



Agenda

- KNX Security general
- KNX Data Security
- KNX IP Security
- Secure Devices
- Security in ETS5

 (\mathbf{R})



KNX Security

KNX[®]

Based on AES

Advanced Encryption Standard

Subset of Rijndael (Rijmen + Daemen) chipher

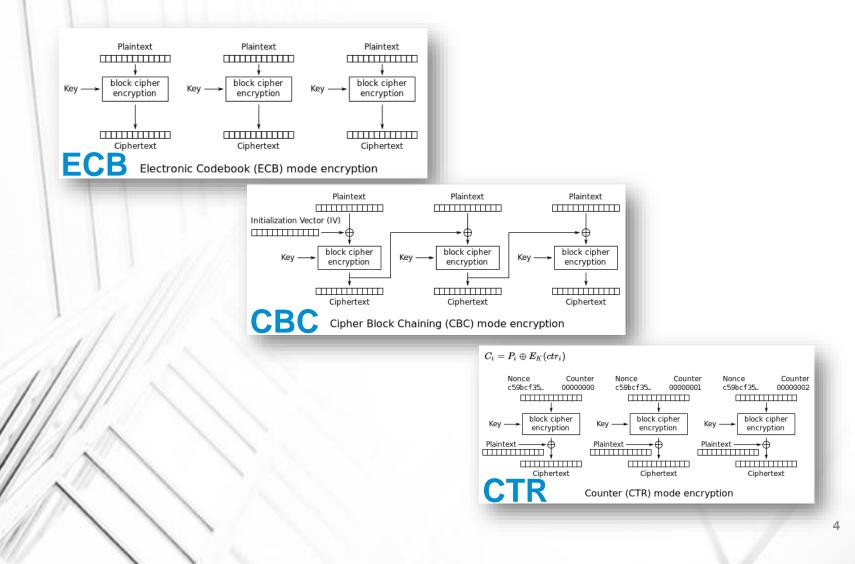
Since 2000 "de facto" standard for symmetric encryption

- Block length: 128 bits
- Key length: 128, 192, 256 bits
- Operational modes: ECB, CBC, CFB, OFB, CTR



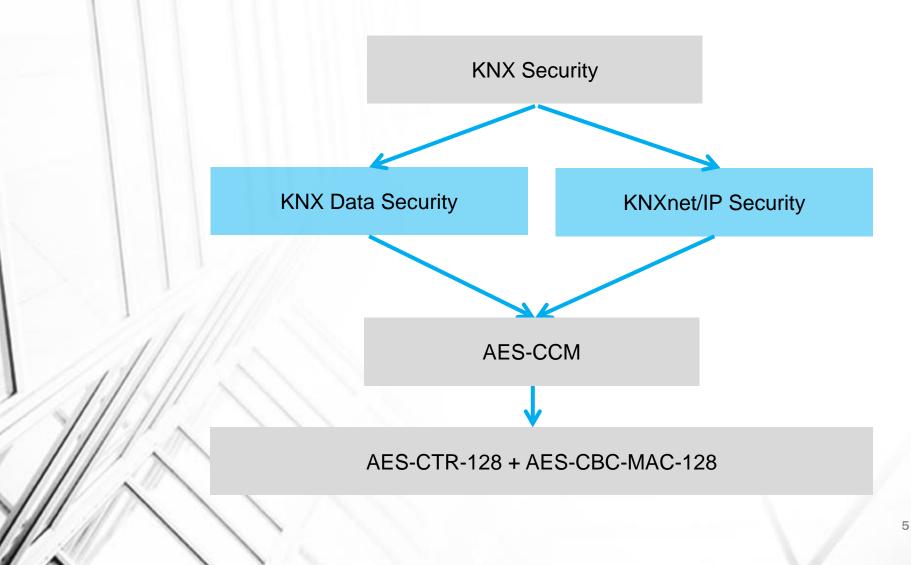


KNX Security: AES modes





KNX Security





KNX Security Properties

Data Integrity

 Prevents an attacker from manipulating the data. (MAC)

Freshness

 Prevents data from being recorded and replayed. (SeqNo)

