Cloud Gateway security & networking brief

Storage
The Cloud Gateway's files are saved on the attached SD-card. The SD-card is not encrypted. We recommend keeping the device physically in a secure location.

Notable:
- If the Cloud Gateway is configured to use a Wi-Fi connection, the Wi-Fi credentials are saved on the SD-card unencrypted.
- An access token that allows the Cloud Gateway to communicate with the target Casambi network is saved on the SD-card unencrypted. If necessary, token can be invalidated by changing the Casambi network admin password.
- Wi-Fi credentials and the access token are removed from the SD-card when the Cloud Gateway is unpaired from the Casambi network while connected to the internet.

Internet connection
Like all IoT devices, we recommend that the Cloud Gateway be added to a network separate from business-critical devices.

The Cloud Gateway initiates almost all network traffic. Only incoming traffic is NTP responses (UDP traffic) which can be linked to outgoing requests by modern firewalls. Proxying is not supported. Firewall must allow the following traffic.

NTP Debian timeservers (UDP):

- *.debian.pool.ntp.org (outgoing port 123)
- Incoming can be any pool server, any port. A modern firewall should handle linking

HTTPS traffic from port 443 to the following URLs:

- api.casambi.com
- bridge.casambi.com
- iot-gateway-prod-westeurope.azure-devices.net
- hosted.mender.io
- *.hosted.mender.io
- hosted-mender-artifacts.s3.amazonaws.com
- s3.amazonaws.com/hosted-mender-artifacts
- c271964d41749feb10da762816c952ee.r2.cloudflarestorage.com

The Cloud Gateway utilizes DHCP (Dynamic Host Configuration Protocol) for automated IP address assignment. The device requests network configuration parameters, including an IP address, subnet mask, default gateway, and DNS server addresses, from the DHCP server within the network. Currently manual configuration of a static IP address for the Cloud Gateway is not possible.