



Question:

Why am I getting the TFTP error message in INCA and in XCT tool or why can I not see the firmware version from my (F/X)ETK in HSP Update Tool?

I want to update my firmware of my (F/X)ETK using the HSP Update Tool, to initialize my (F/X)ETK in INCA or to download the configuration of my (F/X)ETK using the XCT tool. This is unfortunately not possible due to the following error message:

Fehler - H	Hardwarekonfiguration	×
⊗	Die Methode setupTarget für Gerät XETK:3 ist fehlgeschlagen. Fehler im ASAM-MCD-1b-Gerät Kommunikationsfehler Fehler im XETK-Protokolltreiber TFTP-Fehler. Kommunikationsprotokoll konnte nicht vom Gerät abgeholt werden Erneuter Versuch TFTP-Datei zu übertragen (XEtkProtocol_Main.log) (Seriennummer des Gerätes: 2394, Aliasnamen des Gerätes: 'Aliasname nicht gesetzt') (a1b_XETK.log)	
	OK	

ISP Update Tool - XETK (SN 1001191	195)					8 3		×
<u>File Functions View Tools Drivers</u>	Window Help							
🔍 🚳 💋 HSP V11.8.1	- 🔩 🥌 🍓 🖻	1 🗖 😼 🗖 🗖 🕹 🗖 🕯	· £* -					
Hardware	4	Details XETK (S	N 100119195)					1 Þ x 🖪
Ethernet Interface XETK (SN 100119195)		Component -	Installed Version	Version in Serv	State Description			roperties
	**							
		*Starting search for h SPS Server XETK Sys *Search for hardware	ardware .tems : Hardware found: XET finished	K (SN 10011919)	5)			
8							HSP V	11.8.1

Applicati	ion Log 🗸 🗸
Time	Text
14:48:53	Connected (X)ETK has Senal Number 0119195.
14:49:05	Communication-Error, Error in XETKProtocol driver Communication-Error, Error in XETKProtocol driver TFTP error, Unable to get communication protocol from device, Retry TFTP file transfer (XEtk Protocol_Mai.
14:49:05	Unable to load configuration from device with serial number 1001191951
14:49:05	Searched for connected hardware devices.
14:49:05	The currently connected (X)ETK device (XETK-V2.0A) is not yet supported
14:49:09	Connected (X)ETK has Serial Number 0119195.
14:49:21	Communication-Error, Error in XETKProtocol driver Communication-Error; Error in XETKProtocol driver TFTP error; Unable to get communication protocol from device; Retry TFTP file transfer (XEIk Protocol_Mai.
14:49:21	Unable to load configuration from device with serial number 1001191951
14:49:21	Searched for connected hardware devices.
14:49-21	The currently connected (X)ETK device (XETK-V2.0A) is not yet supported





The connection is always initiated by PC to the (F/X)ETK. The (F/X)ETK sends data only if a connection is already established. The XCP connections use the service TCP or UDP and use for that always the port 1802. Changes to the configuration or the firmware will be read so the TFTP protocol will be used.

To use the TFTP protocol the ports 69 and 19000 to 19007 must be released in the firewall for the protocol type UDP. The port 69 of (F/X)ETK waits for the build up of first communication. For all responses to the (F/X)ETK the ports in the range of 19000 to 19007 will be used.

Service	Туре	PC source port number	XETK dest. port number	Remarks / Description
ETAS IP Management	UDP	18001	18001	Not needed for Fixed IP and DHCP managed devices
ХСР	P TCP, 102465535 1802 UDP		1802	MC: INCA uses TCP. 3 rd party tools may also use UDP
				RP: Bypass normally uses UDP, but in special cases could use TCP
TFTP connect	UDP	102465535	69	
TFTP transfer	UDP	102465535	1900019007	PC uses the same random port that was used for TCP connect

The easiest way is to completely deactivate the firewall. If that not possible an exception must be created for the used ports or the programs in the firewall settings.

In *Windows 10* this can be done over the *Windows Defender Firewall*. For other tools the own IT must be requested.



Create an exception for a program:

1. Start the *Windows Defender Firewall* with Advanced Security over the Windows Start icon and the input of the words **Windows Defender**.

0



2. Right click on Inbound Rules and select New Rule....

-			
	New Inbound Rule Wizard	4	×
F	Rule Type		
s	elect the type of firewall rule to c	xeate.	
S	teps:	2	
۲	Rule Type	What type of rule would you like to create?	
۲	Program		
۲	Action	Program	
۲	Profile	Rule that controls connections for a program.	
۲	Name	○ Port	
		Rule that controls connections for a TCP or UDP port.	
		O Predefined:	_
		@FirewallAPI.dll,-80200	×
		Rule that controls connections for a Windows experience.	
		○ Custom	
		Custom rule.	
		× 1	
		< Back Next > Ca	incel
1			





3. Select **Program** as rule and click on **Next**.

💣 Windows Defender Firewall with Advanced Security



4. Then go to **This program path:** and click on **Browse**... and f.e. link the *XCT.exe* file under *C: Program Files* (*x86*)*ETASETKTools4.1 XETKConfigurationTool* and confirm with **Next**.