Confidentiality

Data is encrypted. (AES)

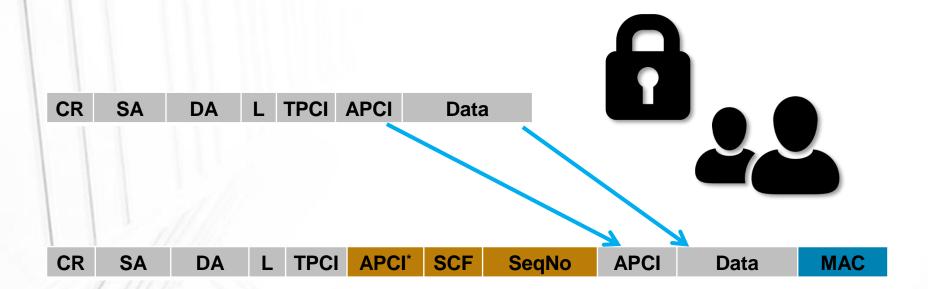








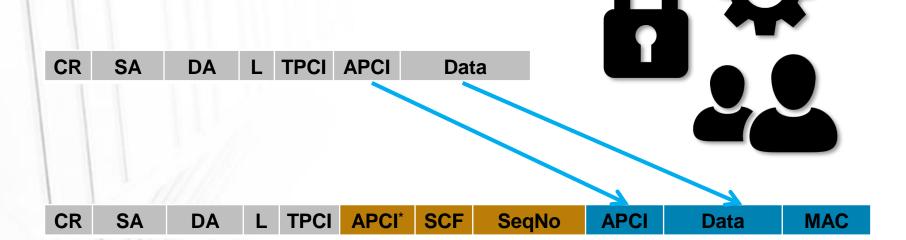
KNX Data Security: Authentication



7



KNX Data Security: Authentication and Encryption





KNX Data Security: Keys

FDSK (Factory default setup key)

- Active on commissioning
- Reactivated after master reset
- Non-readable/non-writable

Tool key

- Replace FDSK
- Writable only

P2P keys

- Point-to-point communication
- Readable/writable

Group keys

- Runtime communication
- Readable/writable



KNX Data Security: Sequence counter

48-bits long

Sending

- One per device
- Continuously incremented on sent message
- PID_SEQUENCE_NUMBER_SENDING

Receiving

- One per communication partner (device)
- Accept only higher values
- PID_SECURITY_INDIVIDUAL_ADDRESS_TABLE

Tool access

- Accept only higher values
- Non-readable/non-writable

Storage!



KNX Data Security: Sync procedure

Request

Secure APCI	SCF	SeqNr _{local}	KNX Serial Number	Challenge	MAC
1 0 bit	1 octet	6 octets	6 octets	6 octets	4 octets
3F1h	9Ah			N ₁	

Response

Secure APCI	SCF	Challenge XOR Random	SeqNr _{remote}	SeqNr _{local}	MAC
10 bit	1 octet	6 octets	6 octets	6 octets	4 octets
3F1h	9Bh			N ₁	

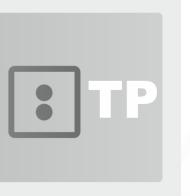


KNX TP Push Button 420 secure

T

KNX TP Push Button

- Series MATCH 55
- For standard frame 55 mm
- Single rocker or double rocker
- With KNX Security





KNX RF / ENO Push Button 440 secure



KNX RF / ENO Push Button 440 secure

- Series MATCH 55
- For standard frame 55 mm
- Single rocker or double rocker
- Integrated interface USB to KNX RF
- Power supply via battery CR2032
- with KNX Security
- KNX RF/TP media coupler
 673.1 secure





