useful if someone needs to change the IP address of Commander and has no access to object-engineering software.

Values Page

View Values from *Essential Data*, presented using the same page/value structure. Click on a value to view it and, if it is adjustable, change the value.

Any pages with the same name will be merged together. Some Markdown formatting is supported for text labels, including **bold** and *italic*.

Download all values in a comma-separated value (csv) file using the 'Export data' option.

Events Page

A single list shows all alarm events stored in *Alarm History*.

Download all events in a comma-separated value (csv) file using the 'Export data' option.

Device Information Page

Other information from Commander that may be useful to different users, including:

- Device hardware – serial number, default configuration, battery state, and program switch

- Network – active IP, subnet, and MAC

- Date and time – local date & time

- Commander Hub – link enabled and status

- Last restart – time since restart, reason, and total restarts

- System firmware – build versions

- Interfaces – list of interfaces started, driver version, and state of connection to external system.

Security Settings

Access to the website can be controlled with several security settings.

Access from local and remote networks can limit the website to view and adjust, view only, or disabled. This takes priority over any user privilege levels.

Local network access refers to access from an IP address on the same subnetwork as Commander, and remote network access refers to access from an IP address on a different subnetwork than Commander.

Specify whether users must sign-in before they can view or adjust values on the website. User authentication and privilege levels are provided by the *Security Server*.

If users are not required to sign-in, set a default access privilege levels for requests.

DEFAULTIP Switch

When DEFAULTIP switch is set ON, unrestricted access to the website is enabled. This includes temporarily allowing view and adjust actions from the local network, full user privilege levels, and disabling user sign-in.

Commander Hub

Commander Hub is a meeting place for Commanders, their installers, their owners, and their service companies. These people can then access Commander's data securely from anywhere, viewing historical data and adjusting values. Events can be emailed to relevant people.

Commander Hub is part of North's cloud-based services. When enabled, all Essential Data values and Alarm History events are sent to North's cloud service. It requires access to the Internet.



The link to Commander Hub is disabled by default.

By enabling the link to Commander Hub, you agree to have read and understand the [Terms of Use](#) and [Privacy Policy](#). Data is encrypted and sent securely to North cloud servers.

Data Collection

Commander continually monitors and records any changes to: values collected by Essential Data; alarm events received by Alarm History; device information

Then, typically every 5 minutes, it encrypts and transfers these changes to Commander Hub, where they are stored.

Keeping it Secure

Data is encrypted from beginning to end, keeping it secure.

Commander encrypts data using the Advanced Encryption Standard (AES) before sending to Commander Hub. The data stays encrypted when it is received and stored, and is decrypted only when an authorised user requests it. Commander Hub serves web content securely using Transport Layer Security (TLS) to a browser.

High Availability Servers

Commander Hub has redundant servers to increase reliability. Commander can send the AES encrypted data to either. Each server shares received encrypted data with the other, naturally creating a data backup. The servers are located in different physical places and use different service providers within the UK.

Easy to Connect

Commander is responsible for sending data to Commander Hub. It uses standard protocols, so most networks require no firewall modification. Data requests are always outgoing, so no additional PCs, port forwarding, complex VPNs, or fixed IP addresses are needed on the network.

If no Internet connection is available during install, use a low-cost 4G/5G LTE gateway with a simple data plan.

My Hub

Connect to Commander Hub using any modern browser at cmdrhub.com. Access multiple sites and Commanders from a single dashboard, My Hub.

Visual alerts direct you to any areas requiring attention, email notifications enable easier real-time maintenance that can become more pro-active.

All Commander's Essential Values are recorded, you can view and change the latest values or examine historical data over many years.

Alarm events from Alarm History are recorded and retained. Examine historical event counts, or drill-down to view individual events.

Commander's data access can be shared with chosen registered users, and each can be assigned a security role.

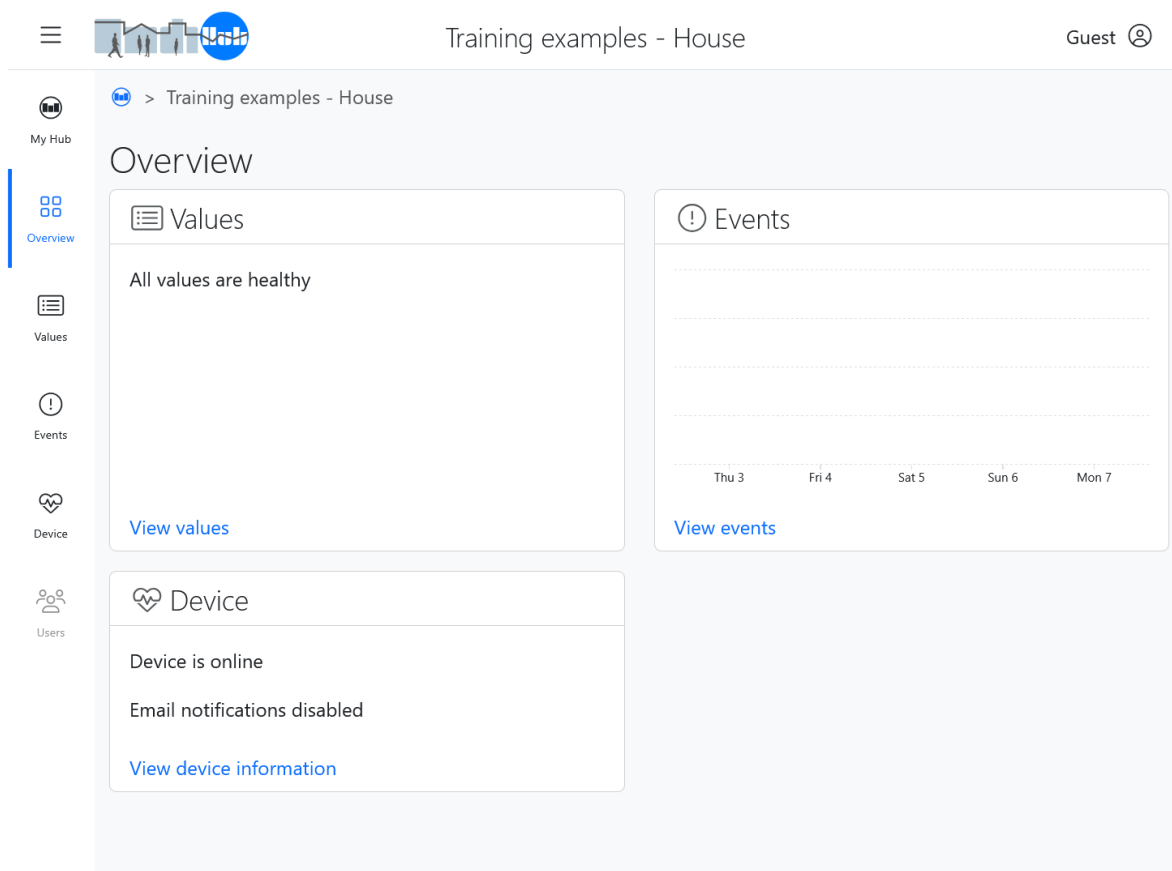


Fig 12 Page from Commander Hub

Security Server

When Commander is connected to a network, the engineer must consider security – to control who can and who cannot view and modify values, and who can engineer Commander itself.

North products, including Commander, that require user authentication have access to a central user database that holds user information. Remote doors could use this, for example, to ask the central user database for authentication when a user requires access.

Commander has Security Server, its own user database – it holds information, including privilege levels, for different users.

Commander's Security Server can support up to 400 users.

It is possible for a task within Commander to use a security server elsewhere in the system – for example in a different Commander or within a PC running ObSys.

User Information

Besides a name, each user has a user ID (or card) and a password – together these form a coded token. It is the coded token that is passed around a system – the password is never seen.

Each user is given eight privilege levels, one for each of eight different areas. The privilege level is in the range 0 (no security clearance) to 7 (maximum clearance).

Individual users can also be enabled or disabled and can be limited to access between certain dates – it is possible to see the last date that a security clearance was requested for the user.

Groups

Each user can be a member of up to three groups. Each group has a list of privilege levels, which act as a base level for users that are a member of the group. This allows a whole group of users to be controlled quickly and easily.

When groups are used, a user is enabled when any of the groups they are a member of is enabled (and the user is enabled).

The user's privilege level in a particular area is the highest level specified in that area from the individual user information and from any group they are a member of

Use by other Tasks

A task that requires security clearance will have one or more access security objects. Each access security object has a two-digit value, which controls access to a particular feature – such as adjusting a value or viewing a page.

The two-digit value is made up of the area digit (1-8), followed by the minimum privilege level (1-7). The user must have a privilege value equal to (or greater than) that specified, in the area specified, before the task will allow access to the feature.

For example, if the minimum privilege level is '6' in area '2', then the two-digit value is '26'. If the value is set to '00', then no security checks are needed.

When the user wants to access the protected feature, the following occurs:

- The task requests identification from the user: this may be done by asking for a name and password; or by scanning a security ID card
- The task encodes the identification, and requests the privilege levels for the user with that identification from the Security Server
- The task receives the eight privilege levels from the server
- The task checks whether the user's privilege level in an area is sufficient to allow access, and if so will grant access
- The task may send an alarm message, indicating whether the user was allowed, or whether the ID was not recognised.

Updating Commander's Firmware

When supplied, the Commander hardware contains the main system firmware released at the time of production, along with several popular North interface drivers. For a list of these factory installed drivers, see [Appendix B](#).

North provide other less-used drivers in separate CDM files, which you need to install before you can use them. North also release updated firmware which you may need to install.

You can set Commander to update its firmware from either North's cloud-services, if it has Internet access, or locally from a PC using the Trivial File Transfer Protocol (TFTP).



As Commander is intended for use in industrial environments, it will not automatically update its firmware as this could cause interference with operations. Instead, an engineer should periodically check for updates and subscribe to software release updates at northbt.link/news.

Before updating Commander's firmware, it must be in Program mode – the internal PROGRAM switch must be set to ON. We also recommend taking a complete backup of the Commander's configuration before updating any firmware.

Cloud Update

If Commander has Internet access, it can be instructed to check and update its firmware to the latest released version available from North's cloud-based servers.

Two different update options are available: the quickest is 'in-use only', and this updates the system firmware and started interfaces; the 'all factory' option updates the system firmware and all the factory-installed drivers.

To add a driver that has not been previously installed, add the driver name to an available Interface before updating the 'in use' firmware.

Updating Commander's firmware

-  To update Commander using North's cloud-based services, follow these steps:
 - Set the PROGRAM switch to ON, and re-power Commander
 - The MODE LED will blink, to show Commander is in Program mode
 - **Start Engineering** your North device using ObSys
 - From the top-level of Commander, navigate to **Configuration, Platform Information, Software Cloud Update**
 - Set **Check and Update Software** to either 'In-use only' or 'All factory installed' to have Commander update the firmware. DO NOT REMOVE THE POWER during this operation
 - Check **Progress** for the current update activity. Commander may restart several times during this time
 - Once completed, the **Check and Update Software** returns to 'Off', and **Progress** shows how many files were updated
 - Set **PROGRAM** switch to OFF, and re-power Commander.

TFTP Update

Commander supports local updates using the Trivial File Transfer Protocol (TFTP). Use TFTP when no Internet connection is available, or a driver is unavailable via cloud update.

TFTP is one of the standard IP protocols. TFTP requires a client (your PC) and a server (Commander).



TFTP is disabled by default, on both your PC and Commander.

Temporarily enable TFTP when required.

Enable TFTP on your PC

Before you can use the TFTP client on your PC, it must first be enabled in Windows.

A shortcut is available to enable TFTP on your PC. Open **Configuration, Interfaces**. Select **Extras, Enable TFTP Client on Windows**.

Locating the CDM Files

North distributes drivers for Commander in CDM files – these files are made to work in certain areas of Commander’s memory – called banks. You can only load one CDM file per bank, so you must choose which CDM to load in each bank.

ObSys setup installs CDM files within the CDMs folder of the ObSys Program Files folder – for example “C:\Program Files (x86)\North Building Technologies\ObSys\CDMs”.

A shortcut to the CDMs folder is available. Open **Configuration, Interfaces**. Select **Extras, Open CDM folder**.

Installing or Updating a CDM

Once you have chosen the CDM file, enable TFTP in Commander and send the file.

If you need to update the system firmware, download three files: *Bank 1.cdm*, *CmdrBase.bin*, then *CmdrExt.bin*.

The easiest way to install or update a CDM is to use the supplied batch file with Commander in Default IP mode.

-  To load a CDM in Default IP mode, follow these steps:
 - Set the internal **PROGRAM** switch to ON, then enable TFTP by setting **DEFAULTIP** switch ON. Commander will re-start
 - The MODE LED will blink, to show Commander is in Program and Default IP mode
 - Open the CDMs folder. A shortcut is available from **Configuration, Interfaces**. Select **Extras, Open CDM folder**
 - Within the CDMs folder, you will find a Windows batch file called *Update Commander at default IP address*. To update Commander, simply drop a CDM file on to this file.
 - Once Commander has received and checked the file, Commander will write the CDM to flash memory (lighting its SAVE LED), and when complete, will restart, and the MODE LED will blink to show it is in Program mode again
 - Repeat the TFTP command for any other files to send
 - Set the internal **PROGRAM** and **DEFAULTIP** switch to OFF
 - Re-power Commander.

Alternatively, you can install or update a CDM when Commander is connected to a network.

