



INSTALLATION INSTRUCTIONS

Model CGAP2

Adapter Plate to mount Model Connect X300 Cloud Gateway

DESCRIPTION

The Model CGAP2 is an adapter Plate, P/N S54811-B102-A1, for mounting the Connect X300 Gateway, P/N S55842-Z121-A100. This adapter plate is mounted inside the PAB-ENCL enclosure, P/N S54339-A8-A1 (Black) and P/N S54339-A9-A1 (Red).

Size: 7.52W X 5.73H

Material: 14 Ga, Steel, Zinc plated

Carton Contents:

1. CGAP2 Adapter plate
2. Installation instructions, CGAP2 and Connect X300
3. Hex Locknuts #10-32, q'ty = 2
4. Power Cable Assembly for Gateway
5. M4X10mm long screws, q'ty = 4

INSTALLATION INSTRUCTIONS

1. Using the hardware provided, mount the Connect X300 Gateway onto the CGAP2 adapter plate as shown on Figure 1.
2. Place the adapter assembly into the PAB-ENCL enclosure, as shown in Figure 2, and secure it using the two locknuts provided.
3. Follow the installation instructions provided, Document ID A6V11649121, for wiring the Connect X300 Gateway.
4. The provided power cable is used to power the Connect X300 from Siemens power supply model FP2011-U1.



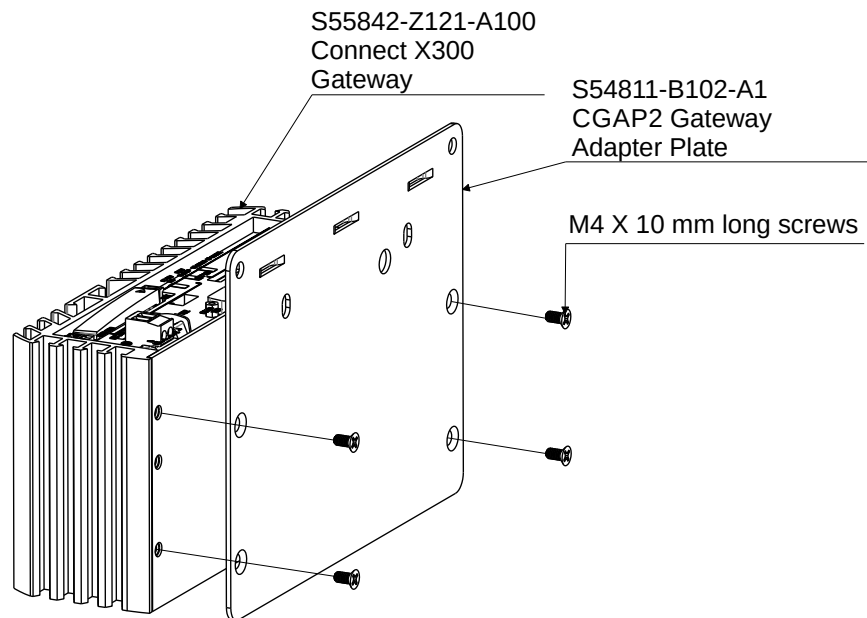


Figure 1
Mounting the Gateway onto the Adapter Plate

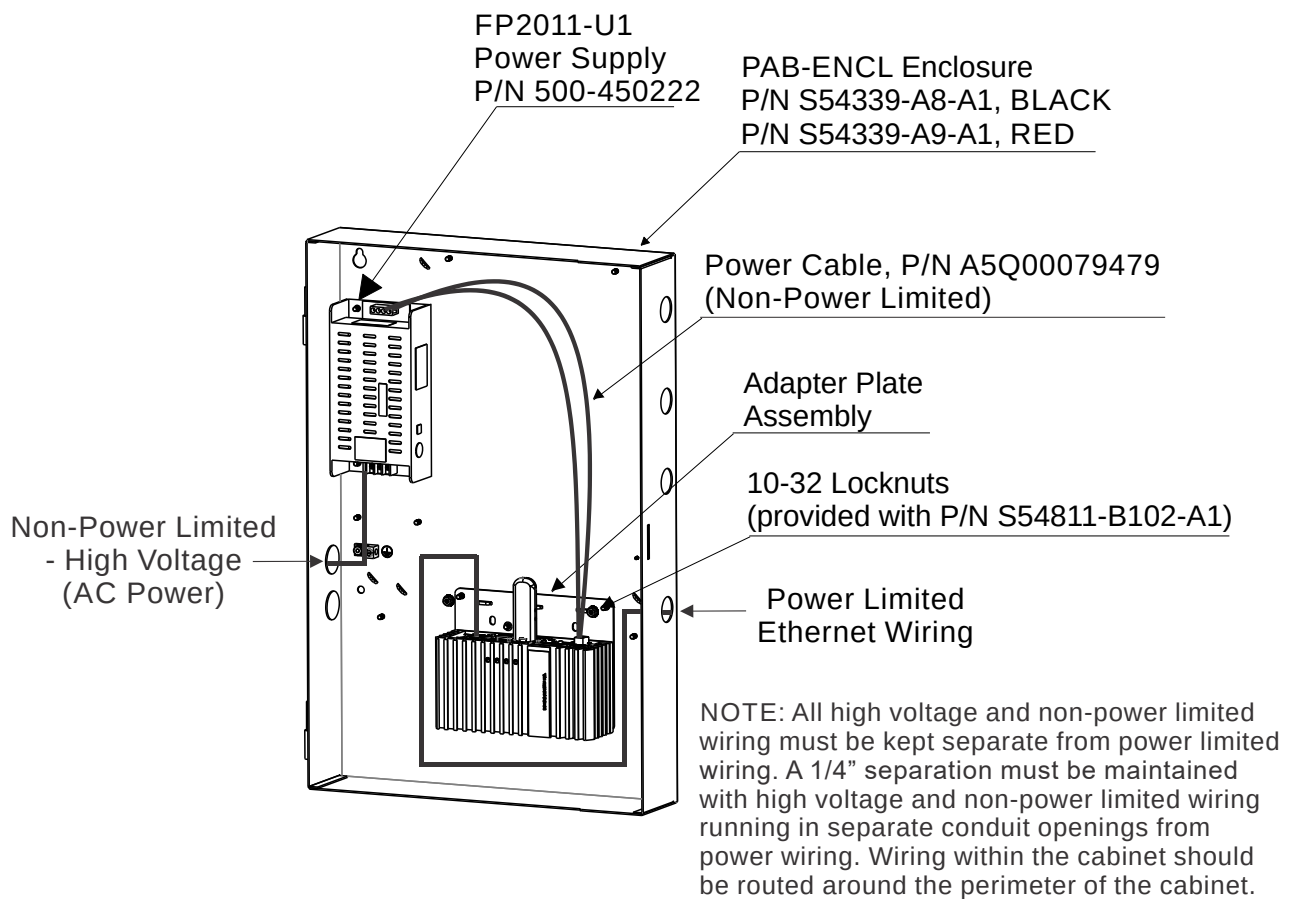


Figure 2
Mounting the Adapter Plate Assembly into the Enclosure

Cyber security 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/topicareas/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>.