KNX IO 511.1 secure

1TE し GRÖSSE OUTPUT INPUT 5 8 • 0 SECURE ETS TP WEINZIERL On/1 Ch/N 10 2I secure -/2 P/Esc O X 511.1 () E S 0 6 📎

Input and Output

For getting started with KNX data security

First secure device of KNX IO compact series

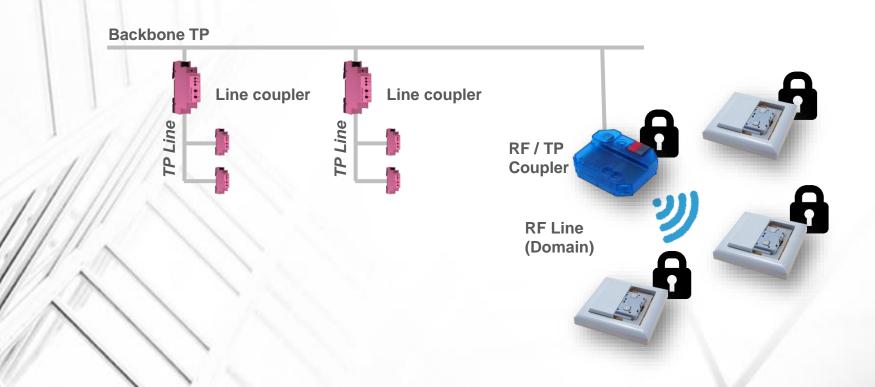
ETS Edit Wg/kplace Commissionin Close Project Copology Copolog	edo Reports	Workplace *	Print tion Ap KND KND	Diagnostic	n		dr Prg Par Grp (Veinzierl			Order KNX IC KNX IC
Topology ▼ Add Devices ▼ X Delete	nload Se Addres Room C 11.05 C 11.021	Reset 4 Unload • Descript	Print tion Ap KND KND	oplication Program X IO 511 (1021) sec	n		0000	Veinzierl	Engineering (GmbH	Order KNX IC KNX IC
Add Devices X Delete Down Topology Cynamic Folders Dynamic Folders I I New area I I New Inee I I ALS KNX IO 511 (1021) secure I I.1.221 KNX IO 511 (1022)	Se Addres Room	Descript	tion Ap KND KND	X IO 511 (102I) sec	ure		0000	Veinzierl	Engineering (GmbH	Order KNX IC KNX IC
Topology Oynamic Folders J 1 New Ince Tot New Ince Tot New Ince Tot New Ince Tot I.1.85 KNX IO 511 (1021) secure Tot I.1.221 KNX IO 511 (1021) secure Te	Se Addres Room	Descript	tion Ap KND KND	X IO 511 (102I) sec	ure		0000	Veinzierl	Engineering (GmbH	KNX IC
Dynamic Folders 11 New area 11 New ine 11.1 New inne 11.1 S KNX IO 511 (1021) secure 11.121 KNX IO 511 (1021) secure Te	est Project KN		KND	X IO 511 (102I) sec	ure		0000	Veinzierl	Engineering (KNX IC
1 New area 1.1 New line 1.1 New line 1.1 S5 KNK IO 511 (102!) secure 1.1.221 KNK IO 511 (102!) secure Te	est Project KN	X_IO511_secu	KNJ			-					KNX IC
E 11 New line E 11 New line E 11.85 KNX IO 511 (102) secure E 11.221 KNX IO 511 (102) secure Te	est Project KN;	X_IO511_secu		X IO 511 (1O2I) sec				- Weinzierl	Engineering (GmbH	
▶ 🙀 1.1.85 KNX IO 511 (1021) secure ▶ 📲 1.1.221 KNX IO 511 (1021) secure ■ TE	2	X_IO511_secu	re								Last Madifieds
▶ 🖬 1.1.221 KNX IO 511 (1021) secure	2	X_IO511_secu	re								Last Madified: 1
Te	2	X_IO511_secu	re								Last Madified: 1
	2	X_IO511_secu	re								Last Madified: 1
	2	X_IO511_secu	re								Last Modified: 1
	2	X_IO511_secu	re								Last Medified:
	2	<_iOD11_secu	e								
ear											Last Moullieu.
	Details	Security		Project Log	Dr	oject Files					
	Details	security		Project Log	PR	oject riles					
	_										
	Export										
	Export Keyring										
_											
	Device Certificates										
	🕂 Add 🛛 🗙 De	elete									
	Serial Number 🔺	Factory Key (FDS	K)	D	evice						
	00C5:05110511	000102030405060	708090A0E	BOCODOEOF 1.	.85 KNX IO	511 (102I)	secure				
	00C5:FFFFEE11	000102030405060	708090A08	BOCODOEOF							
	00C5:FFFFEE22	000102030405060	708090A08	BOCODOEOF							