-  To load a CDM to Commander on a network using your TFTP client, follow these steps:
 - Set the internal **PROGRAM** switch to ON, and re-power Commander
 - Enable TFTP in Commander from the top-level of Commander, open **Configuration, LAN Port** and set **TFTP Enabled** to 'Yes'
 - The MODE LED will blink, to show Commander is in Program mode
 - On your PC start **Terminal** app
 - At the prompt, type the following to change to the CDMs folder:
`cd "\Program Files (x86)\North Building Technologies\ObSys\CDMs"`
 - Type the following format TFTP command to send a file:
`TFTP -i <ip address> PUT "<filename>"`
For example:
`TFTP -i 192.168.2.150 PUT "Bank3 H 200611 OmronPLC.cdm"`
 - Once Commander has received and checked the file, Commander will write the CDM to flash memory (lighting its SAVE LED), and when complete, will restart, and the MODE LED will blink to show it is in Program mode again
 - Repeat the TFTP command for any other files to send
 - Close the Terminal window
 - Set the internal **PROGRAM** switch to OFF
 - Disable TFTP in Commander by setting **TFTP Enable** to 'No'
 - Re-power Commander.

Removing all Data from Commander



At the end of the Commander's useful life, before you recycle it, you can wipe both the default configuration and battery-backed memory.

If you only remove the battery, Commander will reload the default configuration from permanent memory when re-powered.

-  To remove all data from Commander, follow these steps:
- Set the internal **PROGRAM** switch to ON and restart Commander
 - The MODE LED will blink, to show Commander is in Program mode
 - From the top-level of Commander, open **Configuration, Platform Information, Default Configuration**
 - Set the **Save Configuration As** to 'blank' (case sensitive) to delete the default configuration
 - After one minute, or less, **Saved Configuration** shows an empty value ("") and **Saved Time** '00/00/00 00:00:00'. The default configuration has successfully been deleted
 - Remove the battery from Commander
 - Disconnect the power from the Commander for at least 1 minute
 - All data from Commander has now been deleted.

Object Specifications

Once Commander has started, several objects become available within the top-level object of the device. These objects may contain sub-objects (and each of these may contain sub-objects, and so on) – the whole object structure being a multi-layer hierarchy. It is possible to navigate around the objects using the ObSys Engineering Software.

Each object is specified below, along with its sub-objects.

Example Object Reference

An example of a reference to an object within Commander: the Configuration object (O) contains Platform Information (PI), which contains Commander Version (PV) – therefore the complete object reference is ‘O.PI.PV’.

An example of a reference to an object in a different device: the IP network object (IP) contains Default Commander object (CDIP), which contains the object above (O.PI.PV) – therefore the complete object reference is ‘IP.CDIP.O.PI.PV’.

Device Top-Level Objects

Object Type: *[Commander v20\Device]*

When Commander is powered-on, the objects below become available within the top-level object of the device.

Description	Reference	Type
Commander Label Label used to identify this device, including scanning and within alarms. Adjust within the Configuration object.	PL	Obj\Text; Max. 30 chars
Configuration Set up Commander’s main features	O	Variable Container: <i>[Commander v20]</i>
Essential Values Contains the values configured within Essential Data	UD	Variable Container: <i>[UserData\PageList]</i>
Time Control Time and date based control using calendar, timers and profilers	CT	Variable Container: <i>[CalTimer v20]</i>
ObVerse Contains public properties configured in ObVerse Processor x. This object is only available once ObVerse has been downloaded to the processor. The processor number, x is in the range 1...2. ObVerse is set in public property L within the ObVerse.	Px	Variable Container: Type is based on the filename of the ObVerse. For example, if saved as the file ‘TypeInfo\ObVerse\Process.obv’, then the type will be: <i>[ObVerse\Process]</i>
Security Server Edit users and groups in the database for authentication	TK	Fixed Container: <i>[TokenMax v20\400]</i> <i>[TokenMax v20\100]</i>
Data Transfer Transfer values from one place to another	TX	Fixed Container: <i>[TransMax v14\500]</i> <i>[TransMax v14\100]</i>
Alarm Delivery Configure destinations to route alarm events	AR	Fixed Container: <i>[AlmRoute v11]</i>
Alarm History Contains a list of the latest alarms received	AH	Fixed Container: <i>[AlarmHistory v11\100]</i>

Description	Reference	Type
Alarm Emailer Destination for alarms to be emailed to a recipient	AE	Variable Container: [AlmEmail v22]
North IP Devices Available North IP-compatible devices on the network	IP	Variable Container: [IpBus Net]
Interface Setup Set up the driver, started on interface c. This object is only available once an interface has been started. The interface number, c, is in the range 1...4	Mc	Fixed Container: Refer to specific driver manual for type
Interface System Access the system connected to interface c. This object is only available once an interface has been started. The interface number, c, is in the range 1...4	Sc	Fixed or Variable Container: Refer to specific driver manual for type

Configuration

Object Type: *[Commander v20]*

The Commander Configuration object contains the following objects:

Description	Reference	Type
Label Label used to identify this device, including scanning and within alarms	PL	Obj\Text; Max. 30 chars; Adjustable
Local Date & Time Local date and time from Commander's real-time-clock	T	Obj\DateTime; Adjustable
Platform Information General information about Commander, including hardware switches	PI	Fixed Container: <i>[Commander v20\Platform v15]</i>
LAN Port Set up Commander's LAN port, including IP address	N	Fixed Container: <i>[Commander v20\DynamicLAN v13]</i>
UTC & Daylight Savings Set the time and date, UTC offset, and add daylight saving periods	TZ	Fixed Container: <i>[Commander v20\TimeZone v10]</i>
Interfaces Start an interface, list installed drivers, and review interface licence information	O	Fixed Container: <i>[Commander v20\Interfaces v10]</i>
Commander Hub Enabling link to Commander Hub, and monitoring activity	CS	Fixed Container: <i>[Commander v20\CloudSvc v10]</i>
Web Server Enable the web server, edit security, and select the features available from the web site	WS	Fixed Container: <i>[CDM v20\C2Web v31]</i>
Essential Data Configure the database of values used by multiple Commander modules	UD	Fixed Container: <i>[CDM v20\UserData v31\Format0]</i> <i>[CDM v20\UserData v31\Format1]</i> <i>[CDM v20\UserData v31\Format2]</i> <i>[CDM v20\UserData v31\Format3]</i>
Time Control Set the system label and access security	CT	Fixed Container: <i>[CDM v20\CalTimer v20]</i>
ObVerse Processor x Edit the ObVerse for this processor. Where x is in the range 1...2	Px	Fixed Container: <i>[CDM v20\OBVProcess v11]</i>
Security Server Set the label and maximum users available	TK	Fixed Container: <i>[CDM v20\TokenMax v20]</i>
Data Transfer Set the system label, maximum transfers available, and tasks	TX	Fixed Container: <i>[CDM v20\TransMax v14]</i>
Alarm Delivery Set the system label	AR	Fixed Container: <i>[CDM v20\AlmRoute v11]</i>
Alarm History Set the system label and access security	AH	Fixed Container: <i>[CDM v20\AlarmHistory v11]</i>
Alarm Email Configure the SMTP server parameters and destination recipient address	AE	Fixed Container: <i>[CDM v20\AlarmEmail v22]</i>
North IP Devices Manage the list of connected IP devices	IP	Fixed Container: <i>[CDM v20\IpBus v22]</i>

Platform Information

Object Type: [Commander v20\Platform v15]

Object Type: [Commander v20\Platform v14]

The Platform Information object provides *general information about Commander*.

Description	Reference	Type
Commander Version The Commander's main firmware version and release date	PV	Obj\Text
Hardware Version Version number of Commander's physical hardware	HV	Obj\Float
Hardware Mode State of the internal switches – DEFAULTIP and PROGRAM	M	Obj\Enum; Range 0...3 Values: 0=Run, 1=Program mode, 2=Default IP, 3=Program mode & Default IP
Battery State Health of the internal battery. Replace when low. Value refreshed every 60s.	BS	Obj\Enum; Range 0...3 Values: 0=Ok, 1=Low, 2=Very Low, 3=Unknown
Reset Platform Set to perform a soft reset of Commander. Value indicates the seconds before restart	!rst	Obj\Num; Range 0...1000
Default Configuration Save current engineered settings as the default configuration	DC	Fixed Container: [Commander v20\Platform v15\DefCon]
Last Restart Information about the last restart	LR	Fixed Container: [Commander v20\Platform v15\Restart]
Software Versions Software versions for each of Commander's main modules and started interfaces	V	Fixed Container: [Commander v20\Platform v15\Versions]
Software Cloud Update Check and update Commander firmware from North's servers	SU	Fixed Container: [Commander v20\Platform v15\Update]
Recording Enable debug recording, and select which information is recorded	R	Fixed Container: [Commander v20\Platform v15\Record]

Alarm Fields

Alarms are sent by Commander when the battery state reaches a low condition. The Platform Information module places the following information into the North-format fields:

System – 'Commander'

Point – 'Battery'

Condition – either 'Very Low', 'Low', or 'OK'

Priority – '2' for Very Low, '3' for Low and OK conditions

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Commander	Battery	Low	3	23/03/15	13:33:59
Commander	Battery	Very Low	2	15/04/15	07:30:16
Commander	Battery	OK	3	18/04/15	10:15:24

Default Configuration

Object Type: [Commander v20\Platform v15\DefCon]

Object Type: [Commander v20\Platform v14\DefCon]

Object Type: [Commander v20\Platform v13\DefCon]

A Default Configuration object holds details of the current default configuration stored in permanent memory.

Commander's configuration is held in battery-backed memory. If the battery expires (or is removed) when the external power is removed, the configuration is lost. To counter this loss, save the current configuration to permanent memory. Once saved, whenever the configuration in battery-backed memory is lost, it is reloaded from the default configuration in permanent memory.

Before saving the configuration, set the internal PROGRAM switch ON and restart Commander. When saving the configuration, Commander will light the **SAVE LED** for 20-30 seconds, then restart.

Default Configuration is available with Commander hardware version 2.0 or later.

Description	Reference	Type
Saved Configuration Label used when saving the default configuration	LL	Obj\Text: Max 30 chars
Saved Time Date and time the default configuration was last saved	LT	Obj\DateTime
Save Configuration As Set a label to cause the configuration to be written to permanent memory. Set to 'blank' (case sensitive) to reset the default configuration back to factory settings	NL	Obj\Text: Max 30 chars; Adjustable (in PROGRAM mode) Value 'n/a' indicates save configuration is not available due to PROGRAM switch or hardware version.

Last Restart

Object Type: [Commander v20\Platform v15\Restart]

Object Type: [Commander v20\Platform v14\Restart]

Object Type: [Commander v20\Platform v13\Restart]

Object Type: [Commander v20\Platform v12\Restart]

Object Type: [Commander v20\Platform v11\Restart]

A Last Restart object contains information about the last time Commander was powered-up or reset.

Description	Reference	Type
Last Start Date & Time	ST	Obj\DateTime
Reset Count Number of times Commander has been restarted	RC	Obj\Num
Reset Reason The reason for the last reset	RR	Obj\Enum; Range 0...2 Values: 0=Power failure, 1=User reset, 2=Watchdog

Software Versions

Object Type: *[Commander v20\Platform v15\Versions]*

Object Type: *[Commander v20\Platform v14\Versions]*

Object Type: *[Commander v20\Platform v13\Versions]*

Object Type: *[Commander v20\Platform v12\Versions]*

Object Type: *[Commander v20\Platform v11\Versions]*

A Software Versions object holds the version and release date of the sub-components within Commander, and contains the following objects:

Description	Reference	Type
Web Server	WS	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Essential Data	UD	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Time Control	CT	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
ObVerse Processor	P1	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Security Server	TK	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Data Transfer	TX	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Alarm Delivery	AR	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Alarm History	AH	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Alarm Email	AE	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
North IP Devices	IP	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>
Interface x Where x is in the range 1...4	Mx	Fixed Container: <i>[Commander v20\Platform v15\Detail]</i>

Software Version Detail

Object Type: *[Commander v20\Platform v15\Detail]*

Object Type: *[Commander v20\Platform v14\Detail]*

Object Type: *[Commander v20\Platform v13\Detail]*

Object Type: *[Commander v20\Platform v12\Detail]*

Object Type: *[Commander v20\Platform v11\Detail]*

A Software Version Detail object contains the following objects:

Description	Reference	Type
Driver Version Software component name, version and release date	DV	Obj\Text; Max chars 32
CDM Surround Version Common library version and release date	PV	Obj\Text; Max chars 32

Software Cloud Update

Object Type: [Commander v20\Platform v15\Update]

Object Type: [Commander v20\Platform v14\Update]

The Software Cloud Update object enables Commander to start updating its software from North's servers.

Before starting to Check and Update the software, set PROGRAM switch to ON, and confirm an Internet connection is available.

Select one of the following to start the software update:

- In-use only – update started interfaces and system firmware
- All factory installed – updates drivers installed at production time and system firmware, excludes any additional drivers installed.

Software Cloud Update is available with Commander hardware version 2.0 or later.

Description	Reference	Type
Check and Update Software Start checking and updating the selected software	AU	Obj\Enum; Adjustable Where: 0=Off, 1=In-use only, 2=All factory installed
Progress Indicates progress of update	TI	Obj\Text Value 'n/a' indicates save configuration is not available due hardware version.

Recording Configuration

Object Type: [Commander v20\Platform v15\Record]

Object Type: [Commander v20\Platform v14\Record]

Object Type: [Commander v20\Platform v13\Record]

Object Type: [Commander v20\Platform v12\Record]

Object Type: [Commander v20\Platform v11\Record]

The Recording Configuration object enables *debug recording* for Commander.

An ASCII terminal, or PC running terminal software, is needed to receive the debug information. The terminal needs to be set to 38400 baud, no parity, 8 data-bits, 1 stop-bit, and no hardware flow control.

An RS232 null-modem cable is required to connect the terminal software to Commander.

CAUTION: Beware of enabling all record options, particularly Record COMs (C), as this can put a significant loading on Commander.