PNew Inbound Rule Wiz	ard X
Program Specify the full program path a	ind executable name of the program that this rule matches.
Steps: Rule Type Program	Does this rule apply to all programs or a specific program?
 Action Profile Name 	All programs Rule applies to all connections on the computer that match other rule properties.
	%ProgramFiles% (x86))ETAS\ETKTools4.1\XETKConfigurationToo1XCT.exe Browse Example: c:\path\program.exe %ProgramFiles%\browser\browser.exe
	< Back Next > Cancel



5. In the new windows select Allow the connection and confirm with Next.

0



6. The rule shall be applied at least for **Public**.





7. Finally an own name for the rule can be forgiven and will be definitely created with the button **Finish**.

🔗 Windows Defender Fi	rewall with Advanced Security								
File Action View Help									
🗢 🌩 🞽 🖬 🗟	?								
Windows Defender Fi	Inbound Rules								
Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program		
Connection Secur	Sception_XCT		All	Yes	Allow	No	%ProgramFiles% (x86)\ETAS\ETKTools4.1\XETKConfigurationTool\XCT.exe		
> 퇹 Monitoring	All_incoming_allowed				Allow	No	Any		
	All_incoming_allowed				Allow	No	Any		
	All_incoming_allowed				Allow	No	Any		

X

Similarly the same steps can be done for **Outbound Rules**.





Create an exception for the protocoll type UDP:

1. Start the Windows Defender Firewall with Advanced Security over the Windows Start icon and the input of the words **Windows Defender**.

Raoyele	All Apps Documents Settings	Photos	More ▼ ···
5/1-	Best match		
UNCA V	Windows Defender Firewall Control panel	\rightarrow	
	Apps		Windows Defender Firewall
	Windows Defender Firewall with Advanced Security	>	Control panel
16	Settings		Ef Open
22	Windows Security	>	
	Core isolation	>	
100	App & browser control	>	
-	Windows Security settings	>	
	Firewall & network protection	>	
	𝒫 windows defender Firewall		H 🛑 H 🖷 📦 🖬 •

2. Right click on Inbound Rules and select New Rule... .



Pindows Defender Firewall with Advanced Security



3. Select **Port** as rule and click on **Next**.

🔗 New Inbound Rule Wizard		×
Rule Type		
Select the type of newall fulle to deate		
Steps: Rule Type	What type of rule would you like to create?	
 Protocol and Ports Action Profile Name 	 Program Rule that controls connections for a program. Port Rule that controls connections for a TCP or UDP port. Predefined: @FirewallAPI.dll, 80200 Rule that controls connections for a Windows experience. Custom Custom Rule. 	

4. Here choose **UDP** as rule type and enter at **Specific local port:** 69, 19000 – 19007. With that the port 69 and the ports from 19000 to 19007 will be released.

Ö

🔗 New Inbound Rule Wizard			\times						
Protocol and Ports									
Specify the protocols and ports to w	hich this rule applies.								
Steps:									
Rule Type	Does this rule apply to TCP or UD	IP?							
Protocol and Ports	О ТСР								
Action	UDP	● UDP							
Profile									
Name	Does this rule apply to all local po	rts or specific local ports?							
	Specific local ports:	69 19000-19007							
	0	Example: 80, 443, 5000-5010							
	<u></u>								
		×							
		< Back Next > Cancel							

05.05.2021 - 8 -© ETAS GmbH 2019. Alle Rechte vorbehalten, auch bzgl. jeder Verfügung, Verwertung, Reproduktion, Bearbeitung, Weitergabe sowie für den Fall von Schutzrechtsanmeldungen.



5. In the new windows select Allow the connection and confirm with Next.

Ö



6. The rule shall be applied at least for **Public**.





7. Finally an own name for the rule can be forgiven and will be definitaley created over the button **Finish**.

🔗 w	💣 Windows Defender Firewall with Advanced Security											
File	File Action View Help											
(🗢 🤿 📶 🔒 🛛 🖬											
e w	indows Defender Fi	Inbound Rules									_	
	Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local A	Remote	Protocol	Local Port
	Connection Secur	Sception_UDP_Ports_XCT				Allow	No	Any	Any	Any	UDP	69, 19000-19007
> 🛒	Monitoring	All_incoming_allowed				Allow	No	Any	Any	Any	Any	Any
	, in the second s	All incoming allowed				Allow	No	Anv	Any	Anv	Any	Anv

ð,

Similarly the same steps can be done for **Outbound Rules**. Then for the ports 1024 to 65535.

i Additional information:

It can be also added in the firewall as exception the programs INCA.exe, XCT.exe and FWUT.exe (HSP Update Tool).



Please feel free to contact our Support Center, if you have further questions. Here you can find all information: <u>http://www.etas.com/en/hotlines.php?langS=true&</u>

This information (here referred to as "FAQ") is provided without any (express or implied) warranty, guarantee or commitment regarding completeness or accuracy. Except in cases of willful damage, ETAS shall not be liable for losses and damages which may occur or result from the use of this information (including indirect, special or consequential damages).