Mixing secure and non-secure

Security per link Security in sub-systems

- KNX Secure Proxy
- In preparation for ETS





KNX IP Security

XA



- Be secure in IP
- Stay compatible on TP

KNX IP Secure Devices

- KNX IP Security
- KNX Data Security

KNX IP Interface secure

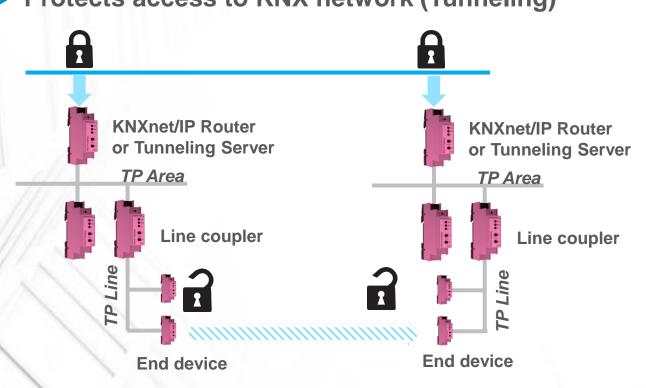
KNX IP Router secure

Medium KNX IP secure



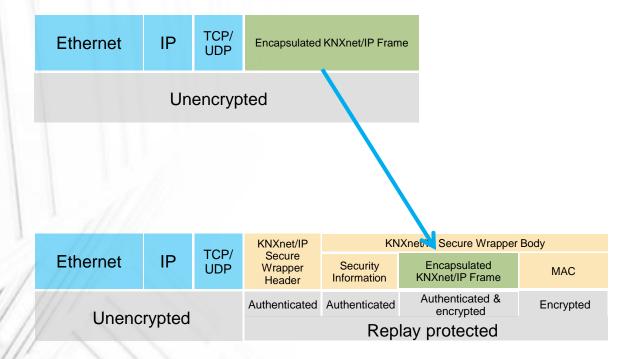
KNXnet/IP Security

Protects data within IP network (Routing)
 Protects access to KNX network (Tunneling)





KNXnet/IP Security: Frame





KNXnet/IP Security: Features

Multicast communication (routing)

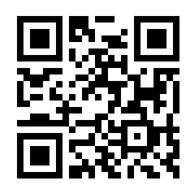
- Fix key
- Sequence counter \rightarrow timer based
- Sync mechanism

Unicast communication (sessions)

- Individual key negotiated using ECDH (Curve25519)
- Device authentication code
- User password



KNX IP Security: Keys



FDSK (Factory Default Setup Key)

- Active on commissioning
- Reactivated after master reset
- Non-readable/non-writable
- Via QR Code

Tool key

- Replace FDSK by ETS
- Not visible to customers



Scanning FDSK in ETS





Adding Device Certificates KNX IP Interface 732 secure

This device supports secure configuration. To do so, ETS must know the factory key of that device, that you can find printed on the device or in the packaging. If you do not have access to this information now, you can enter the key later in the dashboard or before downloading the device.



ADC777 - 674ZZ5 - OIC5HU - OV2JAZ

- IA3DGS

- VDBYEE

Serial Number 00C5:FFFFDFE6

Factory Key 73D7205D3D1D5D2419A8C3821100D8CD

Cancel



Device Certificates

Overview Bus	Catalogs	s Settings								Κ Ν
Projects Archive	ETS Inside			KNX IP Interface 73	2 secure				Last Modified: 02.11.2	018 09:46 Total size:
+ 🗷 🛓 土			Search	Details	Security	Project Log	Project Files			
Name	Last Modified			Export						
KNX IP Interface 732 secure				Export Keyring						
KNX IP Router 752 secure										
2018-10-25-001 Misc. device:				Device Certificates						
KNX Stack Demo	17.10.2018 14:54			🕂 Add 🛛 🗙 Delete						
KNX Stack Demo (Secure)	17.10.2018 14:54	Unknown		Serial Number Facto			Device			
KNX BAOS 83x Demo	17.10.2018 14:54	Unknown		00C5:FFFFDFE8 15CE	43CF0C1C41FF9B394	66CF1077836	1.1.65 KNX IP Interface 7	32 secure		
KNX BAOS 840 Demo	17.10.2018 14:53	Unknown								



