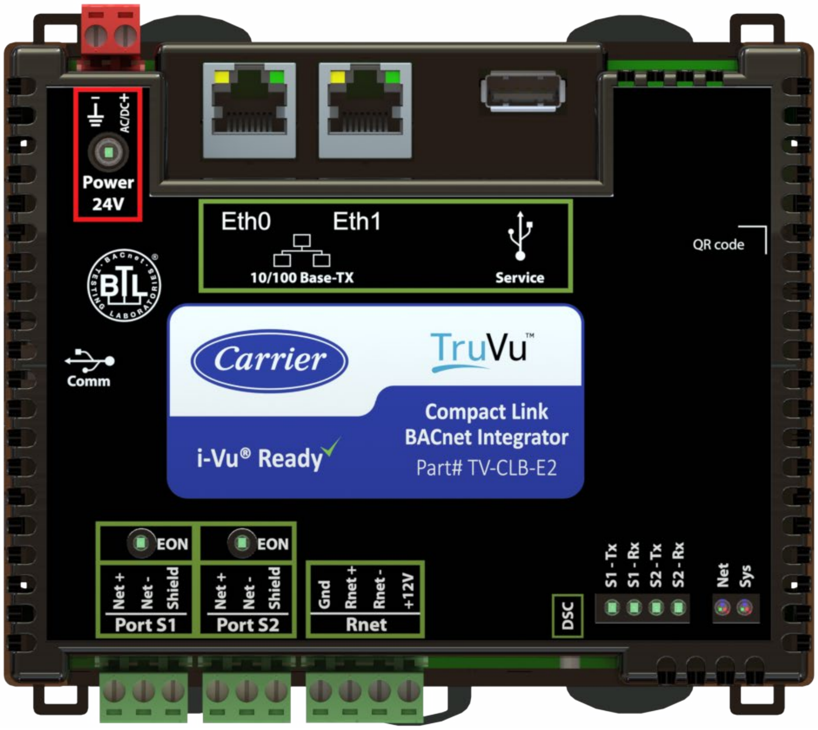
KNX Integration Guide

For TruVu™ controllers (drv_gen5)



• Catalog No. 11-808-1010-01 • 6/23/2025

⚠ Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

Contents

Overview

You can use Carrier TruVu™ controllers to integrate KNX device(s) with your i-Vu® system. The controller communicates via IP with a KNX/IP interface or router (generically referred to as “KNX/IP adapter” in the rest of this document) to read and write KNX data points.

Carrier	
Controllers	TruVu™ gateways
Driver	drv_gen5_108-04-20088.driverx or later
Read/write capability	Can read from and write to the third-party equipment
Ports	Gig-E
Third party	
Supported equipment	Any device that supports the KNX protocol
Network media type	Ethernet
Quantity of devices you can physically connect to the Carrier controller	Up to 5 KNX/IP adapters can be connected to the network, with up to 1000 KNX data points.

Before-you-begin checklist

You need the following items, information, and skills for the integration process:

□ The IP addresses of the KNX/IP adapters

□ A points list for each KNX device that includes:

- Group name
- Group address
- Data type (DPT, as per KNX specification. See *Appendix B* (page 18) for supported data types)

Points lists may be obtained from the third-party manufacturer's representative or website, or by using the KNX Engineering Tool Software (ETS) application.

□ Verification that all communication properties have been set on the KNX adapters.

□ Verification of Ethernet communication with each KNX/IP adapter to which the Carrier controller connects

□ Experience creating control programs in the Snap application

□ Experience installing, wiring, setting up, and downloading to the Carrier controller

The integration process

Follow the steps in this document to integrate one or more third-party KNX devices into an i-Vu® system using a Carrier controller. To install and network the Carrier controller, see the controller's *Installation and Start-up guide*.

1 Add the KNX/IP Adapters to your network

The KNX Engineering Tool Software (ETS) application is used to configure all your KNX devices, including the KNX/IP adapters used to connect your controller to those devices. See the *KNX ETS documentation* to learn how to set up those devices on your network.

A KNX/IP adapter, which can be either an interface or a router, is needed to allow the controller to communicate with the KNX devices. Up to 5 KNX adapters can be used on a single controller.

