



## Warum bekomme ich in INCA und im XCT Tool die TFTP Fehlermeldung oder wieso sehe ich im HSP Update Tool nicht die Firmware Version meines (F/X)ETK's?

Ich möchte meine Firmware meines (F/X)ETK's im HSP Update Tool aktualisieren, in INCA mein (F/X)ETK initialisieren oder im XCT Tool die Konfiguration meines (F/X)ETK's herunterladen. Dies ist leider aufgrund folgender Fehlermeldungen nicht möglich:

Fehler - H	Ier - 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)		
8	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 werder Erneuter Versuch TFTP-Datei zu übertragen (XEtkProtocol_Main.log) (Seriennummer des Gerätes: 2394, Aliasnamen des Gerätes: 'Aliasname nicht gesetzt') (a1b_XETK.log)	1	
	ОК		

ISP Update Tool - XETK (SN 100119195)	- 28- 1 8 - 18 - 18 - 18 - 18 - 18 - 18		2-3		$\times$
<u>File Functions View Tools Drivers Window H</u>	elp				
🔍 🍣 🔊 HSP V11.8.1 🔹 🔩 🕈	🛯 🕲 🖬 🖬 🖥 🕼 🖒 🖄	r 21 _			
Hardware	P Details XETK (S	5N 100119195)			1 Þ 🗙 🛃
Ethernet Interface. VETK (SN 100119195)	Component -	Installed Version Version in Serv State Description			roperties
	Output				Ψ×
	*Starting search for h SPS Server XETK Sys *Search for hardware	hardware stems : Hardware found: XETK (SN 100119195) finished			
			1	LISD V	11.9.1

Applicat	ion Log 👻
Time	Test
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 (XEtkProtocol_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





Eine Verbindung zum (F/X)ETK wird immer vom PC aufgebaut. Der (F/X)ETK sendet nur Daten, wenn eine Verbindung schon aufgebaut wurde. Die XCP Verbindungen verwenden den Dienst TCP oder UDP und nutzen dafür immer den Port 1802. Ändert sich nun die Konfiguration oder die Firmware soll ausgelesen werden, so wird das TFTP Protokoll verwendet.

Um das TFTP Protokoll verwenden zu können, sind die Ports 69 und 19000 bis 19007 für das TFTP Protokoll auf UDP Basis in der Firewall freizuschalten.

Der Port 69 des (F/X)ETK dient zum erstmaligen Kommunikationsaufbau. Für alle Antworten verwendet der (F/X)ETK die Ports im Bereich zwischen 19000 und 19007.

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	TCP, UDP	102465535	1802	MC: INCA uses TCP. 3 <sup>rd</sup> 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

Der einfachste Weg ist die Firewall komplett zu deaktivieren. Ist dies nicht möglich, müssen die verwendeten Ports oder die Programme eine Ausnahme in den Firewalleinstellungen erhalten.

In *Windows 10* wird dies über die *Windows Defender Firewall* wie folgt durchgeführt. Für andere Programme bitte Ihre eigene IT einbeziehen.





## Ausnahme für ein Programm:

1. Starten der *Windows Defender Firewall* mit erweiterter Sicherheit über Windows Startlogo und Eingabe des Wortes **Windows Defender**.



2. Rechtsklick auf Eingehende Regeln und im Kontextmenü Neue Regel... wählen.





- 3. Programm als Regeltyp selektieren und auf Weiter klicken.

矕 Windows Defender Fire	wall mit erweiterter Sicher	heit	
Datei Aktion Ansicht	?		
🗢 🄿 🗖 🔂 🖬	? 🗊		
Windows Defender Fire	wall mit Eingehende Re	geln	
Ausgehende Reg	Neue Regel		Gruppe
🌆 Verbindungssiche > 🌉 Überwachung	Nach Profil filtern Nach Status filtern Nach Gruppe filtern	d	
	Aktualisieren Liste exportieren	ework v. 18.2.0.54383	
	Hilfe	ework v. 18.2.0.54404	

4. Unter **Dieser Programmpfad:** auf **Dursuchen...** klicken und z.B. die XCT.exe Datei unter *C:* |*Program Files* (*x86*)|*ETAS*|*ETKTools4.1*|*XETKConfigurationTool* verlinken und mit **Weiter** bestätigen.

💣 Assistent für neue eingehe	ende Regel	×
Programm		
Geben Sie den vollständigen Prog	rammpfad und den Namen der ausführbaren Datei des Programms an, dem diese Regel entspricht.	
Schritte:		
Regeltyp	Betrifft diese Regel alle oder nur ein bestimmtes Programm?	
Programm		
Aktion	○ Alle Programme	
Profil	Die Regel wird auf alle Computerverbindungen angewendet die mit anderen Regeleigenschaften übereinstimmen.	
Name	Dieser Programmpfad:	
	% Program Files % (x86)\ETAS\ETKTools4.1\XETKConfiguration Tool\XC1 Durchsuchen	
	Beispiel: c:\path\program.exe	
	%ProgramFiles%\browser\browser.exe	
	< Zurück Weiter > Abbrecher	1



5. Im neuen Fenster die Auswahl auf Verbindung zulassen belassen und mit Weiter bestätigen.

0



6. Die Regel sollte mindestens für den Bereich Öffentlich gesetzt bleiben.





7. Abschließend vergeben Sie der Regel noch einen eigenen Namen und erstellen diese endgültig über den Button **Fertig stellen**.