KNX IP Interface 732 secure



First KNX IP Interface with 18mm width (1 Unit)

- KNXnet/IP Tunneling
- Up to 8 simultaneous connections

User Interface

- Display of tunneling connections on the device
- Display of communication errors



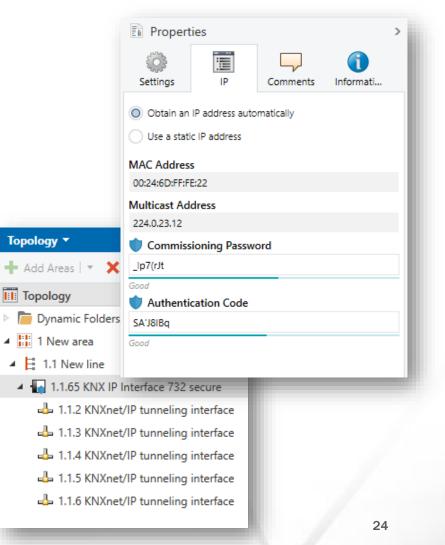
KNX IP: Individual addresses

Device address

As with all devices

Additional physical addresses

- One for each connection
- Must not be the same as your own device address
- Must not be used by other devices
- Since ETS5: Visible in the topology view





IP Settings with Security

ETS5™ - KNX IP Interface 732 secure						-	٥	×
ETS Edit Workplace Commissioning Diagnos								^ ?
Close Project 🖍 Undo 🔨 Redo 🚔	Reports Workplace 🔻 🛄 Cata	alogs Diagnostics						
KNX IP Router 752 secu KNX IP Interface 732 sec	×			🖬 Properti	es			>
Topology 🔻			^	• × 🍈			(1)	
🕂 Add Areas 🔹 🗙 Delete 🔮 Download 🔹 🕜	Help 🌛 Highlight Changes Default Pa	rameters Grant Customer Access		Settings		Comments	Informat	ti
Topology	1.1.65 KNX IP Interface 732 secu	ıre > General settings		Obtain an I	Obtain an IP address automatically			
Dynamic Folders	Use a static	Use a static IP address						
A 11 1 New area	General settings	Prog. mode on device front	Disabled O Enabled	MAC Address				
▲ 🗄 1.1 New line		Manual operation on device	10 min	00:24:6D:FF:FE				
🔺 🌆 1.1.65 KNX IP Interface 732 secure		· · ·		Multicast Add	ress			
1.1.2 KNXnet/IP tunneling interface				224.0.23.12				
👍 1.1.3 KNXnet/IP tunneling interface				Commissi	oning Password			
1.1.4 KNXnet/IP tunneling interface				_lp7(rJt	5			
👍 1.1.5 KNXnet/IP tunneling interface				Good		_		
👍 1.1.6 KNXnet/IP tunneling interface				单 Authentic	ation Code			
				SA'J8IBq				
				Good				
				🔎 Find and	l Replace			
				Workspa	aces			
				O Todo Ite				
				Pending				
1		¢		>				
	Group Objects Parameter			🎸 Undo Hi	story			
KNX IP Interface 732 secure (192.16		1.1.65 KNX IP Interface 732 secure			Last used workspac	e		



