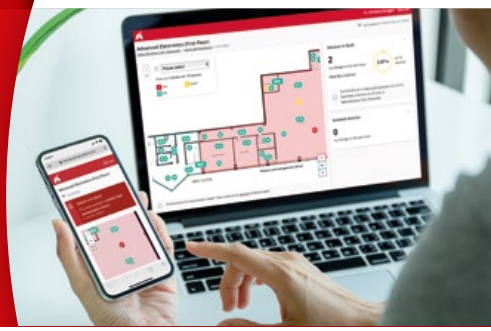
Information for IT Managers



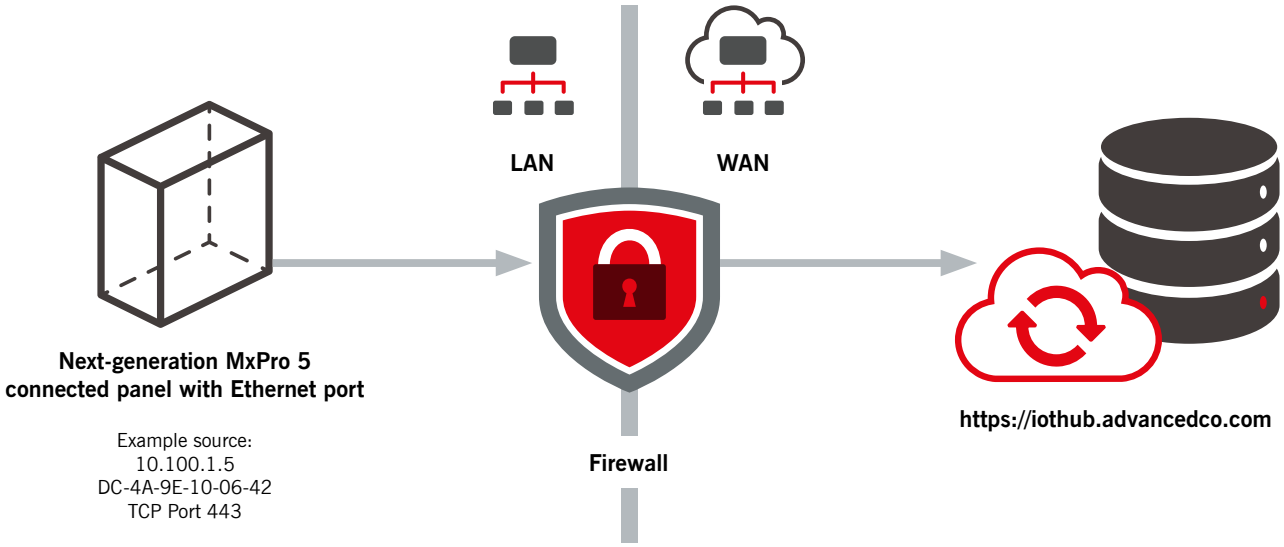
This document is to support IT managers and network administrators so they can integrate AdvancedLive within their existing framework of security policies and procedures.

What is AdvancedLive?

AdvancedLive is cloud-based software for your facilities teams and managers, so they can remotely manage the fire alarm system. It allows them to deal with any fire alarm incidents quickly and efficiently, and easily rectify any issues to ensure that the fire system is in full working order.

The fire system from your fire panel is connected to the cloud where users can access the AdvancedLive software via a web browser using any internet-enabled device such as a laptop, tablet or mobile phone.

How does the fire system communicate with AdvancedLive?



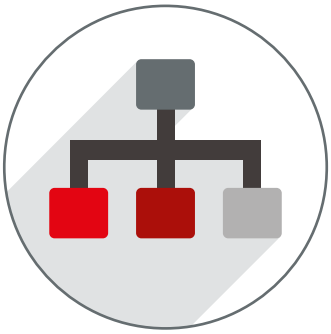
The next-generation MxPro 5:

- has a single RJ45 Ethernet port
- uses HTTPS over TCP port 443 to connect securely to the AdvancedCloud service using a 2048-bit encryption key
- connects outbound only to the AdvancedCloud service, no inbound connection is required.

Tel: +44 (0)345 894 7000 **Email:** enquiries@advancedco.com **Web:** www.advancedco.com

Information for IT Managers

Can a VLAN be used?



The connected Advanced fire panel can be partitioned from your main network or any other network devices or infrastructure using a VLAN.