Description	Reference	Type
Record to Port COM port to send debug text to. Do not select a COM port already in use by an interface	P	Obj\Enum; Range 0...2; Adjustable Values: 0=Off, 1=COM1, 2=COM2
Record Information Record general information such as Commander starting	I	Obj\NoYes; Adjustable
Record Objects Record object request and reply messages between modules, plus any other additional debug messages from a driver	O	Obj\NoYes; Adjustable
Record COMs Record bytes sent and received on COM ports	C	Obj\NoYes; Adjustable
Record Network Record Ethernet information and IP events such as ARP, DNS, etc.	N	Obj\NoYes; Adjustable
Record Internal Comms Record fast request/reply messages between internal modules	T	Obj\NoYes; Adjustable

LAN Port Configuration

Object Type: *[Commander v20\DynamicLAN v13]*

A LAN Port Configuration object allows the *set-up of Commander's LAN port*, including selecting how the IP address is assigned.

After changing the LAN Port objects, reset Commander for the new values to take effect.

Description	Reference	Type
Label Fixed label 'LAN Port' – for compatibility with ObSys	L	Obj\Text; Max chars 20
Link Status Whether the link is down or the result of successful auto-negotiation, including link speed and duplex mode	S	Obj\Enum Value: 0=Down, 1=10M-half, 2=10M-full, 3=100M-half, 4=100M-full
Current IP Address IP address currently in use	CIA	Obj\IP
IP Address Assign a static IP address, or '0.0.0.0' to request a dynamic IP address from a DHCP server	IA	Obj\IP; Adjustable
Subnet Mask Subnet mask to use with a static IP address, e.g. '255.255.255.0' for class C networks	IM	Obj\IP; Adjustable
Gateway Address Gateway IP address to use in static IP mode	IG	Obj\IP; Adjustable
DNS Server Address Domain name server IP address to use in static IP mode, or if not supplied by a DHCP server. If no DNS server address is known, Commander will attempt to use 1.1.1.1	ID	Obj\IP; Adjustable
Time Server Address NTP server IP address to use in static IP mode, or if not supplied by a DHCP server. If no NTP server address is known, Commander will try to use DNS to resolve pool.ntp.org to find one	IT	Obj\IP; Adjustable
Max. Auto-negotiation Speed Whether to limit the link auto-negotiation to a maximum speed. Note: Requires a reset of Commander to use this setting Note: Not used in Default IP mode	SL	Obj\Enum; Adjustable Value: 0=No maximum, 1=10Mbps
MAC Address Physical address (MAC) of Commander's LAN port	MAC	Obj\Text; Format: <i>hh:hh:hh:hh:hh:hh</i> where <i>h</i> is a hexadecimal digit
TFTP Enable Enable TFTP, for updating firmware. The Commander also must be in PROGRAM mode to allow TFTP download	TFE	Obj\NoYes; Adjustable
DHCP Server Information about the DHCP Server operation. The DHCP Server only operates when the Commander is in DEFAULTIP mode	DS	Fixed Container: <i>[Commander v20\DHCP Svr v10]</i>

DHCP Server

Object Type: *[Commander v20\DHCP Svr v10]*

A DHCP Server object contains information about the Commander's built-in DHCP Server. The DHCP Server only operates when the Commander's DEFAULTIP switch is on.

The Commander's DHCP Server can automatically give an IP address to a connected engineering tool using DHCP. The DHCP Server can be disabled if required.

Description	Reference	Type
DHCP Server Enable Whether the DHCP Server should be enabled when the Commander is in DEFAULTIP mode	E	Obj\NoYes; Adjustable If set to 'No', all Leases are cleared
Lease x Information about Lease x, where x is in the range 1...16	Lx	Fixed container: <i>[Commander v20\DHCP Svr v10\Lease]</i>

DHCP Server Lease

Object Type: *[Commander v20\DHCP Svr v10\Lease]*

A DHCP Server Lease object contains information about a lease of an IP address to a device, and contains the following objects:

Description	Reference	Type
Client IP Address The IP address given to a client. The lease may be currently in use or remembered for future leases	IA	Obj\NoYes; Adjustable If any value is written to this object, all values within the lease are cleared
MAC Address The physical hardware or MAC address of the client, either currently in use or remembered for future leases	MAC	Obj\Text; Format: <i>hh:hh:hh:hh:hh:hh</i> where <i>h</i> is a hexadecimal digit
Lease Offered or Renewed The date and time of the last offer or renewal.	T	Obj\DateTime

UTC & Daylight Savings Configuration

Object Type: [Commander v20\TimeZone v10]

A UTC & Daylight Savings object configures *Commander's real-time clock and time zone*, including Coordinated Universal Time (UTC), local time offset, local time, and daylight saving offsets.

Description	Reference	Type
UTC Commander's built-in clock date & time in Universal Coordinated Time	UTC	Obj\DateTime; Adjustable
Local Time Offset from UTC Offset time in hours and minutes to apply to UTC in order to calculate local time	LTO	Obj\Text; Adjustable Value in the format: '+hh:mm' or '-hh:mm'
Daylight Saving Offset Current daylight saving offset applied to local time	DSO	Obj\Text Value in the format: '+hh:mm' or '-hh:mm'
Local Time Commander's local time based on UTC, local time offset, and daylight saving offset	LT	Obj\DateTime
Daylight Saving x Time Date and time to apply the daylight saving offset. Daylight saving index, x, is in the range 1...20	Dx.T	Obj\DateTime; Adjustable
Daylight Saving x Offset Daylight saving offset to apply. Daylight saving index, x, is in the range 1...20	Dx.O	Obj\Text; Adjustable; in the format +HH:MM or -HH:MM
Last Time Sync Source Method last used to update Commander's time and date. If Commander has access to an NTP time server, it will automatically correct its clock	TSS	Obj\Enum Value: 0=Never, 1=Object, 2=NTP server, 3=Other
Days Since Time Adjusted Period since Commander's date and time was last updated	TSD	Obj\Num

Interfaces Configuration

Object Type: [Commander v20\Interfaces v10]

The Interfaces Configuration object allows Commander to *start interfaces to other systems*, list the installed drivers, and review licencing information.

Description	Reference	Type
Interface x Name of driver to start at interface x, where x is in the range 1...4	Ox	Obj\Text; Max. 16 char; Adjustable
Installed Drivers List of installed drivers	A	Fixed Container: [Commander v20\Interfaces v10\Avail]
Interface Licences Licencing information and upgrade	IL	Fixed Container: [Commander v20\Interfaces v10\IntLic]

Installed Drivers

Object Type: [Commander v20\Interfaces v10\Avail]

An Installed Drivers object contains the following objects:

Description	Reference	Type
Installed Driver List of drivers available. The list index, x, is in the range 1...250	Ax	Obj\Text; Max chars 16; Adjustable

Interface Licences

Object Type: [Commander v20\Interfaces v10\IntLic]

Each Commander is supplied with a certain number of *interface licences*. It is possible to add more licences on site, although a phone call is required to check/verify settings.

Call North support on +44 (0) 1273 694422 for more help with adding more licences.

Description	Reference	Type
Serial Number Commander's unique serial number	S	Obj\Text; 8 chars
Total Licences Total number of interface licences installed	T	Obj\Num; in the range 0...4
Available Licences Number of interface licences available. Each started interface will typically use one licence	A	Obj\Num; in the range 0...4
Upgrade Licences Key used to add more interface licences	U	Obj\Text; Max chars 32; Adjustable

Commander Hub

Object Type: [Commander v20\CloudSvc v10]

The Commander Hub object enables the sending of data to [Commander Hub](#), part of North's cloud-based services. It requires access to the Internet, and a valid DNS server.

By enabling the link to Commander Hub, you agree to have read and understand the [Terms of Use](#) and [Privacy Policy](#). If you disable the link, all sending of data between Commander and the Hub will stop.

To add a new Commander to your Hub account, wait for the Registration Code (T) object to update with a value. This may take approximately 15 - 30 minutes after you have enabled the link, or longer if default configuration has been saved. Once the registration code is available, visit the [My Hub](#) page, select **Options, Add device**, and enter the information requested.

If the Commander has already been added to another user's account, give them your Hub username and ask them to share access with you.

Commander Hub is available with Commander hardware version 2.0 or later.

Description	Reference	Type
Enable Link Enables or disables the link to Commander Hub. By enabling the link to Commander Hub, you agree to have read and understand the Terms of Use and Privacy Policy .	E	Obj\NoYes; Adjustable
Collecting Information on which data Commander is currently collecting prior to sending to Hub	C	Obj\Text
Link to Hub Provides information on the communications link with Commander Hub	I	Obj\Text
Serial Number Commander's unique serial number	S	Obj\Text: 8 chars
Registration Code Unique registration code to add this device to Commander Hub. The code will be regenerated after each restart.	T	Obj\Text

Web Server Configuration

Object Type: *[CDM v20\C2Web v31]*

The Web Server Configuration object enables *Commander's web server* and selects what information is accessible from it.

By default the web server is turned off, but can be turned on by selecting the appropriate access required from local and remote networks. To reduce security risk, select the minimum level of access needed.

Description	Reference	Type
Access from Local Network Control access to the web server from devices on the local network – an IP address on the same subnetwork as Commander	E.L	Obj\Enum; Adjustable Values: None,View,View and adjust Default: None
Access from Remote Networks Control access to the web server from devices on a remote network – an IP address with a different subnetwork address than Commander	E.R	Obj\Enum; Adjustable Values: None,View,View and adjust Default: None
Show Alarm History Enables access to alarm history from the website	E.AH	Obj\NoYes; Adjustable
Content Configure options to customise the overview page	C	Fixed Container: <i>[CDM v20\C2Web v31\Content]</i>
Security Configure sign-in and security options	S	Fixed Container: <i>[CDM v20\C2Web v31\Security]</i>
Information Website usage information	I	Fixed Container: <i>[CDM v20\C2Web v31\Info]</i>

Web Server Content

Object Type: *[CDM v20\C2Web v31\Content]*

Object Type: *[CDM v20\C2Web v30\Content]*

A Web Server Content object contains the following objects to customise the site title, and links.

Description	Reference	Type
Title Site title to display. If not specified, then the Commander's Label is shown	T	Obj\Text; Max chars 55; Adjustable
Link x Name Text label for external link x. The link number, x, is in the range 1..5	Lx.N	Obj\Text; Max. 63 chars; Adjustable
Link x URL Resource location for external link x. The link number, x, is in the range 1..5 Examples resources: 'https://www.northbt.com', 'tel:+441273694422', 'mailto:support@northbt.com', etc.	Lx.U	Obj\Text; Max. 126 chars; Adjustable

Web Server Security

Object Type: *[CDM v20\C2Web v31\Security]*

Object Type: *[CDM v20\C2Web v30\Security]*

The Web Server Security object contains *security settings* to enable user sign-in and control access to the server.

Description	Reference	Type
Require Sign-in Enable website authentication using the Security Server	E	Obj\NoYes; Adjustable Default: No
Active Users Number of users currently signed-in	AS	Obj\Num
Sign-out Active Users Set 'Yes' to sign-out all active users	CS	Obj\NoYes; Adjustable
Allow Password Change Enables change password option when user is signed-in	EU	Obj\NoYes; Adjustable
Security Server Object Object reference of a Security Server. Typically, this is set to 'TK' for local Commander, but could be set to the object of a central server	RO	Obj\Obj; Adjustable
Default Access Security Set privilege levels for when user sign-in is not enabled	D	Fixed Container: <i>[CDM v20\C2Web v31\DefaultAccess]</i>

Web Server Default Access Security

Object Type: *[CDM v20\C2Web v31\DefaultAccess]*

Object Type: *[CDM v20\C2Web v30\DefaultAccess]*

Object Type: *[CDM v20\C2Web v20\DefaultAccess]*

Object Type: *[CDM v20\C2Web v11\DefaultAccess]*

A Web Server Default Access Security object contains the privilege levels to use when the user sign-in option is not enabled.

Description	Reference	Type
Privilege Level in Area x The area, x, is in the range 1...8	Px	Obj\Num: 0...7; Adjustable

Web Server Information

Object Type: [CDM v20\C2Web v31\Info]

Object Type: [CDM v20\C2Web v30\Info]

A Web Server Information object contains usage information.

Description	Reference	Type
Pages this period Number of pages served over the current period. Where (<i>a</i>) <i>period</i> is: (1) hour, (2) day, (3) week, (4) month.	P.Ca	Obj\Num
Pages previous period Number of pages served over the previous period. Where (<i>a</i>) <i>period</i> is: (1) hour, (2) day, (3) week, (4) month.	P.Pa	Obj\Num
Sessions this period Number of sessions over the current period. Where (<i>a</i>) <i>period</i> is: (1) hour, (2) day, (3) week, (4) month.	S.Ca	Obj\Num
Sessions previous period Number of sessions over the previous period. Where (<i>a</i>) <i>period</i> is: (1) hour, (2) day, (3) week, (4) month.	S.Pa	Obj\Num
Reset counters Set page and session counters to 0	RC	Obj\NoYes; Adjustable
Active Sessions Current number of active sessions	S.A	Obj\Num

Essential Data Configuration

Object Type: *[CDM v20\UserData v31\Format0]*

Object Type: *[CDM v20\UserData v31\Format1]*

Object Type: *[CDM v20\UserData v31\Format2]*

Object Type: *[CDM v20\UserData v31\Format3]*

Object Type: *[CDM v20\UserData v30\Format0]*

Object Type: *[CDM v20\UserData v30\Format1]*

Object Type: *[CDM v20\UserData v30\Format2]*

Object Type: *[CDM v20\UserData v30\Format3]*

The Essential Data object contains the configuration for *Commander's database of values*.

Essential Data consists of a list of configurable pages, each of which has a list of configurable objects. In total 640 database objects are available.