Secure Interface

ETS5™ - KNX IP Interface 732 secure				– ō ×		
ETS Edit Workplace Commissioning Diagnost	tics <u>A</u> pps Wi <u>n</u> dow			^ (
🔊 Close Project 🌾 Undo 🐴 Redo 🚔 F	Reports 🔡 Workplace 🔻 🧾 Cata	logs Diagnostics				
KNX IP Router 752 secu KNX IP Interface 732 se.	×			Properties >		
Topology 🔻			∧ ∂	× 🔅 🖻 🤉 🕦		
🕂 Add Areas 🔹 🗙 Delete 🔮 Download 🔹 😮	Help 🤌 Highlight Changes Default Pa	rameters Grant Customer Access		Settings IP Comments Informati		
Topology •	1.1.65 KNX IP Interface 732 secu	re > General settings		Name		
Dynamic Folders			KNX IP Interface 732 secure			
▲ 🔡 1 New area	General settings	Prog. mode on device front	Disabled O Enabled	Individual Address		
▲ 🗄 1.1 New line		Manual operation on device	10 min	1.1 . 65 + Park		
🔺 🌆 1.1.65 KNX IP Interface 732 secure				Description		
占 1.1.2 KNXnet/IP tunneling interface						
占 1.1.3 KNXnet/IP tunneling interface						
占 1.1.4 KNXnet/IP tunneling interface						
👍 1.1.5 KNXnet/IP tunneling interface				Last Modified 02.11.2018 08:25		
👍 1.1.6 KNXnet/IP tunneling interface				Last Downloaded 31.10.2018 15:41 Serial Number 00C5:FFFDFE8		
				Senai Number OUCS.FFFFDFE6		
				Secure Commissioning		
				Activated		
				Secure Tunneling		
				🔷 Activated 🗸 🗸		
				Find and Replace		
				Workspaces		
				O Todo Items		
				Pending Operations		
		¢		>		
	Group Objects Parameter			🖍 Undo History		
KNX IP Interface 732 secure (192.16		1.1.65 KNX IP Interface 732 secure		Last used workspace		



Secure Tunnel

ETS Edit Workplace Commissioning Diagnostic Close Project Image: Close	eports Workplace • E Cat		∧ [Properties 2					
Topology ▼ ► Add Areas ▼ 🗙 Delete 붗 Download ▼ 🕜 H	ielp 🥒 Highlight Changes Default Pa	rameters Grant Customer Access	∧ (î						
🕨 Add Areas 🔻 🗙 Delete 🔮 Download 👻 🕜 H		rameters Grant Customer Access	^ ć						
		rameters Grant Customer Access							
Topology	1165 KNIX IP Interface 732 secu	Add Areas 🔹 🗙 Delete 붗 Download 🝷 🔇 Help 🥒 Highlight Changes 🛛 Default Parameters 🛛 Grant Customer Access							
		ure > General settings		Name					
🛅 Dynamic Folders									
1 New area	General settings	Prog. mode on device front	Disabled O Enabled	Individual Address					
▲ 🗄 1.1 New line		Manual operation on device	10 min	1.1 . 2 🗘 Park					
I.1.65 KNX IP Interface 732 secure				Description					
1.1.2 KNXnet/IP tunneling interface									
1.1.3 KNXnet/IP tunneling interface									
1.1.4 KNXnet/IP tunneling interface				•					
占 1.1.5 KNXnet/IP tunneling interface				Password					
📥 1.1.6 KNXnet/IP tunneling interface				bhkgz237					
				➢ Find and Replace					
				Workspaces					
				⑦ Todo Items					
				Pending Operations					
	Associations Parameter	٤		Undo History					
KNX IP Interface 732 secure (192.16 *		1.1.2 KNXnet/IP tunneling interface		Last used workspace					



Password for Tunnel



This connection is secured

Please enter the login data: Commissioning Password

)g/NAAEI

Authentication Code (optional)





KNX IP Router 752 secure



First KNX IP Router with 18mm width (1 Unit)

- KNXnet/IP Tunneling
- Up to 8 simultaneous connections
- KNXnet/IP Routing
- Filter table for main groups 0..31