- A KNX/IP interface is used to provide an IP tunnel between a KNX bus and an Ethernet network. It allows the Carrier controller on the same network to communicate with the devices on the KNX bus.
- A KNX/IP router offers the same functions as the IP interface, and also provides the functionality of an “area coupler” or “line coupler” using a TCP/IP network as the linking medium. An area coupler or a line coupler is a packet forwarding bridge that moves KNX telegrams between KNX physical network segments. The distinction between an “area coupler” and a “line coupler” is simply based on whether you are inserting the router to connect distinct areas (for example, devices where the first number in the group address is different) or just between distinct lines (for example, devices where the middle number of the group address is different). This means that a KNX/IP router can be used in all the scenarios where a KNX command must be propagated to a different KNX trunk.

2 Create a control program in the Snap application

When you create your control program, use a Network I/O microblock for each third-party point.

To...	This network point type...	Use this microblock.
Read	Analog	ANI ANI2
	Binary	BNI BNI2
Write	Analog	ANO ANO2
	Binary	BNO BNO2

Formatting a KNX data point address

Use the information below to format a valid address in each microblock that you use to read or write to a third-party point.

⚠ **CAUTION**

When integrating third-party devices into the i-Vu® system, most communication problems are caused by incorrect data or typing errors in the microblock's **Address** field.

Address format:

```
knx://Data type index/Flags/Group address/IP Address/Port/Data Secure File ID
```

EXAMPLE: `knx://3/TPUE1/1.1.1/192.168.1.1/3671/0`

Where:

Field	Description
Data type index	The index value of the point’s data type. See *Appendix B* (page 18) for a list of supported data types.

Field	Description
Flags	Characters used to identify point attributes: • [U]: Indicates that the point will be updated at startup and each time the IP/KNX adapter comes online from an offline condition. The **Startup Poll Delay** property and number of updated points determine how quickly these points are initialized. See *Set up the KNX driver properties (page 9)* for more information. • [P]: Polling – If specified, indicates that this point will be continuously polled. A combination of the **Poll Delay** property value and the number of polled points determine how often these points are updated. See *Set up the KNX driver properties (page 9)* for more information. NOTES o To avoid overloading the KNX bus, a polling strategy is used to individually read input points. Entries in the **Refresh Time** field on the i-Vu **Network Points** tab are ignored for input points. o For each point configured with the polling flag set, the time between refreshes of each polled point is lengthened by the configured **Poll Delay,** so use this flag only for those points whose value must always be aligned with the current device value. o The [U] and [P] flags can be used separately or together. Behavior is as follows: ▪ U - Initialized with startup polling, after which only updated by change of status events. ▪ P - After startup polling completes, initialized during the first pass through the polling queue, which repeats continually. Change of status events are also processed. ▪ UP - Initialized with startup polling, then updated during regular polling and by change of status events. o Neither the **Update** [U] nor the **Polling** [P] flag should be used in a Data Secure point's URL. Data Secure point values cannot be polled. Their values are updated only by change of status events. o To recognize that a KNX device has gone offline, ensure that at least one of the points on each device is polled using the **Polling** [P] flag. If you are using Data Secure communication, the point that is polled for this purpose must be designated as unsecure on the device, and the **Data Secure File ID** should be set to 0 in the URL. • [T] or [R]: The connection mode of the device. Use to denote either: o Tunneling (T) – If you are using a KNX/IP interface o Routing (R) – If you are using a KNX/IP router • [Ex]: Data index x represents the position of the desired data within the data type. This is required only for data types made up of multiple values. For example, for data type B1U3, add E1 to the Flags field to retrieve the binary value, or E2 to retrieve the unsigned value.

Field	Description
Group address	The point's configured KNX 3-level group address with periods ('.') between the group levels instead of slashes ('/').
IP address	The IP address of the KNX/IP adapter.
Port	The TCP port the KNX/IP adapter uses for local communication with the controller.
Data Secure File ID	For KNX Data Secure communications, enter the ID of the file that contains the KNX keyring for the associated KNX/IP adapter. See *Set up the KNX driver properties* (page 9) for more information about how to load the keyring file(s). Set to 0 if not using KNX Data Secure, in which case unencrypted telegrams are used.

Microblocks required for read and write points

Some KNX Data Point Types (DPTs) contain more than one value. In those cases, use the [Ex] flag in the microblock's **Address** field to designate the particular value desired for the point. See *Formatting a KNX data point address* (page 3) for information about using the [Ex] flag.

For multi-value DPTs, the KNX protocol does not allow writing individual values to the third-party device; it can only write the entire data point. Therefore, multi-value DPTs must be handled in a special way, as explained below.