Description	Reference	Type
Essential Data Label	DL	Obj\Text; Max chars 20; Adjustable
Page x Object Layout Arrangement of pages and objects within the database. Choose from 40 pages of 16 objects (default), 64 pages of 10 objects, 20 pages of 32 objects, or 10 pages of 64 objects. Rescan the Commander Configuration and this object after changing the value	PO	Obj\ENum; Adjustable Values: 0=40x16, 1=64x10, 2=20x32, 3=10x64
Alarm State Overall alarm state of all pages within the database – out-of-range alarm, communications fault	S	Obj\ENum; Range 0...3 Values: 0=Ok, 1=Alarm, 2=Comms, 3=Alarm & Comms
Log Channels Free Count of available object logging channels	FL	Obj\Num; Range 0...40
Page x Configure database page x. Where x is in the range 1...64, depending on Page x Object Layout object (PO) above	Px	Fixed Container: 40 page x16 object layout <i>[CDM v20\UserData v31\PageDef0]</i> 64 page x10 object layout <i>[CDM v20\UserData v31\PageDef1]</i> 20 page x32 object layout <i>[CDM v20\UserData v31\PageDef2]</i> 10 page x64 object layout <i>[CDM v20\UserData v31\PageDef3]</i>
Task Control Allows control and monitoring of the module's operation	TI	Fixed Container: <i>[CDM v20\UserData v31\TaskInfo]</i>

Essential Data Page Configuration

Object Type: [CDM v20\UserData v31\PageDef0]

Object Type: [CDM v20\UserData v31\PageDef1]

Object Type: [CDM v20\UserData v31\PageDef2]

Object Type: [CDM v20\UserData v31\PageDef3]

Object Type: [CDM v20\UserData v30\PageDef0]

Object Type: [CDM v20\UserData v30\PageDef1]

Object Type: [CDM v20\UserData v30\PageDef2]

Object Type: [CDM v20\UserData v30\PageDef3]

The Essential Data Page object contains the configuration for a page within *Commander's database of values*. Each page has a label, access security, remote object prefix, and up to 64 objects.

The Remote Object Prefix (RP), if set, applies a root object to all remote objects within the page. It allows the page to deal with a particular container object, for example an energy meter or fan coil, without the need to enter the full object reference. A benefit of this is that the same page can be copied and used like a template for similar devices. Then by only changing the Remote Object Prefix the same information from an energy meter or fan coil at a different address can be accessed.

When the Remote Object Prefix (RP) is set, then Essential Data uses this to optimize communications in a fault condition. When Object 1 (O1) is in a communications fault alarm state, then only this object on the page performs the remote action – the other objects on the page will automatically fail. Once this first object is communicating again, then normal operation will resume.

Description	Reference	Type
Label Required to enable the page to other modules	L	Obj\Text; Max chars 20; Adjustable
Remote Object prefix Optional prefix to add in front of each database object's Remote Object	RP	Obj\Obj; Adjustable
Access Security Area and minimum privilege level required to read all objects within the page from other modules. See <i>Security Server</i>	AS	Obj\Num; Range 0, 10...87; Adjustable
Page Alarm State Overall alarm state of all objects within the page – out-of-range alarm, communications fault	S	Obj\ENum; Range 0...3 Values: 0=Ok, 1=Alarm, 2=Comms, 3=Alarm & Comms
Comms Alarm Enable/Priority Enables communications fault alarms for the page, see below	P	Obj\Num; Range 0...9; Adjustable Values: 0=no alarms are sent, 1...9=alarm priority (1 is the highest alarm priority, and 9 is the lowest)
Object x Configure database object x. Where x is in the range 1...64, depending on Page x Object Layout object (PO)	Ox	Fixed Container: <i>[CDM v20\UserData v31\ObjDef]</i>

Alarm Fields

Alarms can be sent by the page to indicate the communication state of objects within the page.

The Essential Data module places the following information into the North-format fields:

System – from the Essential Data Label object (DL)

Point – from the page's Label object (L)

Condition – either 'Communications Fault' or 'Communications Ok'

Priority – set using Comms Alarm Enable/Priority object (P)

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Essential Values	Air conditioning	Communications Fault	3	23/03/15	13:33:59
Essential Values	Air conditioning	Communications Ok	3	24/03/15	07:30:16

Essential Data Object Configuration

Object Type: [CDM v20\UserData v31\ObjDef]

Object Type: [CDM v20\UserData v30\ObjDef]

Essential Data Object contains the configuration for an object within *Commander's database of values*.

Essential Data allows the engineer to configure a list of values that other Commander modules can then distribute – as web pages, as BACnet points, as Modbus points, on Zip displays...

Description	Reference	Type
Label Required to enable the object to other modules	L	Obj\Text; Max. 20 chars; Adjustable
Type Specifies the type of value that the database object should hold	T	Obj\Enum; Range 0..9; Adjustable Values: 0=Text, 1=NoYes, 2=OffOn, 3=Number, 4=Float, 5=Times, 6=DateTime, 7=Date, 8=Enum, 9=Profile
Adjustable Specifies whether the user can adjust the value from other modules	A	Obj\NoYes; Adjustable
Units Optional unit of measurement	U	Obj\Text; Max. 8 chars
Access Security Area and minimum privilege level required to adjust the object from other modules. See Security Server	AS	Obj\Num; Range 0, 10...87; Adjustable
Type Enum Alternatives When Type is 'Enum', set this to a comma-separated list of value labels. i.e. 'value-0,value-1,value-2', etc.	EA	Obj\Text; Max. 30 chars; Adjustable
Type Float Dps/Time Periods When Type is 'Float', set this to the number of decimal places to display the current value. With 5 = 0.5 steps When Type is 'Times' or 'Profile', set this to the number of on-off or time-value periods.	D	Obj\Num; Adjustable Type Float: Range 0...5 Type Times: Range 0...4 Type Profile: Range 0...8
Value High Limit Used as alarm limits, if alarms are enabled, and used as value limits when adjustments are made	VH	Obj\Float; Decimal places=4; Adjustable
Value Low Limit Used as alarm limits, if alarms are enabled, and used as value limits when adjustments are made	VL	Obj\Float; Decimal places=4; Adjustable
Current Value Database object's value	V	Obj\Text; Max chars 32; Adjustable
Value Alarm State Delay Duration the Current Value must remain outside the alarm limits, before Value Alarm State is set to an out-of-range alarm NOTE: Only available in v3.1 and later	AD	Obj\Enum: 0...9; Adjustable Values: 0=None, 1=1 sec, 2=5 secs, 3=15 secs, 4=1 min, 5=5 mins, 6=15 mins, 7=1 hr, 8=4 hrs, 9=12 hrs
Value Alarm State Object's alarm state – out-of-range alarm, communications fault	S	Obj\Enum; Range 0...3 Values: 0=Ok, 1=Alarm, 2=Comms, 3=Alarm & Comms
Value Last Updated Time and date the current value was last set, either by a user or remote action	VT	Obj\DateTime

Description	Reference	Type
Value Alarm Enable/Priority Enables out-of-range value alarms, see below	P	Obj\Num; Range 0...9; Adjustable Values: 0=no alarms are sent, 1...9=alarm priority (1 is the highest alarm priority, and 9 is the lowest)
Remote Action Selects that the current value is periodically read from or written to the Remote Object. When set to 'read', and Adjustable to 'yes', then the current value will also be written to the Remote Object when adjusted by a user.	RA	Obj\Enum; Range 0...2; Adjustable Values: 0=None, 1=Read, 2=Write
Remote Object Object reference to read or write. If the Page has a remote object prefix set, then this will be inserted before the Remote Object	RO	Obj\Obj; Adjustable
Remote Rate Frequency to read or write the Current Value. If Remote Action is 'write', then the value is always written on a change-of-value. Set a rate to perform an additional background write periodically.	RR	Obj\Enum; Range 0...9; Adjustable Values: 0=ASAP/COV, 1=1 sec, 2=5 secs, 3=15 secs, 4=1 min, 5=5 mins, 6=15 mins, 7=1 hr, 8=4 hrs, 9=12 hrs
Remote Fails Count of times the remote object has continuously failed to read or write	RF	Obj\Num; Range 0...9
Data Log Enable/Rate Enables logging the current value periodically. There are a limited number of logging channels available, refer to Log Channels Free (FL)	LR	Obj\Enum; Adjustable Values: 0=Disable, 1=1 min, 2=5 mins, 3=15 mins, 4=1 hr, 5=4 hrs, 6=12 hrs, 7=24 hrs
Data Log Access historical log of the value, if enabled	LOG	Obj\Log

Alarm Fields

Alarms can be sent by an object to indicate an out-of-range value alarm state.

The Essential Data module places the following information into the North-format fields:

System – from the Essential Data Label object (DL)

Point – from page Label (L), then ' - ', and then the object Label (L)

Condition – either 'Alarm' or 'Ok'

Priority – set using Value Alarm Enable/Priority object (P)

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Essential Values	Air conditioning - Room temp	Alarm	3	24/03/15	10:16:02
Essential Values	Air conditioning - Room temp	Ok	3	24/03/15	10:52:16

Essential Data Task Control

Object Type: [CDM v20\UserData v31\TaskInfo]

Object Type: [CDM v20\UserData v30\TaskInfo]

The Essential Data Task Control object is used to control and monitor the operation of *Commander's database of values*.

Description	Reference	Type
Enable Option to enable or disable the operation of Essential Data, or to only allow read remote actions. 'Enable reading' will stop all writing to the remote objects and only permit remote actions set to read.	E	Obj\Enum: Range 0...2 ; Adjustable Values: 0=Disable, 1=Enable all, 2=Enable reading
Value being read Page and object index that Essential Data is currently processing with a remote action of read	RT	Obj\Text
Value being written Page and object index that Essential Data is currently processing with a remote action of write	WT	Obj\Text

Time Control Configuration

Object Type: [CDM v20\CalTimer v20]

A Time Control Configuration object contains a label and access security objects for *Commander's calendar, timers and profilers*.

Description	Reference	Type
Time Control Label	DL	Obj\Text; Max chars 20; Adjustable
Security: Read Access Area and minimum privilege level required to read the calendar and timers. See Security Server	AS	Obj\Num; Range 0, 10...87; Adjustable
Security: Edit Timer Area and minimum privilege level required to adjust a timer or profiler	AS.ET	Obj\Num; Range 0, 10...87; Adjustable
Security: Edit Calendar Area and minimum privilege level required to adjust the calendar	AS.EC	Obj\Num; Range 0, 10...87; Adjustable
Maximum Timers/Profilers	MT	Obj\Num; Range: 0, 20; Adjustable Default: 20

ObVerse Processor Configuration

Object Type: [CDM v20\OBVProcess v11]

Object Type: [CDM v20\OBVProcess v10]

An ObVerse Processor Configuration contains an object to engineer the strategy within the *ObVerse Processor*. Use the North ObvEditor application to create and edit a cause-and-effect strategy.

Description	Reference	Type
ObVerse Edits ObVerse strategy within the processor. Connect using ObvEditor software	P	Obj\EProcess; Adjustable
Idles per second Number of times the complete ObVerse strategy is processed per second. Not available in driver version 1.0.	IR	Obj\Num
Object Modules Monitor the operation of object module types within the processor. These include Object-Read and Object-Write modules. Not available in driver version 1.0.	T	Fixed container: [OSM v20\OBVProcess v11\ObjMods]

Alarm Fields

Alarms can be sent by any alarm module within the ObVerse strategy. Refer to *ObVerse Manual: Standard Processor* for more information on the alarm module.

The ObVerse Processor places the following information into the North-format fields:

System – from label of the process

Point – from alarm module's point object

Condition – from alarm module's condition field

Priority – from alarm module's priority field

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Main Plant	Temperature	Too High	3	23/03/16	13:33:59
Main Plant	Temperature	OK	3	23/03/16	15:21:16

ObVerse Object Modules

Object Type: [CDM v20\OBVProcess v11\ObjMods]

ObVerse Object Modules contain objects to enable and monitor the operation of object modules types within the processor. These modules perform a remote object operation and include the Object-Read, Object-Write, and Alarm modules.

Description	Reference	Type
Operation Temporarily disable the remote object operation of all object module types in the processor	D	Obj\Enum; Adjustable Values: 0=Enabled, 1=Disabled
Active Module Indicates which object module the processor is performing the remote object operation	M	Obj\Text Format: <i>item=module-type object-reference</i> Examples: V6=!Obv\ObjRead S1.M3.UI1.V V21=!Obv\ObjWrite UD.P2.O6 V36=!Obv\Alarm ALARM
Last Failed Module Indicates the last object module the processor failed to perform the remote object operation	FM	Obj\Text Format: <i>item=module-type object-reference</i>
Last Failed Time Indicates the date and time the processor failed to perform the remote object operation	FDT	Obj\DateTime

Security Server Configuration

Object Type: [CDM v20\TokenMax v20]

A Security Server Configuration contains objects to set a label, and the number of users stored by *Commander's Security Server*.

Description	Reference	Type
Security Server Label	DL	Obj\Text; Max chars 20; Adjustable
Maximum Users Sets the maximum number of users available within the Security Server. Set this to 100, 400, or 0 only.	MU	Obj\Num; Range: 0,100,400; Adjustable Default: 400

Data Transfer Configuration

Object Type: *[CDM v20\TransMax v14]*

A Data Transfer Configuration object enables the *transferring of values by Commander*, and contains objects to set the maximum transfers available and to monitor its operation.

Description	Reference	Type
Transfer Enable Option to enable or disable the operation of transfers, or to only allow reading. 'Enable reading' will stop all writing to destination objects and only read source objects.	E	Obj\Enum; Range 0...2; Adjustable Values: 0=Disable, 1=Enable All, 2=Enable Reading
Maximum Transfers Sets the maximum number of transfers available. Set this to 100, 500, or 0 only.	MT	Obj\Num; Range: 0,100,500; Adjustable Default: 500
Maximum Tasks Sets the number of simultaneous transfer tasks performed. Typically set this to '1'.	XT.M	Obj\Num; Range 1...4; Adjustable
Task x Allows monitoring of the module's four transfer tasks. The task number, x, is in the range 1..4	XTx	Fixed Container: <i>[CDM v20\TransMax v14\Task]</i>

Data Transfer Task

Object Type: *[CDM v20\TransMax v14\Task]*

A Data Transfer Task object contains information about a transfer task.

