Horizon

X300 4G Dongle Support

Commissioning
Edition notice

Technical specifications and availability subject to change without notice. This document may not be reproduced, disseminated to third parties or processed and its contents may not be used or disclosed without express permission. Non-compliance shall result in compensation for damages. All rights, including those resulting from a successful patent application and registration of a utility model or design patent, are reserved.

Edition: 2020-07-03
Document ID: A6V12059208_en--a

© Siemens Switzerland Ltd, 2020
Cybersecurity disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens’ portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html.

Siemens’ portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under https://www.siemens.com/cert/en/cert-security-advisories.htm.
Table of Contents

Edition notice ........................................................................................................... 000

1 X300 4G Dongle Support Commissioning Guide .............................................. 5

1.1 Preparing dongle for installation ................................................................. 5

1.2 Installing dongle ......................................................................................... 6

1.3 Configuring dongle ...................................................................................... 6

1.3.1 Huawei E3372/E3372h ....................................................................... 7

1.3.2 Alcatel IK40V-2AALDE1 .................................................................... 7

1.3.3 Verizon USB730L/MC730 USA ............................................................ 7
1 X300 4G Dongle Support Commissioning Guide

This guide describes the workflow for connecting 4G USB dongles to a PXG3.300. Please follow the steps properly to avoid cyber security risks.

Supported devices
- Huawei E3372/E3372h
- Alcatel IK40V-2AALDE1
- Verizon USB730L/MC730 (USA)

1.1 Preparing dongle for installation

1. Connect 4G dongle to a local PC.

   The Dongle will be displayed as a drive when connected.

   1. Connect 4G dongle to a local PC.

   2. Open web UI of the dongle if it doesn't open automatically.

   - Current signal strength is displayed.

   To disable PIN protection of the SIM card, enter initial PIN and then select change PIN. Leave new PIN empty and confirm.

   - Verify APN of your provider.
   - Check the internet for firmware updates.

   Having the latest updates is mandatory! Otherwise cyber security of your connection can not be granted. It is recommended to update the firmware manually, not automatically.
- Enable **4G connectivity only** (see chapter Configuring dongle [➙ 6] for details).
- Check all other project specific settings such as data roaming and auto disconnect interval. It is recommended to set auto disconnect interval to maximum time limit.

⚠️ Dongle is ready for installing.

### 1.2 Installing dongle

LAN cable is connected to X1P1 port on X300.

The USB dongle can be plugged into any USB port. It is recommended to use port X60. A connected WAN cable can be plugged in. The dongle has higher priority and the communication channel will be changed automatically as soon as a connection is established. When the dongle is removed, WAN port will be activated again automatically.

⚠️ Connect dongle to USB port X60 on X300.

⚠️ The **WWAN0** interface will be created if an internet connection exists. If 4G connection fails and WAN port X2P1 is connected to a wired network, the system will try to connect via WAN0.

⚠️ A proper connection state is indicated as following:
- Connection LED on X300 is flashing orange.
- WWAN0 port is displayed in local webserver HEdge UI of the X300 in the list under **Network > Route**.
- Cloud Connectivity displays the state **Connected** in HEdge UI.

### 1.3 Configuring dongle

Due to cyber security reasons it is recommended to set network mode to **4G only**.
1.3.1 Huawei E3372/E3372h

1. In **Networks** tab, select **Global** as Preferred Network Technology.

2. In **SIM** tab, select **Turn off PIN Lock**.

1.3.2 Alcatel IK40V-2AALDE1

1.3.3 Verizon USB730L/MC730 USA

1. In **Networks** tab, select **Global** as Preferred Network Technology.

2. In **SIM** tab, select **Turn off PIN Lock**.
3. In Software Update tab, click Check for Update.