For one-value DPTs:

- To read, use an input network microblock.
- To write, use an output network microblock.
- It is not necessary to include the [Ex] flag in the microblock **Address.**

For multi-value DPTs:

- To read:
    - For each value in the DPT that you want to read, use an input network microblock with the value's data index specified by the [Ex] flag in the microblock **Address.**
- To write:
    - For DPTs that are 32 bits or smaller:
        - Use one output network microblock that contains all the individual values of the DPT. Your program must construct the combined value before writing. **NOTE** As an alternative to this method, the method described below for DPTs that are larger than 32 bits also works for DPTs that are 32 bits or smaller.

- For DPTs that are larger than 32 bits:
  NOTE For the following method to work, the DPT must be readable. The DPT must be read before it can be written to gather the information necessary to write the entire data point without losing existing data.
  - For every value in the DPT, even the ones you do not want to write, use an input microblock to read the current value with the value's data index specified by the [Ex] flag in the microblock **Address.**

    NOTE To resolve the "13 - Write Pending" message as quickly as possible, these input microblocks should be configured with:
    - The 'U'parameter in the Address so the point is read during startup polling
      And
    - A **Refresh Time** for periodic polling, rather than COV, should ensure that the point is read in a timely manner.
  - For each value in the DPT that you want to write, use an output microblock with the value's data index specified by the [Ex] flag in the microblock **Address.**
    NOTE You may see the "13 - Write Pending" message on this point for a short while after startup. This status will resolve itself shortly if the associated input microblocks are configured correctly (see above).

Editing a microblock address

You can edit a microblock address in the following places:

- In the Snap Property Editor
- In the i-Vu® interface, on the microblock's **Properties** page > **Details** tab
- In the i-Vu® interface, on the control program's **Properties** page > **Network Points** tab

3 Download the driver and control programs

The KNX PPD is available with driver drv_gen5_108-04-20088.driverx or later. To get and download the latest driver, see the controller's *Installation and Start-up Guide*.

1. In SiteBuilder's **Geographic** tree, add equipment for each of your control programs.
2. On the **Network** tree, assign the equipment to the controller by dragging each equipment from the **Geographic** tree and dropping it on the controller in the **Network** tree.
3. Click 💾.
4. In the i-Vu® interface, download the driver and control programs to the Carrier controller.

See the "Managing third-party points and feature licenses" section of the controller's *Technical Instructions* for instructions on how to ensure you have adequate FlexPoints licensed for your integration.

4 Set up the KNX driver properties

The driver properties can be configured in either the:

- Controller's Service Port setup pages - See *Appendix D* (page 22).

  or

- i-Vu® driver page - Select the controller's driver on the i-Vu® **Network** tree

NOTE If you are using Data Secure communications, you will need to use the controller's Service Port setup pages rather than the i-Vu® driver page to import the necessary KNX keyring files. See step 4 below.

1 On the **Protocols** > **KNX** tab, select **Enabled**.

2 In **Protocol Settings** configure the following properties:

Property	Description
Group Read Timeout	Number of seconds before declaring a **Group Value Read** request as failed if no answer is received. Valid range: 1-60
Startup Poll Delay	For points defined with the **Update** [U] flag, the time (in milliseconds) between successive Group Read requests when initializing points at controller startup and when reinitializing points after an IP/KNX adapter comes online from an offline condition. Each point with the 'U' flag is polled sequentially with this delay between each one. Valid Range: 200-3000 ms
Startup Poll Retries	For points defined with the **Update** [U] flag and without the **Polling** [P] flag, polling initially occurs during startup to establish status but isn't regularly polled after startup. If the initial startup polling fails, Startup Poll Retries is the number of times the read is retried while processing the regular polling queue. If all retries fail, the point will stay in the error state until the device receives a changes of status event. Valid Range: 1-5
Poll Delay	For points defined with the **Polling** flag, the time (in seconds) between requests to update a polled point's current value. After the startup polling is complete, each point with the 'P' flag is polled sequentially with this delay between each one. Valid range: 1-300.
User Network Interface	For points defined with the **Routing** [R] flag, enter the controller's IP address that is configured on the Gig-E Port tab. This is the network interface that listens for multicast messages. Points defined with the **Tunneling** [T] flag do not use this property.

3 If using Data Secure communication:

a) Export the keyring file from the ETS application and assign it a password (see ETS documentation for instructions). The password should be between 8-20 characters long.

b) In **Data Secure Keyring Files**, click **Add** to add a new row to the table. Enter a **File ID** from 1-5, then enter the password of the exported keyring file. **NOTE** Valid **File IDs** are 1-5. Do not add more than five rows to this table. The rows correspond to the five files in the **Files** section below.

c) In **Files,** click **Import** on the file corresponding to the **File ID** entered in the step above, then select the exported keyring file. If the keyring file saves successfully inside the controller, the **Status** column of the **Data Secure Keyring Files** table changes to "Successfully loaded".