Description	Reference	Type
Process Current action the transfer task is performing	P	Obj\Enum; Range 0...2 Values: 0= Idle, 1=Reading, 2=Writing
Transfer Number Transfer the task is currently performing an action on	X	Obj\Num; Range 0...500

Alarm Delivery Configuration

Object Type: [CDM v20\AlmRoute v11]

An Alarm Delivery Configuration object contains a label for the *alarm delivery system*.

Description	Reference	Type
Alarm Delivery Label	DL	Obj\Text; Max chars 20; Adjustable

Alarm History Configuration

Object Type: [CDM v20\AlarmHistory v11]

An Alarm History Configuration object contains a system label and access security objects for *Commander's alarm history list*.

Description	Reference	Type
Alarm History Label	DL	Obj\Text; Max chars 20; Adjustable
Read Access Security Area and minimum privilege level required to read the alarms. See Security Server	AS	Obj\Num; Range 0, 10...87; Adjustable
Delete Access Security Area and minimum privilege level required to delete the alarms	AS.D	Obj\Num; Range 0, 10...87; Adjustable

Alarm Email Configuration

Object Type: [CDM v20\AlarmEmail v22]

An Alarm Email Configuration contains objects that set up how *Commander's alarm emailer* connects to an SMTP relay server, and set up the six destinations to provide email addresses for recipients.

Description	Reference	Type
Alarm Email label	DL	Obj\Text; Max chars 20; Adjustable
Email server IP/FQDN IP address or host name of SMTP relay server, e.g. '102.13.14.15' or 'mail.domain.com'. If a host name is used, ensure a DNS server address is also configured in the LAN port settings	IA	Obj\Text; Max chars 127; Adjustable
Email server port TCP/IP port number of SMTP service, default 25. If a firewall is in use, ensure it permits outbound traffic on this port number. SMTP servers supporting encryption are not supported, so check compatibility of servers using ports 465 or 587.	PN	Obj\Num; Adjustable
Email server reachable Indicates that the email server IP and port have been configured correctly	DS	Obj\NoYes
Server timeout (s) Maximum time to wait for a response from the SMTP server	TO	Obj\Num; Range 5...120; Adjustable
Authentication name User name to use when sign-in is required. A sign in may be required on some public SMTP relay servers, such as from BT Internet. The authentication supported by the Alarm Email module is AUTH LOGIN.	A.ID	Obj\Text; Max chars 40; Adjustable
Authentication password Password to use when sign in is required	A.PW	Obj\Text; Max chars 40; Adjustable If a password is set, it will read as '****'
From name Label describing the email author, Commander. If not specified, Alarm Email Label (DL) will be used	FT	Obj\Text; Max chars 40; Adjustable
From email address Email address to use for the email author. Usually required by the SMTP server	DFA	Obj\Text; Max chars 40; Adjustable
Client Domain Name Optional hostname used to identify Commander when connecting to the SMTP server. E.g. 'cmdr.domain.com' If not specified, then Commander's IP address will be used	FQDN	Obj\Text; Max chars 127; Adjustable
Web page address Optional url to include in the email message. Configure the link with the url of Commander's website, e.g. 'cmdr.domain.com'	WV	Obj\Text; Max chars 120; Adjustable
Sent email count Total number of emails send since Commander last started	SC	Obj\Num

Description	Reference	Type
Failed email count Count of times email messages have continuously failed to send	FC	Obj\Num
Last Fail Message Message from server indicating reason last message failed to send	FM	Obj\Text
Sent test to destination Triggers a test email message to the destination number specified	TST	Obj\Num; Range 0...6; Adjustable
Debug enable Enables the recording of communication with the SMTP server. Use this when instructed by North support to assist with fault finding sending emails to an SMTP server. See Debug recording	DE	Obj\NoYes; Adjustable
Destination x Configure a destination with filtering options and email address. The destination, x, is in the range 1...6	Dx	Fixed Container: [CDM v20\AlmEmail v22\Dest]

Alarm Email Destination Configuration

Object Type: *[CDM v20\AlmEmail v22\Dest]*

An Alarm Email Destination Configuration contains up to five addresses of where an alarm message is sent by *Commander's alarm emailer*. An optional comparison method can be specified to filter alarms received from the system's ALARM object.

Description	Reference	Type
Label Description of destination group	L	Obj\Text; Max chars 20; Adjustable
Send as text only Send emails as text-only format rather than HTML	EF	Obj\NoYes; Adjustable
Comparison Method Optional filter, so that only alarms containing certain text are emailed	C	Obj\Enum; Range ; Adjustable Values: 0=Begins with, 1=Contains, 2=Does not begin, 3=Does not contain, 4=Always send
Comparison String Optional text used with the comparison method to filter incoming alarms. String comparisons are case insensitive	S	Obj\Text; Max chars 20; Adjustable
Address x Configure an email recipient. The address, x, is in the range 1..5	TOx	Fixed Container: <i>[CDM v20\AlmEmail v22\Addr]</i>

Email Address Setup

Object Type: [CDM v20\AlmEmail v22\Addr]

An Email Address Setup object contains the following objects.

When the Fails (F) count reaches 3 for the address, then Enable (E) is set to 'No' and a destination failed alarm is sent.

Description	Reference	Type
Email address Single email address to email alarms, e.g. 'name@domain.com'	A	Obj\Text; Max chars 63; Adjustable
Enable Enables emailing alarms to the address	E	Obj\NoYes; Adjustable
Fails Count of times email messages have continuously failed to send to this address	F	Obj\Num; Range 0...9; Adjustable

Alarm Fields

Alarms are sent by an address to indicate a fail state.

The Alarm Email module places the following information into the North-format fields:

System – from the Alarm Email Label object (DL)

Point – from the email destination's Label object (L), or 'Destination x' if no label is set, then ' - ', then the Email address (A)

Condition – set to 'Destination Failed'

Priority – set to '3'

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Alarm Emitter	Destination 1 - name@domain.com	Destination Failed	3	23/03/15	13:33:59

North IP Devices Configuration

Object Type: [CDM v20\IPBus v22]

A North IP Devices Configuration object manages inbound access to this Commander, and outbound access to other Commanders, ObSys PCs, etc. that are available on the local and remote networks. Refer to *Communicating with other North IP Devices* for an introduction on this module.

By default, Commander is set with a random authentication key and AES-128 encryption. During initial configuration, with DEFAULTIP switch set ON, set Inbound Authentication Key (K).

Remember to document any keys used. Each Commander can have a unique authentication key, or for ease, you may decide to use the same authentication key for all devices on a site. You should not use the same key for more than one site or project.

By default, Commander is set to allow read-and-write access from the local network and no access from any remote networks (such as via a gateway). If you wish to engineer the Commander remotely, such as using a VPN, you will need to turn on Access from Remote Networks (RNA).

North IP devices on the local network are discovered automatically when the North IP Devices system object is scanned from engineering software, or using Scan device list (AF) object. Devices that are on a remote network must be added to the device list manually.

Before a device can be accessed using objects, set the Device's Outbound Encryption Method (KT) and Outbound Authentication Key (K).

When DEFAULTIP switch is set ON, the authentication key and encryption method are temporarily disabled. This enables an engineer to access the Commander regardless of this security setting (as long as they have physical access to the Commander).

Description	Reference	Type
Access from Local Network Control North IP access from devices on the local network – an IP address on the same subnetwork as Commander	LNA	Obj\Enum; Adjustable Values: 0=None, 1=Read-only, 2=Read-Write
Access from Remote Networks Control North IP access from devices on remote networks – an IP address with a different subnetwork address than Commander	RNA	Obj\Enum; Adjustable Values: 0=None, 1=Read-only, 2=Read-Write
Inbound Encryption Method Set with encryption method required to access this device	KT	Obj\Num; Adjustable Values: 0=None, 1=AES-128
Inbound Authentication Key Set with authentication key required to access this device	K	Obj\Text; Adjustable only
Restart required for changes Changes have been made to Inbound security. Restart device is required.	KC	Obj\NoYes
Scan device list Discover North IP devices on the LAN. Select 'scan now' to perform an immediate scan for new devices. Use 'wipe then scan', to erase the list and then scan for devices. After performing an action, refresh the object view.	AF	Obj\Enum; Range 0...2; Adjustable Values: 0=Auto, 1=Scan now, 2=Wipe then scan
Device x North IP device x configuration, where x is in the range 1...200	Ax	Fixed Container: [CDM v20\IPBus v22\Alias]

North IP Device Configuration

Object Type: [CDM v20\IPBus v22\Alias]

A North IP Device Configuration object contains an object reference, an IP address, and outbound encryption method and key for a Commander, ObSys PC, etc.

The module can also periodically check communications with the other device and generate an alarm message when communications fail.

Description	Reference	Type
Reference A short object reference for the device	N	Obj\Text; Max chars 5; Adjustable
IP address The IP address of the device	A	Obj\IP; Adjustable
Outbound Encryption Method Set with encryption method required to access the remote device	KT	Obj\Enum; Adjustable Values: 0=None, 1=AES-128
Outbound Encryption key Set with authentication key required to access the remote device	K	Obj\Text; Adjustable only
Comms Check Rate If required, Commander will periodically check it can request objects from the device, and send an alarm message if communication cannot be established	R	Obj\Enum; Range ; Adjustable Values: 0=Off, 1=1m, 2=5m, 3=15m, 4=1h, 5=4h
Comms Fails Count of consecutive failed attempts, or 0 when communication is successful	F	Obj\Num; Range 0...9

Alarm Fields

Alarms can be sent by the module to indicate a communications failure when value of Comms Fail reaches 3.

The North IP Devices module places the following information into the North-format fields:

System – ‘North IP Devices’

Point – from Reference (N), then ‘ at ’, then the IP Address (A)

Condition – either ‘Comms Fail’ or ‘Comms Ok’

Priority – ‘2’

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
North IP Devices	A1 at 192.168.192.167	Comms Fail	2	24/03/15	10:16:02
North IP Devices	A1 at 192.168.192.167	Comms Ok	2	24/03/15	10:52:16

Essential Values

Object Type: *[UserData\PageList]*

The Essential Values object contains pages of values from *Commander's database of values*.

Configure the database using the *Essential Data Configuration* object.

Description	Reference	Type
Page Label Page of values with label <i>Page Label</i> . The page number, <i>x</i> , is in the range 1...64	Px	Variable Container: <i>[UserData\Page]</i>
Alarm State Overall alarm state of all pages within the database – out-of-range alarm, communications fault	S	Obj\Enum; Range 0...3 Values: 0=Ok, 1=Alarm, 2=Comms, 3=Alarm & Comms

Essential Values Page

Object Type: *[UserData\Page]*

An Essential Values Page object contains a value for each of the objects configured in the database.

Description	Reference	Type
Label Object's value with label <i>Label</i> . The object number, <i>x</i> , is in the range 1...64	Ox	Type as configured for the object in the database, could be: Obj\Text Obj\NoYes Obj\OffOn Obj\Num Obj\Float Obj\Times Obj\DateTime Obj\Date Obj\Enum Obj\Profile If the object has been set to Adjustable, then the value will be adjustable here.
Alarm State Alarm state for all objects within the page – out-of-range alarm, communications fault	S	Obj\Enum; Range 0...3 Values: 0=Ok, 1=Alarm, 2=Comms, 3=Alarm & Comms

Time Control

Object Type: *[CalTimer v20]*

A Time Control object is used to provide time-based control. The control can be simple timer on-off control, for things such as lighting. The control can also be profile-based control, for things such as temperature set points.

For an overview, see the section on *Controlling using Time and Date*.

Description	Reference	Type
Calendar Set day-types for standard days of the week and exception days	C	Fixed Container: <i>[CalTimer v20\Calendar]</i>
Timer x Set a time-list for each day-type. Timer number, x, is in the range 1...20	Tx	Fixed Container: <i>[CalTimer v20\Timer]</i>
Profiler x Set a profile for each day-type. Profiler number, x, is in the range 1...20	Px	Fixed Container: <i>[CalTimer v20\Profiler]</i>

Calendar

Object Type: *[CalTimer v20\Calendar]*

A Calendar object is used to determine today's day-type. This is calculated from a set of day-types based on the day-of-week, which can be overridden by a list of exception dates. Each day-type can be assigned a label. If necessary, rather than calculate today's day-type, a Calendar can read a day-type calculated by a Calendar in a different device.

Description	Reference	Type
Source Object Optional current day-type object of the calendar in a different device, e.g. 'IP.A1.CT.C.T'	SO	Obj\Obj; Adjustable
Source Read Rate The rate to read the calendar source object in a different device	SR	Obj\Enum; Range 0...9; Adjustable Values: 0=ASAP, 1=1s, 2=5s, 3=15s, 4=1m, 5=5m, 6=15m, 7=1h, 8=4h, 9=12h
Source Fail Count Count of consecutive times the source object has failed to read successfully	SF	Obj\Num; Range 0...9
Day-type x Label Label for day-type x, where x is in the range 0...9. The label for day-type 0 is fixed to 'Off'.	Tx.L	Obj\Text; Max chars 20; Adjustable
Current Day-type Calculated day-type for today	T	Obj\Num; Range 0...9
Current Day-type label Calculated day-type for today	T.L	Obj\Text; Max chars 20
Monday Day-type Set to the day-type required for each standard Monday	D1.T	Obj\Num; Range 0...9; Adjustable
Tuesday Day-type Set to the day-type required for each standard Tuesday	D2.T	Obj\Num; Range 0...9; Adjustable
Wednesday Day-type Set to the day-type required for each standard Wednesday	D3.T	Obj\Num; Range 0...9; Adjustable
Thursday Day-type Set to the day-type required for each standard Thursday	D4.T	Obj\Num; Range 0...9; Adjustable
Friday Day-type Set to the day-type required for each standard Friday	D5.T	Obj\Num; Range 0...9; Adjustable
Saturday Day-type Set to the day-type required for each standard Saturday	D6.T	Obj\Num; Range 0...9; Adjustable
Sunday Day-type Set to the day-type required for each standard Sunday	D7.T	Obj\Num; Range 0...9; Adjustable
Exceptions Used Count of exceptions currently in use	EC	Obj\Num; Range 0...40
Exception Date x List of non-standard exception days. Where x is in the range 1...40	Ex	Fixed Container: <i>[CalTimer v20\Calendar\Except]</i>
dd/mm/yy day-type Alternative object to set the exception day-type for a specific date, dd/mm/yy	EDdd.mm.yy	Obj\Num; Range 0...9; Adjustable

Calendar Exception Date

Object Type: *[CalTimer v20\Calendar\Except]*

A Calendar Exception Date contains the date and day-type to use on a specific exception day.