User Interface

- Diagnosis functions via buttons
- Display of communication errors



Secure Router

ETS5™ - KNX IP Router 752 secure ETS Edit Workplace Commissioning Dia	mostics Apps Window						-	٥	×
Close Project 🖍 Undo 🐴 Redo 🧯		Catalogs Diagnostics							
KNX IP Router 752 secu × KNX IP Interface 73					Prope	rties			>
Topology ▼ I Add Areas ▼ 🗶 Delete 붗 Download ▼	🕜 Help 🥒 Highlight Changes Defau	ult Parameters Grant Customer Access		▲ 🗆 🗙	Settings	IP	Comm	(i) Inform	
 Topology Dynamic Folders 15 New area 15.15 New line 15.15 New line 15.15.1 Additional individual address 15.15.2 Additional individual address 15.15.4 Additional individual address 15.15.4 Additional individual address 15.15.5 Additional individual address 15.15.5 Additional individual address 	15.15.0 KNX IP Router 752 > Routing General settings Routing (KNX -> IP) Routing (IP -> KNX)	ting (IP -> KNX) Group telegrams (main groups 0 to 13) Group telegrams (main groups 14 to 31) Individual addressed telegrams Broadcast telegrams Repetition of group telegrams Repetition of individual addressed telegram Repetition of broadcast telegrams	Filter Filter Filter Block Route Disabled Finabled Disabled Finabled Disabled Finabled	•	 Obtain a Use a sta MAC Addree Unknown Multicast A 224.0.23.12 Commi Y,Xz#.A2 Good Authen 4R,Pfj20 Good Good Find a Works 	tic IP addre ss ddress ssioning P tication Co	assword ode	/	
	Group Objects Parameter				 Todo I Pendir Undo 	ng Opera	tions		
KNX IP Interface 732 secure (192.16 +		15.15.0 KNX IP Router 752			Last use	d workspace			



Secure Router general

III ETS5™ - KNX IP Router 752 secure ETS Edit Workplace Commissioning Dia	monting Appr Window				- 0 ×
ETS Edit Workplace Commissioning Dia		Catalogs Diagnostics			^ U
KNX IP Router 752 secu × KNX IP Interface 73				Properties	>
Topology 🔻					- ()
🕂 Add Areas 🔹 🗙 Delete 🛨 Download 🔹	🕐 Help 🥒 Highlight Changes Defa	It Parameters Grant Customer Access			mm Inform
Topology	15.15.0 KNX IP Router 752 > Gen	eral settings		Name KNX IP Router 752	^
▲ 👫 15 New area	General settings	Note: For device name and IP settings	see dialog "Properties"	Individual Address	
 I5.15 New line I5.15.0 KNX IP Router 752 	Routing (KNX -> IP)	Prog. mode on device front	Disabled O Enabled	Description	0 🗘 Park
 15.15.1 Additional individual address 15.15.2 Additional individual address 	Routing (IP -> KNX)	Manual operation on device	Enabled without time limit	•	
 15.15.3 Additional individual address 15.15.4 Additional individual address 15.15.5 Additional individual address 				Last Modified 02.11.20 Last Downloaded - Serial Number - Secure Commissioning Activated Activated Add Device Certificate Status Unknown ✓ Find and Replace ✓ Vindo History	• •
KNX IP Interface 732 secure (192.16	Group Objects Parameter	15 15 O KNIV ID Pourses 750			
KINA IF Interface / 52 Secure (192.10		15.15.0 KNX IP Router 752		Last used workspace	



Secure Router KNX -> IP

Image: Image	gnostics Apps Window				- 0 × ^ (2)
Close Project Oracle Close Project Oracle Close Project Oracle Close Project Oracle Close Close Project Oracle Close Project Oracle Close Close Project Oracle Close Project Orac	Reports Workplace •	It Parameters Grant Customer Access		▲ 🗇 🗙	Properties Settings IP Comm Name
 Dynamic Folders Dynamic Folders I 5 New area 15.15 New line 15.15.0 KNX IP Router 752 15.15.1 Additional individual address 15.15.2 Additional individual address 15.15.4 Additional individual address 15.15.5 Additional individual address 15.15.5 Additional individual address 15.15.5 Additional individual address 	General settings Routing (KNX -> IP) Routing (IP -> KNX)	Group telegrams (main groups 0 to 13) Group telegrams (main groups 14 to 31) Individual addressed telegrams Broadcast telegrams Acknowledge (ACK) of group telegrams Acknowledge (ACK) of individual addressed telegrams	Filter Filter Filter Block Only if routed Only if routed	•	KNX IP Router 752 Individual Address 15.15 0 C Park Description Last Modified 02.11.2018 08:24 Last Downloaded - Serial Number - Secure Commissioning Activated C Secure Commissioning Activated C Secure Commissioning Activated C Secure Commissioning Activated C Secure Commissioning Activated C Secure Commissioning C Activated C Activated C Activated C C Activated C Activated C A
KNX IP Interface 732 secure (192.16	Group Objects Parameter	15.15.0 KNX IP Router 752			Last used workspace