NOTES

- The **Files** section of the **Protocols > KNX** tab is only available when using the controller's Service Port setup pages, not when accessing the driver page from i-Vu®.
- It may take a few minutes for the imported file to load. When the file has been successfully loaded, a success message will be displayed and the **Status** value of the corresponding row in the **Data Secure Keyring Files** table will be updated

  TIP File loading will be faster if the controller is not connected to the network
- To delete an imported file:
  - In **Files**, click **Delete** beside the file corresponding to the **File ID** you wish to delete. If there is an associated row in the **Data Secure Keyring Files** table, the **Status** field will change to “File not found”.
  - In **Data Secure Keyring Files**, select the row corresponding to the **File ID** you deleted, then click **Delete**.
- For more information on how to set up a Data Secure device, see *Appendix C* (page 20).

4 If you used the controller's Service Port to configure the properties:

a) If the **Restart** button is displayed, restart the controller.

b) On the i-Vu® **Network** tree, select the controller and **Upload** parameters from the controller.

5 If you used the controller's driver pages on the i-Vu® **Network** tree, select the controller and **Download** parameters to the controller.

5 Connect the Carrier controller to the third-party device

Use CAT5 or higher Ethernet cables to connect the controller and the KNX/IP adapters to a hub or switch on your network. Maximum cable length: 328 feet (100 meters)

1 Turn off the Carrier controller's power.

2 Check the communications wiring for shorts and grounds.

3 Wire the Carrier controller's Gig-E port to the network.

NOTE The Gig-E port is still capable of BACnet communication.

4 Turn on the Carrier controller's power.

5 See the KNX/IP adapter's *Installation and Start-up guide* to connect it to the network.

6 Verify the integration is set up correctly

1 On the i-Vu® **navigation** tree, select the control program for the Carrier controller.

2 Select the **Properties** page > **Network Points** tab.

If...	**Then...**
You see the point value you expect with no errors in the **Error** column	You have successfully established communication with the third-party device.
All points show question marks instead of values	The i-Vu® application is not communicating with the Carrier controller or the control program. Troubleshoot the controller's communications. See the controller's *Installation and Start-up guide*.
Error message appears	Do one of the following actions based on the code or description in the **Error** column. • **Communications Disabled for this Microblock** On the microblock's **Network Points** tab (or **Properties** page > **Details** tab), enable the microblock's **Comm Enabled** field. • **No protocol support** Verify that the **Address** in the microblock has the correct prefix: knx:// • **Unlicensed Point** You have configured more integration points than are licensed for this controller. See the "Managing third-party points and feature licenses" section of the controller's *Installation and Start-up Guide* for instructions on how to ensure you have adequate FlexPoints licensed for your integration. • All other errors: See *Appendix A* (page 15) for troubleshooting information for error codes and diagnostic information.
A value is incorrect	Verify that: • The **Address** in the microblock is correct. • The retrieved value is scaled properly, if necessary. For example, scaled from Celsius to Fahrenheit. Refer to the third-party manufacturer's documentation or the controller's Installation and Start-up guide for scaling information.

If the solutions above do not resolve the problem, gather the following information for Technical Support:

- A diagnostic capture. See *To capture communication using Wireshark* (page 14).
- Screenshots of the driver configuration pages:
    - **Protocols** > **KNX** tab
    - **Control Programs** tab
- Log files downloaded from the driver's **Advanced > Diagnostics** tab.
- A screenshot of the **Properties** page > **Network Points** tab showing addresses and errors.
- All information from a controller Modstat copied into a text file. Right-click the Modstat, then select Select All. Press Ctrl+C to copy the information, then open Notepad and paste the information into a text file.
- Installation and Start-up guide for the third-party device, if available.

To capture communication using Wireshark

Use Wireshark, a network analysis tool, to capture the Ethernet communication between the Carrier controller and the KNX/IP adapter.