Description	Reference	Type
Date The date to apply the exception	D	Obj\Date; Adjustable
Day-type Set to the day-type to use on the exception date	T	Obj\Num; Range 0...9

Timer

Object Type: *[CalTimer v20\Timer]*

A Timer object uses today's day-type, from the Calendar, to select one of several on-off times to be used today. It uses the current time to determine from those on-off times to determine whether it should be on or off at this time. It can calculate a profile, based on simple on and off values.

A Timer object contains the following objects:

Description	Reference	Type
Label	L	Obj\Text; Max chars 20; Adjustable
Day-type x Times Times for day-type x, where x is in the range 1...9	Tx	Obj\Times; Max periods 5; Adjustable
State Current state of timer, based on today's times, and the current time	S	Obj\OffOn
Destination Object Optional object to write State to when it changes	DO	Obj\Obj; Adjustable
Destination Fails Count of consecutive fails when writing to destination object, or 0 if successfully written	DF	Obj\Num; Range 0...9
Today's Times A copy of the times for today's day-type. Adjusting this object will adjust the times for today's day-type	TT	Obj\Times; Adjustable; Max periods 5
Profile Off Value Used for converting Today's Times to Today's Profile, the value in the profile when the time is off	V0	Obj\Float; Adjustable; Range 0.0...100.0
Profile On Value Used for converting Today's Times to Today's Profile, the value in the profile when the time is on	V1	Obj\Float; Adjustable; Range 0.0...100.0
Today's Profile A calculated profile based on Today's Times	TP	Obj\Profile; Max points 8

Profiler

Object Type: [CalTimer v20\Profiler]

A Profiler uses today's day-type, from a Calendar, to select one of several profiles to be used today. It then uses the current time, along with the change-points specified in today's profile, to determine whether to change the profiler's value. It can also calculate a set of on-off times, based on a switch level.

A Profiler object contains the following objects:

Description	Reference	Type
Label	L	Obj\Text; Max chars 20; Adjustable
Day-type x Profile Profile for day-type x, where x is in the range 1...9	Px	Obj\Profile; Max points 8; Adjustable
Value Current value of the profiler, based on today's profile and current time	V	Obj\Float; Range 0.00...100.0; Adjustable
Destination Object Optional object to write State to when it changes	DO	Obj\Obj; Adjustable
Destination Fails Count of consecutive fails when writing to destination object, or 0 if successfully written	DF	Obj\Num; Range 0...9
Today's Profile A copy of the profile for today's day-type. Adjusting this object will adjust the profile for today's day-type	TP	Obj\Profile; Adjustable; Max points 8
Time Switch Value Used for converting Today's Profile to Today's Times. The threshold value in today's profile below which the time is off, and above which the time is on	TV	Obj\Float; Adjustable; Range 0.00...100.0
Today's Times Calculated on-off times based on Today's Profile	TT	Obj\Times; Max period 5

ObVerse

Object Type: [ObVerse\Process]

The ObVerse object contains a list of the public properties available within the ObVerse processor.

The public properties are defined by the engineer of the ObVerse, so cannot be listed here. Instead, we list an object for each property type available.

Objects may be adjustable depending on the ObVerse. If the property is linked to the output of a module, then the module controls the value of the property, and so the property is not adjustable here. If the property has no module output linked to it, then the property is adjustable here.

For more information, refer to the *ObVerse Manual – Standard Processor* document.

Description	Reference	Type
Enum Label Enum property, holding an enumerated value, with reference <i>r</i>	<i>r</i>	Obj\Enum Text alternatives for each number are defined in the property
Float Label Float property, holding a floating-point value, with reference <i>r</i>	<i>r</i>	Obj\Float Value high and low limits, and decimal places are defined in the property
NoYes Label NoYes property, holding a binary state, with reference <i>r</i>	<i>r</i>	Obj\NoYes
Num Label Num property, holding an integer value, with reference <i>r</i>	<i>r</i>	Obj\Num: -2147483648... 2147483647 Value high, and low limits are defined in the property
Obj Label Obj property, holding an object reference, with reference <i>r</i>	<i>r</i>	Obj\Obj
OffOn Label OffOn property, holding a binary state, with reference <i>r</i>	<i>r</i>	Obj\OffOn
Text Label Text property, holding a text string value, with reference <i>r</i>	<i>r</i>	Obj\Text: max 31 chars. Maximum length is defined in the property

Security Server

Object Type: *[TokenMax v20\100]*

Object Type: *[TokenMax v20\400]*

The Security Server object provides user authentication to Commander and connected devices. For an overview, refer to the [Security Server](#) section.

Use the Editor Sign-in object to sign-in before configuring users and groups in the server.

Set the maximum users available in the server using the [Security Server Configuration](#) object.

Description	Reference	Type
Editor Access Allowed Indicates if the editor has signed-in	MP.S	Obj\NoYes
Editor Sign-in Write the password to sign-in, or any other value to sign-out. A password recovery key is returned when reading this object	MP.L	Obj\Text; Adjustable
Change Editor password Once signed-in, set a new editor password	ML.P	Obj\Text; Max 20 chars; Adjustable
Next available user Indicates the next unused user record available	FT	Obj\Num; Range 0...400
Area x Label Label of Security Area x, where x is in the range 1...8	Ax	Obj\Text; Max chars 20; Adjustable
Privilege Level x Label Label of Security Privilege Level x, where x is in the range 0...7	Lx	Obj\Text; Max Chars 20; Adjustable
Group x Set privilege levels for a group of users. The group number, x, is in the range 1...31	Gx	Fixed Container: <i>[TokenMax v20\Group]</i>
User x Configure a user's authentication credentials. The user number, y, is in the range 1...400, depending on the maximum users available set in the configuration object	Uy	Fixed Container: <i>[TokenMax v20\User]</i>

Security Server Group

Object Type: *[TokenMax v20\Group]*

A Security Server Group object contains privilege levels for a *group of users*.

Description	Reference	Type
Name Group name or description	N	Obj\Text; Max chars 20; Adjustable
Enabled Enable or disable all users that are a member of this group	E	Obj\NoYes; Adjustable
Privilege Level in Area x Area x privilege level, where x is in the range 1...8	Px	Obj\Num; Range 0...7; Adjustable

Security Server User

Object Type: *[TokenMax v20\User]*

A Security Server User object contains *user information* and credentials to provide authentication.

Description	Reference	Type
Name User name or description	N	Obj\Text; Max chars 20; Adjustable
Enabled If set to yes, the user is enabled if all groups that they belong to are also enabled	E	Obj\NoYes; Adjustable
User ID/Card Sign-in user name or access card number	ID	Obj\Text; Max Chars 20; Adjustable
Password This object always has a value of '****' when read	PW	Obj\Text; Max chars 20; Adjustable
Token This is a combination of the User ID and coded password	T	Obj\Text; Max chars 30
Group x Group x membership information, where x is in the range 1...3 When a user is a member of a group, then the group's privilege levels are combined with the user's own.	Gx	Obj\Num; Range 0...31; Adjustable
Privilege Level in Area x User's privilege level in Area x, where x is in the range 1..8	Px	Obj\Num; Range 0...7; Adjustable
Valid Start Date Optionally enables a temporary user between the start and end dates specified. For permanent users, set the start and end dates to the same value	SD	Obj\Date; Adjustable
Valid End Date Optionally enables a temporary user between the start and end dates specified. For permanent users, set the start and end dates to the same value	ED	Obj\Date; Adjustable
Last Validation Date Date the user was last validated successfully	LD	Obj\Date

Data Transfer

Object Type: *[TransMax v14\100]*

Object Type: *[TransMax v14\500]*

A Data Transfer object contains up to 500 transfers, where each transfer reads from one place and then writes to another. For an overview, see the section on *Transferring Values*.

Set the maximum transfers available using the *Data Transfer Configuration* object.

Description	Reference	Type
Transfer x Configure a transfer's information. The transfer number, x, is in the range 1...500, depending on the maximum transfers available set in the configuration object	Tx	Fixed Container: <i>[TransMax v14\Transfer]</i>

Transfer

Object Type: *[TransMax v14\Transfer]*

A Transfer object contains the following objects:

Description	Reference	Type
Source Object Object reference to read	SO	Obj\Obj; Adjustable
Source Read Rate Frequency to read the value. See <i>Reading the Value</i>	SR	Obj\Enum; Range 0...9; Adjustable Values: 0=ASAP, 1=Never, (2 and 3 not allowed,) 4=1m, 5=5m, 6=15m, 7=1h, 8=4h, 9=12h
Source Read Fails Count of times the remote object has continuously failed to read	SF	Obj\Num; Range 0...9
Value Transfer's current value	V	Obj\Text; Max chars 32; Adjustable
Dest Write Object Object reference to write	DO	Obj\Obj; Adjustable
Dest Write Rate Frequency to write the value. The value is always written on a change-of-value. Set a rate to perform an additional background write periodically. See <i>Writing the Value</i>	DR	Obj\Enum; Range 0...10; Adjustable Values: 0=COV, 1=Never, (2 and 3 not allowed,) 4=1m, 5=5m, 6=15m, 7=1h, 8=4h, 9=12h, 10=Every 00:00
Dest Write Fails Count of times the remote object has continuously failed to write	DF	Obj\Num; Range 0...9

Alarm Delivery

Object Type: *[AlmRoute v11]*

The Alarm Delivery object contains 16 destinations to route North-format alarms received.

All alarms arriving at or being produced by Commander are passed to the ALARM object for distribution. For an overview, see the section on *Alarm Basics*.

Description	Reference	Type
Route New Alarm	ALARM	Obj\Alarm; Adjustable
Destination x Destination x information, where x is in the range 1...16	Dx	Fixed Container: <i>[AlmRoute v11\Dest]</i>

Alarm Delivery Destination

Object Type: *[AlmRoute v11\Dest]*

An Alarm Delivery Destination object contains the following objects:

Description	Reference	Type
Label Description of this destination	L	Obj\Text; Max 20 chars; Adjustable
Enable If set to yes, alarms can be delivered to this destination	E	Obj\NoYes; Adjustable
Destination Object Object reference to route alarms. Typically this object reference ends '.ALARM'	R	Obj\Obj; Adjustable
Add Device Label If set to yes, prefixes the alarm system field with Commander's label	CL	Obj\NoYes; Adjustable
Fail State Indicates the Destination Object is failing to accept alarms	F	Obj\NoYes
High Priority Only alarms with a priority number equal or greater than this value are delivered. To disable priority filtering, set the high and low priority to the same value. See <i>Filtering Delivery</i>	HP	Obj\Num; Range 0...9; Adjustable
Low Priority Only alarms with a priority number equal or less than this value are delivered. To disable priority filtering, set the high and low priority to the same value.	LP	Obj\Num; Range 0...9; Adjustable
Comparison Method Optional text filter. Specify the method to use along with up to three comparison strings. See <i>Filtering Delivery</i>	C	Obj\Enum; Range 0...3; Adjustable Values: 0=Begins with, 1=Contains, 2=Not begin with, 3=Not contain
Comparison String x Text string to use with the comparison method. The string number, x, is in the range 1...3	Sx	Obj\Text; Max 20 chars; Adjustable
Any Group Join this destination to the any group. When one destination accepts the alarm, it will not be sent to any other destinations in the group. See <i>Delivery to a Group</i>	A	Obj\NoYes; Adjustable

Alarm Fields

Alarms are sent by the delivery destination to indicate a fail state.

The Alarm Delivery module places the following information into the North-format fields:

System – from the Alarm Delivery Label object (O.AR.DL)

Point – from the delivery destination's Label object (L), or 'Destination x' if no label is set

Condition – either 'Comms Fail' or 'Comms Ok'

Priority – set to '1'

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Alarm Delivery	Destination 1	Comms Fail	1	23/03/15	13:33:59
Alarm Delivery	Destination 1	Comms Ok	1	24/03/15	07:30:16

Alarm History

Object Type: *[AlarmHistory v11\100]*

An Alarm History object contains a *list of the last 100 alarms* received.

Deliver new alarms, using *Alarm Delivery*, to the ALARM object.

Description	Reference	Type
Alarm count To clear all alarms, set value to '0'	C	Obj\Num; Range 0..100; Adjustable
Store new alarm	ALARM	Obj\Alarm; Adjustable
Alarm x List of alarms, where Alarm 1 is the last alarm received. The alarm number, x, is in the range 1...100	Hx	Obj\Alarm

Alarm Emailer

Object Type: *[AlmEmail v22]*

An Alarm Emailer contains six destinations to send alarms, plus a system ALARM object that sends to multiple destinations based on their comparison settings. The email destinations are set in the *Alarm Email Configuration* object.

Description	Reference	Type
Destination Label Destination email group to deliver an alarm, where x is in the range 1...6, depending on whether each has been set up	Dx	Fixed Container: <i>[AlmEmail v22\Dest]</i>
Deliver New Alarm Delivers an alarm to multiple destinations based on the comparison settings configured in each	ALARM	Obj\Alarm; Adjustable

Alarm Emailer Destination

Object Type: *[AlmEmail v22\Dest]*

An Alarm Emailer Destination object contains a queue of alarms to send via email to a destination.

Deliver new alarms, using *Alarm Delivery*, to the ALARM object.