ð,

 $\swarrow$ 

💣 Windows Defender Firewall mit	erweiterter Sicherheit						
Datei Aktion Ansicht ?							
🗢 🄿 🙋 🖬 🗟 🖬							
Windows Defender Firewall mit	Eingehende Regeln						
Eingehende Regeln	Name	Gruppe	Profil	Aktiviert	Aktion	Außer Kraft setzen	Programm
	ssicherheitsrege 🖉 Ausnahme XCT Alle Ja Zulassen Nein	Nein	%ProgramFiles% (x86)\ETAS\ETKTools4.1\XETKConfigurationTool\XCT.exe				
> 🖳 Überwachung	All_incoming_allowed		Domä	Nein	Zulassen	Nein	Beliebig
_	All_incoming_allowed		Domä	Nein	Zulassen	Nein	Beliebig
	All_incoming_allowed		Domä	Nein	Zulassen	Nein	Beliebig

Zum Schluss können Sie das gleiche noch für die **Ausgehende Regeln** erstellen.





## Ausnahme für den Protokolltyp UDP:

1. Starten der *Windows Defender Firewall* mit erweiterter Sicherheit über das Window Startlogo und Eingabe des Wortes **Windows Defender**.



2. Rechtsklick auf Eingehende Regeln und im Kontextmenü Neue Regel... wählen

🔗 Windows Defender Firewall mit erweiterter Sicherheit									
Datei Aktion Ansicht ?									
🗢 🄿 🖄 📰 🗟 🛛 😰									
Windows Defender Firewa	ll mit Eingehende Reg	Jeln							
Ausgehende Reg	Neue Regel		Gruppe						
Verbindungssiche Uberwachung	Nach Profil filtern	> d							
, and obermaching	Nach Status filtern	> d							
	Nach Gruppe filtern	>							
	Ansicht	>							
	Aktualisieren								
	Liste exportieren	ework v. 18.2.0.54	383						
	Hilfe	ework v. 18.2.0.54	305 404						
	Contraction of the second seco								



3. Port als Regeltyp selektieren und auf Weiter klicken.



4. Hier wählen Sie **UDP** als Porttyp und geben bei **Bestimmte lokale Ports:** 69, 19000-19007 ein. Damit werden der Port 69 und die Ports von 19000 bis 19007 freigegeben.

D

🔗 Assistent für neue eingel	iende Regel	$\times$
Protokolle und Ports		
Geben Sie die Protokolle und Po	rts an, für die diese Regel gilt.	
Schritte:		
Regeltyp	Betrifft diese Regel TCP oder UDP?	
Protokolle und Ports	О ТСР	
Aktion	● UDP	
Profil		
Name	Gilt diese Regel für alle lokalen Ports oder für bestimmte lokale Ports?	
	○ Alle lokalen Ports	
	Bestimmte lokale Ports: 69, 19000-19007	
	Beispiel: 80, 443, 5000-5010	
	X	
	< Zurück Weiter > Abbrechen	



5. Im neuen Fenster die Auswahl auf Verbindung zulassen lassen und mit Weiter bestätigen.

Ö



6. Die Regel sollte mindestens für den Bereich Öffentlich gesetzt bleiben.





7. Abschließend vergeben Sie der Regel noch einen eigenen Namen und erstellen diese endgültig über den Button **Fertig stellen**.

Windows Defender Firewall mit		Eingehende Regeln								_		
	Eingehende Regeln	Name	Profil	Aktiviert	Aktion	Außer	Programm	Lokale Adresse	Remoteadresse	Protokoll	Lokaler Port	
	Verbindungssicherheitsrege	Ausnahme_UDP_Ports_XCT	Alle	Ja	Zulassen	Nein	Beliebig	Beliebig	Beliebig	UDP	69, 19000-19007	
	> 🖳 Überwachung	All_incoming_allowed	Domä	Nein	Zulassen	Nein	Beliebig	Beliebig	Beliebig	Alle	Beliebig	
	· · · · · · · · · · · · · · · · · · ·	All_incoming_allowed	Domä	Nein	Zulassen	Nein	Beliebig	Beliebig	Beliebig	Alle	Beliebig	
		All_incoming_allowed	Domä	Nein	Zulassen	Nein	Beliebig	Beliebig	Beliebig	Alle	Beliebig	

Zum Schluss können Sie das gleiche noch für **Ausgehende Regeln** erstellen. Hier für die Ports 1024 bis 65535.

## *i* Weitere Informationen:

Es können ebenso die Programme INCA.exe, XCT.exe und FWUT.exe (HSP Update Tool) in der Firewall als Ausnahme hinzugefügt werden.



Für weitere Fragen stehen wir Ihnen gern zur Verfügung. Unsere Hotline-Nummer finden Sie unter <u>http://www.etas.com/de/hotlines.php</u>

Die hier dargestellten Informationen (hier auch "FAQ" genannt) werden ohne jegliche (ausdrückliche oder konkludente) Gewährleistung, Garantie bzw. Zusage über Vollständig- oder Richtigkeit zur Verfügung gestellt. Außer im Falle vorsätzlicher Schädigung, haftet ETAS nicht für Schäden, die durch oder in Folge der Benutzung dieser Informationen (einschließlich indirekte, mittelbare oder sonstige Folgeschäden) aufgetreten können bzw. entstanden sind.