PREREQUISITES

To use Wireshark to capture all Ethernet communication, provide one of the following devices:

- Ethernet hub (not a common switch)
- Port mirror on mirroring-capable switch
- Network sniffer/Test Access Port (TAP) such as SharkTap

1 Download the latest version of Wireshark from the Wireshark website (http://www.wireshark.org).

2 Run the Wireshark install program, accepting all defaults. Include WinPcap in the installation.

3 Place your capture device between the Carrier controller and the KNX/IP adapter by either:

- ○ Disconnecting the Carrier controller from the network and plugging its cable into the hub/TAP

  or

- ○ Disconnecting the KNX/IP adapter from the network and plugging its cable into the hub/TAP.

  or

- ○ Configuring the mirroring port on your switch to mirror the port the Carrier controller is connected to.

4 Connect the Ethernet port of the computer running Wireshark to the hub/TAP/port mirror.

5 Identify the IP addresses of the controller and the KNX/IP adapter(s). These will be needed to decipher the capture.

6 On the computer, go to **Start > All Programs > Wireshark.**

7 From the menu bar, select **Capture > Interfaces.**

8 Click **Start** next to the interface that is connected to the network. This starts the IP capture.

TIP Choose the interface that shows activity.

9 Allow the capture to run long enough to ensure that there is sufficient data to allow a technician to review the problem.

10 On the menu bar, select **Capture > Stop** to stop the data capture.

11 Select **File > Save** and save the capture to a convenient location. Leave the **Save as type** default set to Wireshark/tcpdump/... - libpcap (*.pcap, *.cap).

12 Send the file to Carrier Technical Support for analysis.

TIP You can color code the information in the Wireshark capture file based on user-defined criteria. See Wireshark's Help for instructions on setting up Coloring Rules.

Appendix A - Error codes and messages

PPD error codes

Error Code or Message	Possible Causes and Solutions
0 – No Error	None; point is being read or written successfully.
1 - Address Error - Invalid Data Type	Verify that the data type index given in the URL is supported. See *Appendix B* (page 18) for list of supported data types.
2 - Address Error - Invalid Flags	Verify that all characters included in the Flags field of the URL are valid. See *Formatting a KNX data point address* (page 5) for list of valid characters and their usage.
3 - Address Error - Invalid Connection Mode	Verify that the Flags field of the URL contains either a 'T' for tunneling mode or an 'R' for routing mode.
4 - Address Error - Invalid Data Index	Verify that the data index given in the URL is valid for the selected data type. Data index values start at 1, which represents the first value in the data type.
5 - Address Error - Invalid Group Identifier	Verify that the KNX group in the URL is a valid KNX 3-level group address with periods ('.') between the group levels instead of slashes ('/'). Verify that the 3 numbers are in the correct range. Assuming that the group identifier is <Main>.<Mid>.<Sub>, valid ranges are: • Main: 0-31 • Mid: 0-7 • Sub: 0-255
6 - Address Error - Invalid IP Address	Verify that the IP address given in the URL is correct and valid. IP addresses are made up of four dot-separated numbers in the range 0-255.
7 - Address Error - Invalid Port	Verify that the port given in the URL is correct and valid. Ports are integers in the range of 0-65535.
8 – Address Error – Invalid KNX Keyring File Index	The Data Secure File ID given in the URL is invalid or the loaded file is not a valid KNX keyring file. Verify that the Data Secure File ID field in the URL is in the correct range: • 0 - If KNX Data Secure is not used • 1-5 - A keyring file must be loaded in the corresponding entry in the keyring table. The keyring file's password must be entered correctly in the keyring table.
9 - Comm Error - No Response	The third-party device did not respond to a request or command. Verify

	that the data point configuration in the KNX integration matches the configuration of the third-party device (in particular, check the **Group Address**). Also, in the ETS project, check that the read operation has been enabled for the given **Group Address**.
10 - Comm Error - Invalid response	The third-party device generated an invalid response to a request or command. The packet may be incomplete, incorrect, or have an invalid checksum. Verify that the data point configuration in the KNX integration matches the configuration of third-party device (in particular, check **Group Address** and **Data Point Type**).
11 - Comm Error - Command Failed	The third-party device did not accept a command. Verify that the data point configuration in the KNX integration matches the configuration of third-party device (in particular, check **Group Address** and **Data Point Type**). Also verify that the value you are writing is within a range allowed by the device.
12 - Comm Error – Adapter offline	The KNX/IP adapter is not responding. Verify that the configured IP address and port are correct, and both the controller and the KNX/IP adapter are reachable on the network.
13 – Write Pending	At start-up, the values needed to write a multi-value DPT have not yet been read from the device. Until they are read, attempts to write will result in this message. The situation will resolve itself shortly if the necessary microblocks are configured correctly. See the "For multi-value DPTs" section of *Microblocks required for read and write points* (page 5) for more information on how to configure the microblocks needed for writing to a multi-value DPT.

