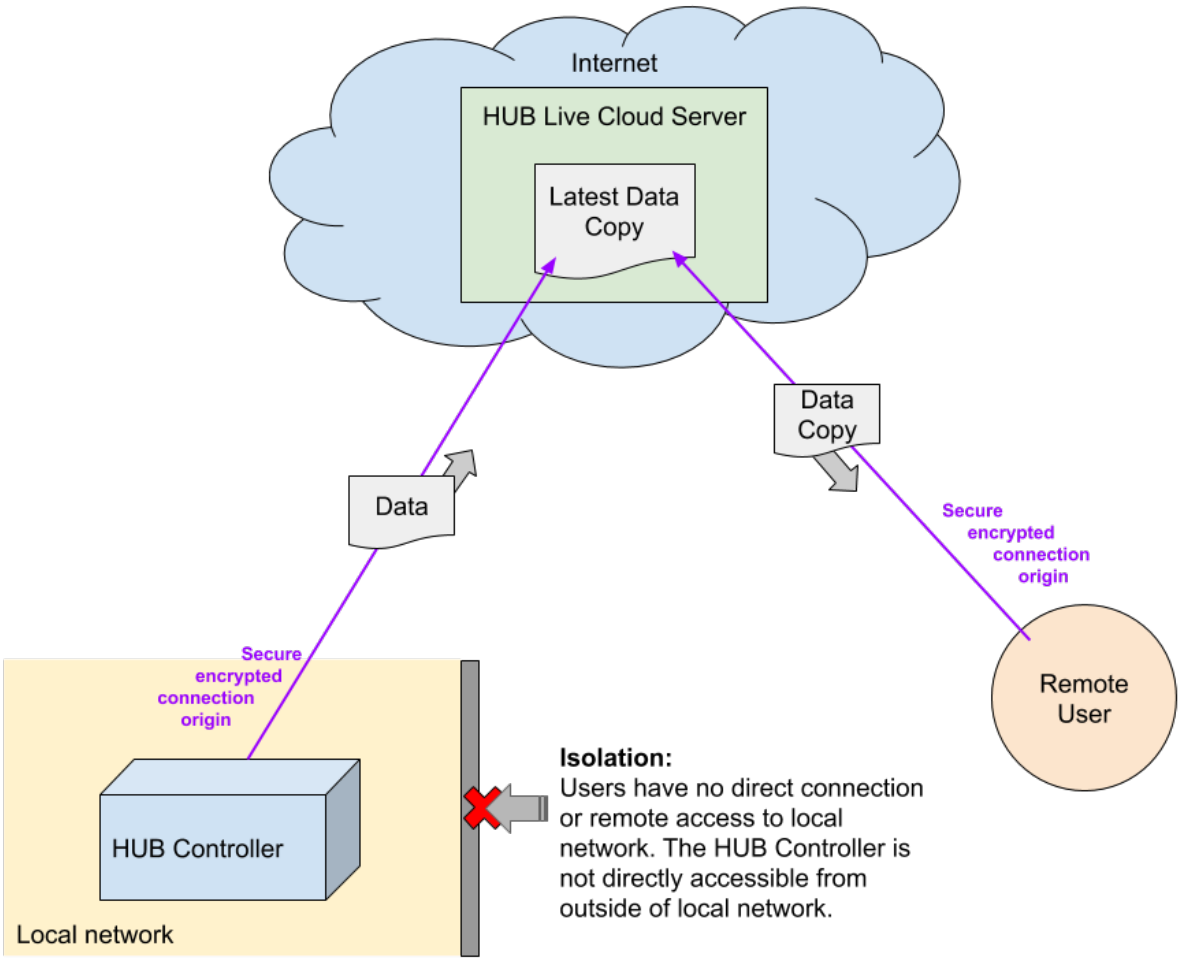
CH-Cloud
Product Data Sheet

Secure Data Transfer



Remote control, not remote access

The cloud architecture is designed with industry best practices, to ensure both a secure cloud connection and isolation of the controller from any outside connection.

The HUB controllers establish a secure and encrypted connection to the HUB Live cloud server. This means the connection originates from the controller on the local network. The HUB controller is not accessible from outside of the local network.

In general, this is how a device can connect to the Internet securely, but is isolated from incoming connections (i.e. a computer on a local network accessing the Internet, but is inaccessible from outside connections).

Connection details

The HUB Live cloud connection requires access to the internet using standard ports, as detailed:

HUB Live cloud server connection:

- The HUB Live URL is: **https://hubautomation.live**
- The HUB Live IP address is: **52.63.147.140**
- The port used is: **443** (HTTPS)

Time clock synchronisation can be achieved in two ways - using standard NTP servers, or failing that, with a HTTP header timestamp - as detailed below:

- NTP servers: ***.pool.ntp.org**
- NTP port: **123** (NTP)
- HTTP head server: **google.com**
- HTTP head port: **80** (HTTP)

Once the HUB controller has established a secure connection the cloud server, it sends packets of data at interval - this data includes things like aircon status, temperatures, set points, etc. The cloud server keeps a copy of the latest data sent, keeping an up-to-date state of the controller.

When a user connects to the cloud server to view their system remotely - the cloud server presents a copy of the latest data packet from this controller.

In this way the user does not have a direct connection to the controller. Instead, they see a copy of the controller's data securely provided by the cloud server, not the controller, maintaining isolation.

Any commands that the uses issues are also stored on the server, and not sent to the controller directly. At intervals, the controller will establish it's secure connection to the cloud server, and retrieve any command. Again, in this way the controller is isolated, and no direct remote access to the local network is used.

Fault Harvesting and Email Notifications

The ClimateHUB harvests faults from the air conditioner or third party building management systems, interacts with the AutomationHUB for alarms and sends notifications. The email server is ‘mail.hubautomation.com.au' and the port is 587.

Dynamic Host Configuration, Static Lease, Fixed IP

A typical ClimateHub installation can utilise DHCP, if an AutomationHUB (Modbus TCP or BACnet TCP) is used or for any other reason the network administrator requires that each ClimateHub is assigned an IP address permanently we prefer that a static lease is set at the router. A Static IP can be set for each ClimateHub if required.

AutomationHub

The AutomationHub communicates with other building management products using Modbus TCP or BACnet TCP. Unlike the ClimateHub, LightingHub, EnergyHub and the IAQT-Hub the AutomationHub does not have an associated cloud service. The AutomationHub is used for running custom actions or scenes for specific sites.

Key considerations:

- AutomationHub requires a static IP address
- Communicates with other Hub products on port 502
- Notifications email server is ‘mail.hubautomation.com.au'
- For remote support via VPN, access to 13.55.17.15 port 443 is needed

Time clock synchronisation can be achieved in two ways - using standard NTP servers, or failing that, with a HTTP header timestamp - as detailed below:

- NTP servers: *.pool.ntp.org
- NTP port: 123 (NTP)
- HTTP head server: google.com
- HTTP head port: 80 (HTTP)