Secure Router IP -> KNX

III ETS5™ - KNX IP Router 752 secure					- 0 ×
ETS Edit Workplace Commissioning Diag					^ (2
💿 Close Project 🦨 Undo 🔷 Redo 🦨	Reports Workplace •	Catalogs Diagnostics			
KNX IP Router 752 secu X KNX IP Interface 73	32 se				Properties >
Topology 🔻				∧ □ ×	۵ 🖵 🛅
🕂 Add Areas 👻 🗙 Delete 붗 Download 🔻	🕐 Help 🤌 Highlight Changes Defa	ult Parameters Grant Customer Access			Settings IP Comm Inform
Topology •	15.15.0 KNX IP Router 752 > Rou	iting (IP -> KNX)			Name
Dynamic Folders					KNX IP Router 752
▲ 🔢 15 New area	General settings	Group telegrams (main groups 0 to 13)	Filter	•	Individual Address
▲ 🗄 15.15 New line	Routing (KNX -> IP)	Group telegrams (main groups 14 to 31)	Filter	-	Description
 In 15.15.0 KNX IP Router 752 In 15.15.1 Additional individual address 		Individual addressed telegrams	Filter	•	
 15.15.2 Additional individual address 	Routing (IP -> KNX)	Broadcast telegrams	Block O Route		
15.15.3 Additional individual address		Repetition of group telegrams	Disabled Enabled		
15.15.4 Additional individual address					Last Modified 02.11.2018 08:24
15.15.5 Additional individual address		Repetition of individual addressed telegran	ns 🔵 Disabled 🔘 Enabled		Last Downloaded - Serial Number -
		Repetition of broadcast telegrams	Disabled O Enabled		
					Secure Commissioning
					Activated
					Add Device Certificate
					Status Unknown
					Find and Replace
					Workspaces
					🕗 Todo Items
					Pending Operations
	Group Objects Parameter				🖍 Undo History
KNX IP Interface 732 secure (192.16		15.15.0 KNX IP Router 752			Last used workspace



ETS Connection Manager

ETS5™ - KNX IP Interface 732 secure ETS Edit Workplace Commissioning	Diagnostics Apps Window			- ¤ ×
	atalogs Settings			KNX
 Connections Interfaces Options Monitor 	Current Interface L1.60 KNX IP Interface 732 secure Individual Address: 11.2 Configured Interfaces +			 IP Tunneling Name KNX IP Interface 732 secure Host Individual Address 1.1.60
Group Monitor Bus Monitor	Discovered Interfaces 15.15.99 00-24-6D-01-80-68 10.1 KNX IP BAOS 777 - Rt 15.15.55 KNX IP Baos 777 Ms	192.168.1.68:3671 192.168.1.224:3671 192.168.1.45:3671	00:24:6D:01:80:68 00:24:6D:01:06:94 00:24:6D:00:E1:33	Individual Address 1.1.2 Address free? IP Address
 Diagnostics Unload Device Device Info 	L1.60 KNX IP Interface 732 secure	192.168.1.47:3671	00:50:C2:55:40:78	192.168.1.47 Port 3671
 Individual Addresses Programming Mode Individual Address Check 				MAC Address 00:50:C2:55:40:78
Line Scan				
			ETS Version	Ok Test Select ETS 5.6.6 (Build 1190) License Demo Apps 0 active



Thank You for your Attention!

Weinzierl Engineering GmbH