General error codes

Error Code/Message	Possible Causes/Solutions
Protocol disabled or unsupported	The protocol defined in the signature of the address is either unsupported by the controller or disabled. To enable a protocol that is available on the controller: On the Network tree, click on the controller's driver, then select the Protocols tab, and then select the desired protocol tab (e.g. BACnet, Modbus, etc.) to enable. **NOTE** Enabling protocols requires a controller restart.
Initializing	This point is either: • In the process of being validated • Queued up for the initial read or write attempt to the third party device, • In the process of its initial read or write attempt to the third party device • Waiting for the initial response from the third party device. Once the startup process has completed, this error should switch to No Error or a different error that will identify any problems that may have occurred.".

Error Code/Message	Possible Causes/Solutions
No Error	The microblock is not in error. No solution needed.
Communications Disabled for this Microblock	The microblock's communications are not currently enabled. Enable the microblock's communications by checking the box under **Com Enable** in I-Vu.
Not Linked	The microblock was not successfully linked to the object to which it is addressed. Ensure that the address is entered correctly and that the object the microblock is addressed to is functioning properly.
Programmer Error – Invalid MB State	The data integrity of the microblock was compromised. This is the default error code if none of the other errors apply. If this error is persistent, contact Technical Support to let them know there is a defect to address.
Undefined Client Microblock Error	An error occurred while the microblock was attempting to write a value. This is the default error code when something goes wrong trying to write a value over the network. If this error is persistent, contact Technical Support to let them know there is a defect to address.
Device Offline – Temporary Backoff	The device hosting the object that the microblock is attempting to interact with is not powered on. Ensure that the device hosting the object, in which the microblock is addressed to, is powered on and functioning properly.

Appendix B - Supported Data Types

Use the value in the **Index** column of this table as the **Data Type Index** in your microblock address.

Index	Data Point ID	Data Point Format	**Data Point Names (examples)**
1	1.xyz	B1	DPT_Switch, DPT_Bool, DPT_Enable, ...
2	2.xyz	B2	DPT_Switch_Control, DPT_Bool_Control, DPT_Enable_Control, ...
3	3.xyz	B1U3	DPT_Control_Dimming, DPT_Control_Blinds
4	4.xyz	A8	DPT_Char_ASCII, DPT_Char_8859_1
5	5.xyz	U8	DPT_Scaling, DPT_Angle, DPT_Percent_U8, ...
6	6.xyz	V8	DPT_Percent_V8 , DPT_Value_1_Count
7	6.020	B5N3	DPT_Status_Mode3
8	7.xyz	U16	DPT_Value_2_Ucount , DPT_TimePeriodMsec, ...
9	8.xyz	V16	DPT_Value_2_Count , DPT_DeltaTimeMsec, ...
10	9.xyz	F16	DPT_Value_Temp DPT_Value_Tempd, ...
11	12.xyz	U32	DPT_Value_4_Ucount, DPT_LongTimePeriod_Sec, ...
12	13.xyz	V32	DPT_Value_4_Count, DPT_FlowRate_m3/h, ...
13	14.xyz	F32	DPT_Value_Acceleration, DPT_Value_Acceleration_Angular, ...
14	15.000	U4U4U4U4U4U4B4N4	DPT_Access_Data
15	17.001	R2U6	DPT_SceneNumber
16	18.001	B1R1U6	DPT_SceneControl
17	20.xyz	N8	DPT_SCLOMode, DPT_BuildingMode, ...
18	21.xyz	B8	DPT_StatusGen, DPT_Device_Control, ...
19	23.xyz	N2	DPT_OnOffAction, DPT_Alarm_Reaction, ...
20	26.001	R1B1U6	DPT_SceneInfo
21	27.001	B32	DPT_CombinedInfoOnOff
22	29.xyz	V64	DPT_ActiveEnergy_V64, DPT_ApparantEnergy_V64, ...
23	219.001	U8N8N8N8B8B8	DPT_AlarmInfo
24	221.001	N16U32	DPT_SerNum
25	202.xyz	U8Z8	DPT_RelValue_Z, DPT_UCountValue8_Z
26	203.xyz	U16Z8	DPT_TimePeriodMsec_Z, DPT_UFlowRateLiter/h_Z,