Description	Reference	Type
Deliver New Alarm	ALARM	Obj\Alarm; Adjustable
Alarms in Queue	C	Obj\Num; Range 0...31

North IP Devices

Object Type: *[IPBus Net]*

The North IP Devices object provides access to other *North devices on the IP network*.

Scan the object to automatically discover North IP devices on the local network, or add a device via the *North IP Devices Configuration* object.

Description	Reference	Type
North Device's Label Access device with label <i>North Device's Label</i>	<i>ref</i>	Variable container. Type varies depending on the North Device. Typically this is <i>[Commander v20\Device]</i> for other Commanders, or <i>[ObSys]</i> for ObServer based devices
North Device's Label [Secure] A secure device with label <i>North Device's Label</i> requires authentication details	<i>ref</i>	Fixed container <i>[Commander v20\SecureDevice]</i>

North IP Secure Device

Object Type: *[Commander v20\SecureDevice]*

The North IP Secure Device object manages outbound access to another Commander, ObSys PC, etc. that is available on the local and a remote networks.

Before the secure device can be accessed using objects, set the Device's Encryption Method (IPKT) and Authentication Key (IPKEY).

Once the encryption method and authentication key for the device have been entered, rescan the North IP Devices object. If incorrect details are entered, reconfigure via the *North IP Devices Configuration* object.

Description	Reference	Type
Encryption Method Set with encryption method required to access the secure device	IPKT	Obj\Enum; Adjustable Values: 0=None, 1=AES-128
Authentication Key Set with authentication key required to access the secure device	IPKEY	Obj\Text; Adjustable only

Object Specifications from Previous Versions of Firmware

Platform Information

Object Type: *[Commander v20\Platform v13]*

Object Type: *[Commander v20\Platform v12]*

Object Type: *[Commander v20\Platform v11]*

The Platform Information object provides *general information about Commander*.

Description	Reference	Type
Commander Version The Commander's main firmware version and release date	PV	Obj\Text
Hardware Version Version number of Commander's physical hardware	HV	Obj\Float
Hardware Mode State of the internal switches – DEFAULTIP and PROGRAM	M	Obj\Enum; Range 0...3 Values: 0=Run, 1=Program mode, 2=Default IP, 3=Program mode & Default IP
Battery State Health of the internal battery. Replace when low.	BS	Obj\Enum; Range 0...3 Values: 0=Ok, 1=Low, 2=Very Low, 3=Unknown
Reset Platform Set to perform a soft reset of Commander. The value indicates the seconds before restart	!rst	Obj\Num; Range 0...1000
Default Configuration Save current engineered settings as the default configuration	DC	Fixed Container: <i>[Commander v20\Platform v13\DefCon]</i>
Last Restart Information about the last restart	LR	Fixed Container: <i>[Commander v20\Platform v13\Restart]</i>
Software Versions Software versions for each of Commander's main modules and started interfaces	V	Fixed Container: <i>[Commander v20\Platform v13\Versions]</i>
Recording Enable debug recording, and select which information is recorded	R	Fixed Container: <i>[Commander v20\Platform v13\Record]</i>

Alarm Fields

Alarms are sent by Commander when the battery state reaches a low condition.

The Platform Information module places the following information into the North-format fields:

System – 'Commander'

Point – 'Battery'

Condition – either 'Very Low', 'Low', or 'OK'

Priority – '2' for Very Low, '3' for Low and OK conditions

Date & Time – from Commander

Alarm Examples

System	Point	Condition	Priority	Date	Time
Commander	Battery	Low	3	23/03/15	13:33:59
Commander	Battery	Very Low	2	15/04/15	07:30:16
Commander	Battery	OK	3	18/04/15	10:15:24

LAN Port

Object Type: [Commander v20\DynamicLAN v12]

Object Type: [Commander v20\DynamicLAN v11]

Object Type: [Commander v20\DynamicLAN v10]

A LAN Port Configuration object allows the *set-up of Commander's LAN port*, including selecting how the IP address is assigned.

After changing the LAN Port objects, reset Commander for the new values to take effect.

Description	Reference	Type
Label Fixed label 'LAN Port' – for compatibility with ObSys	L	Obj\Text; Max chars 20
Network Available Whether the network port has been initialised, link is up with remote end, and has IP address assigned	S	Obj\NoYes
Current IP Address IP address currently in use	CIA	Obj\IP
IP Address Assign a static IP address, or '0.0.0.0' to request a dynamic IP address from a DHCP server	IA	Obj\IP; Adjustable
Subnet Mask Subnet mask to use with a static IP address, e.g. '255.255.255.0' for class C networks	IM	Obj\IP; Adjustable
Gateway Address Gateway IP address to use in static IP mode	IG	Obj\IP; Adjustable
DNS Server Address Domain name server IP address to use in static IP mode, or if not supplied by a DHCP server. If no DNS server address is known, Commander will attempt to use 1.1.1.1	ID	Obj\IP; Adjustable
Time Server Address NTP server IP address to use in static IP mode, or if not supplied by a DHCP server. If no NTP server address is known, Commander will try to use DNS to resolve pool.ntp.org to find one	IT	Obj\IP; Adjustable
TFTP Enable Enable TFTP, for updating firmware. The Commander also must be in PROGRAM mode to allow TFTP download. Available from DynamicLAN v11	TFE	Obj\NoYes; Adjustable
MAC Address Physical address (MAC) of Commander's LAN port	MAC	Obj\Text; Format: <i>hh:hh:hh:hh:hh:hh</i> where <i>h</i> is a hexadecimal digit
DHCP Server Information about the DHCP Server operation. The DHCP Server only operates when the Commander is in DEFAULTIP mode. Available from DynamicLAN v12	DS	Fixed Container: [Commander v20\DHCP Svr v10]

Web Server Configuration

Object Type: [CDM v20\C2Web v30]

The Web Server Configuration object enables *Commander's web server* and selects what information is accessible from it.

Description	Reference	Type
Enable Web Server	E	Obj\NoYes; Adjustable
Show Alarm History Enables access to alarm history from the website	E.AH	Obj\NoYes; Adjustable
Content Configure options to customise the overview page	C	Fixed Container: [CDM v20\C2Web v30\Content]
Security Configure sign-in and security options	S	Fixed Container: [CDM v20\C2Web v30\Security]
Information Website usage information	I	Fixed Container: [CDM v20\C2Web v30\Info]

Web Server Configuration

Object Type: [CDM v20\C2Web v20]

Object Type: [CDM v20\C2Web v11]

The Web Server Configuration object enables *Commander's web server* and selects what information is accessible from it.

Description	Reference	Type
Enable Web Server	E	Obj\NoYes; Adjustable
Show Essential Values Enables access to values from Essential Data	UD.EV	Obj\NoYes; Adjustable
Show Extra Values Enables access to values from Extra Data. Available in C2Web v2.0 and later	UD.XV	Obj\NoYes; Adjustable
Show Values in Sub-menu Places pages from Essential Values and Extra Values in their own sub-menus on the website. Without this option enabled, pages are displayed in the main menu	UD.PL	Obj\NoYes; Adjustable
Show Calendar Enables access to the calendar, timers and profilers from the website	C.E	Obj\NoYes; Adjustable
Show Alarms Enables access to alarm history from the website	AM.E	Obj\NoYes; Adjustable
Total Pages Served A count of the total web pages requested	PC	Obj\Num;
Template Configure options on the web template	T	Fixed Container: [CDM v20\C2Web v20\Template]
Home Page Configure options to customise the home page	H	Fixed Container: [CDM v20\C2Web v20\HomePage]
Security Configure sign-in and security options	S	Fixed Container: [CDM v20\C2Web v20\Security]

Web Server Template

Object Type: [CDM v20\C2Web v20\Template]

Object Type: [CDM v20\C2Web v11\Template]

A Web Server Template object contains the following objects to *define the page template*.

Description	Reference	Type
Show Value Reliability Enables the display of status information for values, e.g. Ok, Alarm states	SS	Obj\NoYes; Adjustable
Link x Label Label for external link x. The link number, x, is in the range 1..3	Lx.L	Obj\Text; Max. 20 chars; Adjustable
Link x URL Web page address for external link x. E.g. 'www.northbt.com'. The link number, x, is in the range 1..3	Lx.U	Obj\Text; Max. 125 chars; Adjustable

Web Server Home Page

Object Type: [CDM v20\C2Web v20\HomePage]

Object Type: [CDM v20\C2Web v11\HomePage]

The Web Server Home Page object contains configuration options to *enhance the home page*, including a title, optional text paragraphs, informative widgets from Essential Data, and an alarm list summary.

Description	Reference	Type
Title Headline to display on home page. If not specified, then the date is shown	T	Obj\Text; Max chars 60; Adjustable
Info Para x Set with a line of text to display as an informational paragraph on the home page. The paragraph number, x, is in the range 1...4	Px	Obj\Text; Max chars 125; Adjustable
Widget Style Select what information from Essential Data is displayed in the widget area	WS	Obj\Enum; Range 0..2; Adjustable Values: 0=Off, 1=1 st object of each page, 2=Objects in page 1
Max Widgets Maximum number of widgets to display	WM	Obj\Num; Range 0..32; Adjustable
Max Alarms Maximum number of alarms to display	WA	Obj\Num; Range 0..127; Adjustable

Web Server Security

Object Type: [CDM v20\C2Web v20\Security]

Object Type: [CDM v20\C2Web v11\Security]

The Web Server Security object contains *security settings* to enable user sign-in and control access to the server.

Description	Reference	Type
Require User Sign-in Enable website authentication using the Security Server	M	Obj\NoYes; Adjustable
Allow Password Change Enables change password option when user is signed-in	UPC	Obj\NoYes; Adjustable
Security Server Object Object reference of a Security Server. Typically, this is set to 'TK' for local Commander, but could be set to the object of a central server	R	Obj\Obj; Adjustable
Default Access Security Set privilege levels for when user sign-in is not enabled. Available in C2Web v2.0 and later	D	Fixed Container: [CDM v20\C2Web v20\DefaultAccess]

North IP Devices Configuration

Object Type: [CDM v20\IPBus v21]

A North IP Devices Configuration object manages a list of other Commanders, ObSys PCs, etc. that are available on the LAN or WAN. Refer to *Communicating with other North IP Devices* for an introduction on this module.

Description	Reference	Type
Scan device list Discover North IP devices on the LAN. Select 'scan now' to perform an immediate scan for new devices. Use 'wipe then scan', to erase the list and then scan for devices. After performing an action, refresh the object view.	AF	Obj\Enum; Range 0...2; Adjustable Values: 0=Auto, 1=Scan now, 2=Wipe then scan
Local encryption key If specified, all other devices that communicate with this Commander must be set to use this encryption key. Once set, reads as '*****'	K	Obj\Text; Max chars 8; Adjustable
Device x North IP device x configuration, where x is in the range 1...200	Ax	Fixed Container: [CDM v20\IPBus v21\Alias]

North IP Device Configuration

Object Type: [CDM v20\IPBus v21\Alias]

A North IP Device Configuration object contains an object reference, IP address, and encryption key for a Commander, ObSys PC, etc.

The module can also periodically check communications with the other device and generate an alarm message when communications fail.

Description	Reference	Type
Reference A short object reference for the device	N	Obj\Text; Max chars 5; Adjustable
IP address The IP address of the device	A	Obj\IP; Adjustable
Encryption key If the device has IP encryption enabled (with the Local Encryption Key object), this key must match that in the device. Always reads as '*****'	K	Obj\Text; Max chars 8
Comms Check Rate If required, Commander will periodically check it can request objects from the device, and will send an alarm message if comms cannot be established	R	Obj\Enum; Range ; Adjustable Values: 0=Off, 1=1m, 2=5m, 3=15m, 4=1h, 5=4h
Comms Fails Count of consecutive fails, or 0 is comms were successful	F	Obj\Num; Range 0...9

Telnet Setup

Object Type: [CDM v20\Telnet v10]

Telnet was removed from firmware dated 01/06/25 onwards, but can be started as an Interface.

For information on establishing a Telnet session and the commands supported, refer to the *Telnet Driver Manual*.

Description	Reference	Type
Session Label Provided when a Telnet session is opened	DL	Obj\Text; Max chars 20; Adjustable
Telnet Enabled Enables the Telnet service	TE	Obj\NoYes; Adjustable
User/Password User name required to access the Telnet service	PSW	Obj\Text; Max chars 7; Adjustable
Connections Number of Telnet sessions currently established	CC	Obj\Num: 0...4

Appendix A - Ethernet/IP Protocols

The RJ-45 LAN port on Commander (hv 3.0) is fully-compliant with IEEE 802.3/802.3u standards. Supporting: 10Base-T/100Base-TX, full and half-duplex auto-negotiation, and auto MDI-X sensing crossover cable.

For information on a particular driver's IP port usage, refer to the relevant *Driver Manual*.

Address Resolution Protocol (ARP)

Commander supports ARP to determine IP-to-Ethernet mapping.

Table size: 128. Request timeout: 100ms. Entry cache life: 1200s

Internet Control Message Protocol (ICMP)

Commander supports ICMP and responds to the PING request.

Dynamic Host Control Protocol (DHCP)

The DHCP client, enabled by setting the IP address to '0.0.0.0', requests IP information from a DHCP server.

Ports used: UDP 67 (remote), UDP 68 (local).

Requests: IP address, network mask, gateway address, DNS server address, NTP server address.

The DHCP server, enabled by setting the DEFAULTIP switch to ON, provides IP address leases in the range 192.168.192.101 to 192.168.192.116, with the network mask 255.255.255.0 and gateway address 192.168.192.1.

Ports used: UDP 67 (local), UDP 68 (remote).

Domain Name System Protocol (DNS)

When needed, the DNS client resolves fully qualified domain names by requesting from a DNS server.

Ports used: UDP 53 (remote), UDP ephemeral (local)

Default server: 1.1.1.1

Network Time Protocol (NTP)

Commander will periodically try to synchronise its real-time clock with an NTP server.