			…
27	204.001	V8Z8	DPT_RelSignedValue_Z
28	205.xyz	V16Z8	DPT_DeltaTimeMsec_Z, DPT_TempHVACAbs_Z, …
29	217.001	U5U5U6	DPT_Version
30	218.xyz	V32Z8	DPT_VolumeLiter_Z, DPT_FlowRate_m3/h_Z
31	225.xyz	U16U8	DPT_ScalingSpeed, DPT_Scaling_Step_Time, DPT_TariffNext
32	231.001	A8A8A8A8	DPT_Locale_ASCII
33	234.xyz	A8A8	DPT_LanguageCodeAlpha2_ASCII, DPT_RegionCodeAlpha2_ASCII
34	235.001	V32U8B8	DPT_Tariff_ActiveEnergy
35	236.001	B1N3N4	DPT_Prioritised_Mode_Control
36	238.xyz	B2U6	DPT_SceneConfig, DPT_DALI_Diagnostics
37	239.001	U8R7B1	DPT_FlaggedScaling
38	255.001	F32F32	DPT_GeographicalLocation
39	22.xyz	B16	DPT_StatusDHWC, DPT_Media, …
40	25.1000	U4U4	DPT_DoubleNibble
41	30.1010	B24	DPT_Channel_Activation_24
42	31.101	N3	DPT_PB_Action_HVAC_Extended
43	200.xyz	B1Z8	DPT_Heat/Cool_Z, DPT_BinaryValue_Z
44	201.xyz	N8Z8	DPT_HVACMode_Z, DPT_DHWMode_Z, …
45	206.xyz	U16N8	DPT_HVACModeNext, …
46	207.xyz	U8B8	DPT_StatusBUC, DPT_LockSign, …
47	209.xyz	V16B8	DPT_StatusHPM, …
48	210.100	V16B16	DPT_TempFlowWaterDemAbs
49	211.100	U8N8	DPT_EnergyDemWater
50	212.xyz	V16V16V16	DPT_TempRoomSetpSetShift[3], …
51	213.xyz	V16V16V16V16	DPT_TempRoomSetpSet[4], …
52	214.xyz	V16U8B8	DPT_PowerFlowWaterDemHPM, …
53	215.xyz	V16U8B16	DPT_StatusBOC, DPT_StatusCC
54	216.100	U16U8N8B8	DPT_SpecHeatProd
55	220.100	U16V16	DPT_TempHVACAbsNext
56	222.xyz	F16F16F16	DPT_TempRoomSetpSetF16[3], …
57	223.100	V8N8N8	DPT_EnergyDemAir
58	224.100	V16V16N8N8	DPT_TempSupplyAirSetpSet
59*	229.001	V32N8Z8	DPT_MeteringValue

60*	230.1000	U16U32U8N8	DPT_MBus_Address
61	232.600	U8U8U8	DPT_Colour_RGB
62	237.600	B10U6	DPT_DALI_Control_Gear_Diagnostic
63	240.800	U8U8B8	DPT_CombinedPosition
64	241.800	U8U8B16	DPT_StatusSAB
65	242.600	U16U16U8r6B2	DPT_Colour_xyY
66	243.600	U16U16U16U8r6B2	DPT_Colour_Transition_xyY
67	244.600	N4B4N2N2N2N2	DPT_Converter_Status
68	245.600	N4N4N4N2N2N2N2U16U8	DPT_Converter_Test_Result
69	246.600	r5B3U8	DPT_Battery_Info
70	248.600	N8U8U8U8B8	DPT_Converter_Info_Fix
71	250.600	r4B1U3r4B1U3B8	DPT_Brightness_Colour_Temperature_Control
72	251.600	U8U8U8U8r8r4B4	DPT_Colour_RGBW
73	252.600	r4B1U3r4B1U3r4B1U3r4B1U3B8	DPT_Relative_Control_RGBW
74	253.600	r4B1U3r4B1U3r4B1U3B8	DPT_Relative_Control_xyY
75	254.600	r4B1U3r4B1U3r4B1U3	DPT_Relative_Control_RGB
76	257.wxyz	F32F32F32	DPT_Value_Electric_Current_3
77	272.600	N8U16U16U8U8	DPT_Converter_Info
78	273.xyz	B8U16U8F16F16	DPT_Forecast_Temperature, …
79	274.001	B8U16U8U8U8	DPT_Forecast_Wind_Direction
80	276.1200	U8U8U8r3B5	DPT_ERL_Status

*Microblocks convert integer values to floats. Therefore, integer values outside the following ranges will result in a loss of precision.

- Unsigned Integer (U32): 0 – 16,777,215
- Signed Integer (V32): -8,388,608 – 8,388,607

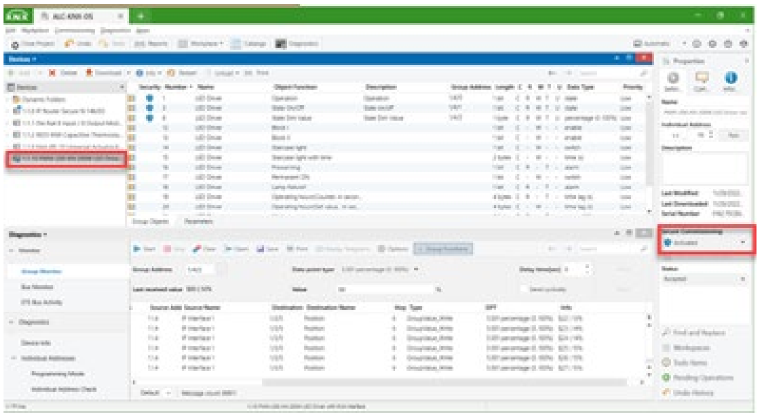
Appendix C - KNX Data Secure Commissioning

Set up KNX device to communicate in Data Secure mode

1 In ETS, add the Data Secure device to the KNX project.

2 Highlight the device and activate **Secure Commissioning**. A blue shield will be displayed over the device's icon in the list.

NOTE **Secure Tunneling** should remain deactivated.



3 Enter the **Device Certificate**, which can be found on the front of the device label (example pictured below). You can either enter the key manually, or use a scanner connected to your device.

4 Assign a **Group Address** to desired objects. To do this, right-click the object and choose **Link with...** A Blue Shield will be displayed in the **Security Column**.

5 Highlight the device in the project, click **Download**, then choose **Download All** from the drop-down to download your configuration to the device. Follow the download prompt to press the programming button on the device to start the download process.

Export KNX Keyring File of a Data Secure Device

1 Click on ⓘ above **Project Details**, then click **Security**.

2 Select all secure devices that will be connected to a single KNX/IP adapter, then click **Backup Keyring**.

3 Enter Keyring password.

Set up the controller to use Data Secure Keyring File

1 Log in to the controller's Service Port and select **Protocols > KNX**.

2 Click **Add** and enter a **File ID** between 1 and 5, then enter the **Keyring File Password**.

3 In the **Files** section, click **Import** for the keyring file that corresponds to the **File ID** given in the table in the previous step. For instance, if the **File ID** entered was "1", click **Import** for **Keyring File 1**.

Configure network microblock URL

Select a network microblock (ANI/BNI/ANO/ANO2/BNO/BNO2) and enter the URL address, indicating which Keyring File applies to the point.

Neither the **Update** [U] nor the **Polling** [P] flag should be used in a Data Secure point's URL. Data Secure point values cannot be polled. Their values are changed when the device sends a change of status event.

Example: **knx://10/T/1.0.4/169.135.66.153.3671/1** where the "1" at the end of the URL indicates you are using Data Secure with Keyring File 1.

Appendix D - Configuring the driver parameters by using the Service Port

You can set many driver parameters locally from the controller by using the **Service Port's** web-based controller setup interface. You can set operational parameters, such as port and communications' protocol settings, without the need to connect the i-Vu® application to the controller. Any parameters set locally through this interface take effect immediately. To connect to the controller setup pages, some controllers have an Ethernet Service Port, and some have a USB Service Port.

⚠ **WARNING** After setting parameters locally through the Service Port interface and then connecting the controller to the i-Vu® application, proceed carefully, as follows:

In the i-Vu® application, you must **upload** the parameters that you set locally BEFORE you **download** memory or parameters. Downloading, without uploading first, overwrites all the settings you made through the **Service Port**. Uploading first preserves those parameters.

NOTE There are a few parameters that can **only** be set through the **Service Port**, such as the controller's IP address, and these are not overwritten by a memory or parameter download from the i-Vu® application.

For more information on connecting to the Service Port, see the "Connecting to the router through the Service Port" and the "Connecting to the router through the Gig-E Port" sections of the controller's *Installation and Start-up guide*.

Appendix E - Module status field descriptions

Property	Description
KNX Protocol Details	Communications - Number of data packets transmitted and received by the integrator - Number of timeouts that occurred when attempting to read or write to a third-party device

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
		No updates yet	

* For internal use only

Carrier ©2025 · Catalog No. 11-808-1010-01 · 6/23/2024