Ports: UDP 123 (local and remote)

Default server: pool.ntp.org

Simple Mail Transfer Protocol (SMTP)

Once Alarm Emailer is configured with a server address, this SMTP client sends emails to the specified server. Disabled by default.

Ports used: TCP 25 (configurable, remote), TCP ephemeral (local)

Hypertext Transfer Protocol (HTTP)

The Web Server, if enabled, serves simple HTML pages when requested. Disabled by default.

Ports used: TCP 80 (local)

North Cloud Services

If the link to Commander Hub is enabled, or firmware updates requested, outgoing session to send and receive AES-128 encrypted data over HTTP to North's cloud-based services. Disabled by default.

Port used: TCP 80 (remote), TCP ephemeral (local)

North/IP

The North/IP Protocol allows North products that support IP networking to communicate. By default AES-128 encryption is enabled with a random authentication key.

Ports used: UDP 37926 (local and remote)

Trivial File Transfer Protocol (TFTP)

The TFTP protocol allows new CDMs and system firmware to be downloaded into Commander. It is enabled by either [LAN Port Configuration](#) or DEFAULTIP switch, and when the PROGRAM switch is ON.

Ports used: UDP 69 (local)

Appendix B – Factory Installed Drivers

Commander contains several pre-installed drivers, and you can *install others as necessary*.

North devices

North Zip (ZipMaster*)

North Compass*

Building Automation

BACnet/IP Standard (BACnetIP*)

KNX Standard (KNXIP)

LonWorks networks (LonSLTA)

MBus

Meaco Radio Telemetry (Meaco)

Modbus*

Trend Control Systems IQ series (TrendIQ)

Cylon

Johnson Controls Metasys N2

Air Conditioning

Carel

Carrier CCN DataPort (CCNDP2)

Daikin

Mitsubishi Electric (MitsubishiG50)

Mitsubishi Electric City Multi (MitsCity)

Panasonic VRF

Fire & Security

Advanced MxPro series (Advanced)

Colt International OPV (ColtOPV)

Kentec Electronics Syncro (Kentec)

Kentec Electronics Taktis (KentecTaktis)

Morley-IAS ZX series (Morley)

Notifier ID3000 series (Notifier)

Protec

Ziton ZP3 (ZitonZP3)

Lighting

DALI Standard

Helvar

iLight

Luxmate

Philips Hue (Hue)

Philips Lightmaster (PhilipsLM)

Power

APC

OCPP

Eltek

GeistPDU

Power One DC power (PowerOne)

Home Automation

DraytonWiser

EIB

EnOcean

Heatmiser Neo

Lutron QS

Lutron HomeWorks

Data import/export

Convert alarm events to objects (AlmSet*)

Import CSV data (CsvRead)

Monitor health of remote devices
(DeviceCheck*)

SMS portal (GSMSMS*)

Serial printer output (Printer)

Send SNMP Trap messages (SNMPTrap*)

Monitor digital states (StateCheck)

Send simple text commands (TextOut)

Import XML data (XMLRead)

API

DataSync

JSONData*

JSONNotify

MQTT

SG*

Telnet*

Weather

Davis Weather

* indicates driver does not require an interface licence to start.

For a full list of available drivers, visit northbt.link/drivers.

Appendix C – Internal Switch Features



Remove the lid to access Commander's switches. By default these are OFF. Turning switches ON will enable configuration options, potentially making Commander insecure.

PROGRAM switch

When the internal switch labelled **PROGRAM** is set ON, and Commander re-powered, the Commander enters Program mode, where the following flash memory functions are enabled:

- Commander can be updated with new firmware, either using Software Cloud Update or TFTP service
- Saving the Commander's current configuration as the Default Configuration becomes possible
- Upgrading Interface Licences is enabled, as licences are held in flash memory.

DEFAULTIP switch

When the internal switch labelled **DEFAULTIP** is set ON, Commander automatically restarts and enters Default IP mode, where the following happens:

- Commander operates with a static IP address of 192.168.192.167, and network mask of 255.255.255.0
- DHCP Server is enabled, and will assign an IP address to any connected PC
- TFTP server is enabled (also requires Program mode)
- Within North IP Devices service, the Encryption Method and Authentication Key is temporarily disabled. This allows an engineer to access the Commander without knowledge of this security setting (as long as they have physical access to the Commander)
- Web server is enabled, with view and adjust access, and Require Sign-in is temporarily disabled. This allows access to all web pages and adjustment of any adjustable values
- Changing network settings and Commander Hub link via the Web server is enabled.

Warranty, Safety, Environmental, and Regulatory Information

Commander is manufactured by North Building Technologies Limited in the UK.

The device is intended for use as a building automation controller. It provides monitoring and control of compatible systems using North drivers. It requires installing and configuring by a competent engineer, who has completed at a minimum the North Integration training course.

Product documentation, support, and contact details are available from www.northbt.com/cmdr.

Warranty

North warrants goods of its manufacture as being free of defective materials and faulty workmanship for three years from the date of purchase. If this product should become defective, please contact our support team. This warranty becomes invalid if the product has been tampered with, not used for its intended purpose, incorrectly installed, or used in an unsuitable environment.

If you require further help, please contact our support team on +44 (0) 1273 694422, or visit www.northbt.com/support

Support Period

North provides at least five years of security updates from the date of purchase.

Refer to the [Updating Commander's Firmware](#) section for details on how to install the latest update.

Security

Commander is *secure by default*, follow guidance in this manual to ensure secure use.

North strongly advise that you keep Commander up to date with the latest firmware. Details of firmware updates and vulnerabilities are available on the release notes page at northbt.link/update.

If you believe you have found a vulnerability please contact us via our disclosure program at northbt.link/security.

Declaration of Conformity

We, North Building Technologies Limited, PO Box 2673, Brighton BN1 3US, United Kingdom

declare that this Commander product conforms with the relevant EU harmonization legislation (Europe only) and UK legislation (Great Britain only).

A copy of the Declaration of Conformity is available from www.northbt.com/cmdr.

UK PSTI Statement of Compliance

We, North Building Technologies Limited, PO Box 2673, Brighton BN1 3US, United Kingdom

declare that this Commander product, manufactured solely by us, conforms with the applicable security requirements of Schedule 1 of the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

A copy of the PSTI Statement of Compliance is available from www.northbt.com/cmdr.

Recycling information

This product is marked with the crossed-out wheelie bin symbol which signifies that it should not be disposed of in general waste or landfill. At the end of its life, it should be deposited at an appropriate facility to enable recovery and recycling.



Refer to the [Removing all Data from Commander](#) section for details on how to remove all data from this device before disposal.

Battery Disposal

The removable lithium-ion battery contained within this product is marked with the crossed-out wheelie bin symbol. This signifies that it should not be disposed of as unsorted municipal waste at the end of its working life.

Refer to the [Internal Battery](#) section for information on the replacement and safe handling of the battery.

Commander Versions

Build Date	Details
21/01/2012	Released
10/05/2012	Low-level TCP idle timeout increased
09/09/2012	Recording to COM port now closed when attempting to use driver on same COM
08/04/2013	Reset Reason object now provides indication of reset caused by power and user Resolved issue with defrag eating messages Resolved issue with PING messages larger than 128 bytes Resolved issue when DNS server not reachable Resolved DHCP renewal issue Modified RS232 flow control pins
01/07/2013	Telnet driver rework
19/09/2013	Now uses fixed values provided for gateway and NTP if not provided by DHCP server
01/03/2014	Resolved issue when receiving intensive messages from IP network Added Last Time Sync information
01/04/2014	Added support for version 2.0 hardware Resolved issue when terminating TCP connection
20/08/2014	Resolved issue when Ethernet link established, but no IP address Add new hardware RTC support, including adjustments Updated NTP code NOTE: Commander will clear it's memory on installing this update
02/06/2015	Battery hysteresis added to stop repeat battery alarms
07/03/2016	Added support for new internal requests (FastComms). Increased number of pre-installed drivers. Essential Data upgraded to 640 objects. ObvProcess: new Raise-Lower and Usage modules. New objects to monitor state on remote-object actions. Minor changes some module categories to tie in with ObVerse Manual.
01/11/2016	Add support for 300 and 600 baud on serial ports. Resolved issue on receiving short TCP/UDP messages with additional padding Update to DHCP
24/02/2017	Improve operation when receiving a broadcast storm on the Ethernet network
17/03/2017	Added Default Configuration support. ObvProcess supports Essential Values as properties Changing DEFAULTIP switch causes restart
01/11/2017	Telnet supports up to 4 sessions. Optimisations to Essential Data, Alarm Email, ObVerse Processor, and Web Server
07/12/2017	Resolved issue when adjusting Essential Data Task Control object (introduced in build 01/11/17). Modifying this value may cause Essential Data's operation to be disabled
01/03/2018	Resolved additional issue with Essential Data. When an object is configured with a remote action of 'read' <u>and</u> the current value does not change for 24 days, then Essential Data will stop reading the object for the next 24 days, after which it will start reading again. If Commander is restarted during this time, then reading will resume and the timer restarted.
01/11/2018	ObvProcess: Added support for cancelling upload/download in latest ObvEditor. Resolved issues with OODelay (restart fix), Rescale (divide by zero error), Counter (reset fix). Data Transfer: added support for transferring values from times and profile object types. North IP Devices: Speed improvements Web Server: resolved issue with page navigation when viewed on a slow VPN connection.
01/06/2019	Essential Data (v3.1): Added Alarm Delay object (AD). Resolved issue when object value adjusted multiple times before remote device acknowledges first write. In this situation, last adjustment was not written to remote device. North IP Devices: New feature with DEFAULTIP switch on, local encryption key not checked. Resolved issue when requesting object from device reference not configured. This caused Commander to reset.
01/09/2019	Essential Data: when Remote Fails are 9, retry period reduced from 15min to 5min.
28/07/2020	Essential Data: resolved issue when linking to invalid page/object within ObvProcessor Data Transfer: resolved issue in calculating value change, resulting in write action when not needed

Build Date	Details
25/08/2021	Update to support new hardware components Telnet: Fixed issue with opening TCP socket when re-enabling.
01/10/2021	North's cloud-based services added: Commander Hub and Software Cloud Update Default DNS server (1.1.1.1) and Time server (pool.ntp.org) used when not specified. Some features enabled by PROGRAM switch now use DEFAULTIP switch – refer to Appendix C. Web service: Support page updated. Essential Data: resolved issue with communications alarm state clearing, when value had not changed. North IP Devices: resolved issue with comms check when reference contained an alias.
23/12/2021	General improvement to TCP/IP communications, including increased memory allocation. Fixed issue with ARP and Telnet that could impact TCP communications. Fixed issue with label corruption on Hub.
02/06/2022	Added TFTP Permitted object Web Server: re-designed ObVerse Processor: Added Times-State, Profile-Value, Date-Pulse, and Smooth module types; and Profile, Times, and DateTime property types. Essential Data: Float-type object, added 0.5 dp option
17/08/2022	Fixed issue with Hub: clearing events in Alarm History may stop sending to Hub. Fixed issue with TCP socket link closure. Web Server: data refresh, value page remembers expand/collapse all, updated content-security-policy, fix displaying month, fix battery state value on old hardware. Alarm Emailer: improved sending on poor connections. Added fail message object (FM) Changed factory installed drivers
01/01/2023	Improved power-loss detection and shut-down. Hub data encryption block size optimised to increase idle time. Improved Hub delivery after loss of Internet connection. Alarm Emailer: resolved issue causing email to resend. Web Server: fixed issue with formatting of profile and times objects on refresh.
01/11/2023	Improved power-loss detection on start-up. DHCP client: provides host name to server when requesting lease. Web Server: modified export data CSV format. LAN Port: Added DHCP server in DEFAULTIP mode. ObVerse Processor: added Last-Change module type. Text module types now available in standard processor, including: Text-Equal, Text-In-Text, Text-Join, and Text-Split.
01/06/2024	Fixed issue with watchdog reset on a small number of devices. North IP Devices: operates with network port translation (replies sent to UDP source port). Web Server: Added objects to control access from local networks and remote networks. ObVerse Processor and Alarm Emailer: general performance enhancements.
01/01/2025	NTP: additional checking of NTP response to help resolve issue of momentarily incorrect year affecting Hub reporting. Web Server: resolved issue where web server was not enabled in DEFAULTIP mode, when both local/remote access set to none. Added Website access item to device information page.
01/06/2025	Support for Commander hardware version 3.0, with 10/100 Mbps Ethernet port. Changes to make Commander secure by default: North IP Devices: AES-128 encryption enabled by default. Added objects to control access from local and remote networks. Web Server: Disabled by default. TFTP: Disabled by default Telnet: Removed from Commander base, now available as a driver
01/10/2025	Local Date & Time: Additional checking when reading time from hardware RTC. Added hardware support for upcoming flash memory component change. North IP Devices: Fixed issue where Access from Local/Remote Network setting could block a reply. Changing Inbound Encryption settings now requires a device restart. Essential Data: Reset fail counters when changing from DEFAULTIP mode. Data Transfer: Reset fail counters when changing from DEFAULTIP mode. Added object to indicate if transfers have been configured. Data Transfer, Security Server, Time Control: maximum items accept '0' to hide system object.

Build Date	Details
01/06/26	LAN Port: Updated Link Status (S) object to report network speed and duplex. Max Auto-negotiation Speed (SL) object added. North IP Devices: Fixed an issue where encrypted device discovery messages caused a message queue resource leak. This could cause services to stop, requiring a device restart to restore operation. Base: Added driver support for sending serial BREAK signals.

Next Steps...

If you require help, contact support on 01273 694422 or visit www.northbt.com/support



North Building Technologies Ltd
+44 (0) 1273 694422
support@northbt.com
www.northbt.com

This document is subject to change without notice and does not represent any commitment by North Building Technologies Ltd.

ObSys and Commander are trademarks of North Building Technologies Ltd. All other trademarks are property of their respective owners.

© Copyright 2026 North Building Technologies Limited.

Author: TM
Checked by: JF

Document issued 25/06/2026.