The connected panel requires nothing more than the ability to connect to the internet over port 443 using an HTTPS request.

Can a Wi-Fi connection be used?

If the connected panel is not located close to a suitable Ethernet connection point, then a Wi-Fi bridge can be used to wirelessly connect the panel to a LAN or VLAN and then on to the internet.

Can a 4G connection be used?

The connected panel can be connected to a 4G router, to provide internet access.

The panel does not require any inbound connection paths, so a fixed public IP SIM card is NOT required.

Any industrial 4G router can be used with a SIM card from any local provider.

How is the connected panel's IP address managed?

The default factory setting is for the panel to request an IP address from a DHCP service when it is connected to an Ethernet connection.

If an IP reservation is preferred, then the MAC address for the device can be obtained by following the directions in: **Where is the connected panel's MAC address located?**

Alternatively, a static IP address can be configured within the connected panel using the built-in configuration tool by following the steps in: **How can the connected panel be configured with a static IP address?**

Can the resilience of AdvancedLive connection be boosted?

A backup product is available for purchase which includes battery, power supply and optional modem to provide redundancy. For further details, please speak to an Advanced sales representative or contact **customerservices@advancedco.com**

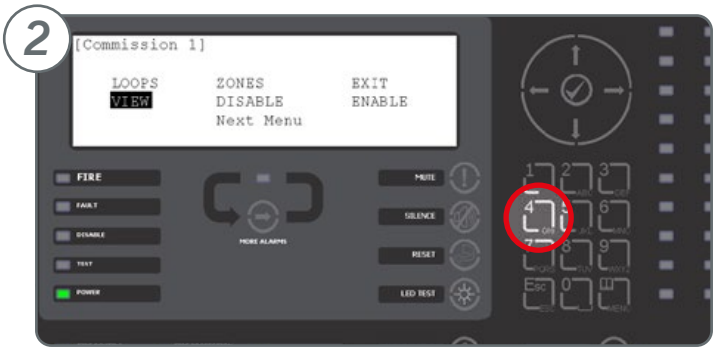
Information for IT Managers

Where is the connected panel's MAC address located?

The panel has a unique MAC address which can be located in the built-in configuration tool.

On the connected panel press the **MENU** button, located on bottom/right of the numeric keypad.

Press **[4]** to select **VIEW**.



From the **VIEW** menu press **[6]** to select the **CONNECTION** option.

Within the **CLOUDVIEW** menu press **[✔]** to select the **IPCONFIG** option.

The **IPCONFIG** menu shows the panel's MAC address, and the current dynamic IP address or static configured IP address.

Information for IT Managers

How can the connected panel be configured with a static IP address?

The panel can be configured with a static IP address, and the preferred DNS server IP addresses can be configured via the built-in configuration tool. This is a system configuration function, which requires LEVEL 3 access, so should be carried out with the installation engineer.

Press the **MENU** button, located on the bottom right of the numeric keypad.

1

Press **[7]** to select the **NEXT MENU** option.

2

Press **[7]** to select the **NEXT MENU** option again.

3

Press **[4]** to select the **CLOUD** option.

4

Press **[3]** to select the **CONFIGTOOL** option

5

Press **[3]** to select the **STATIC-IP** option.

6

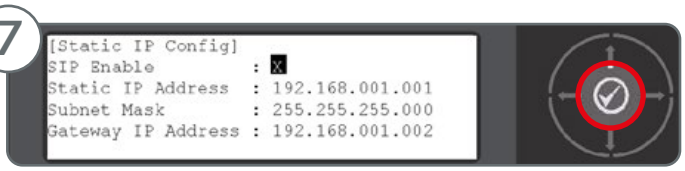
Tel: +44 (0)345 894 7000 **Email:** enquiries@advancedco.com **Web:** www.advancedco.com

Advanced

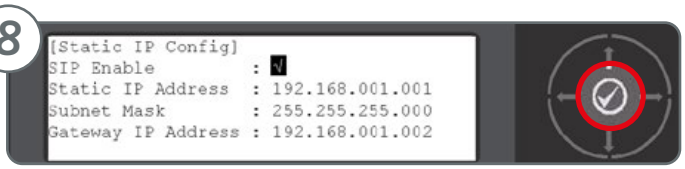
Information for IT Managers

Press the **tick button** within the arrow keypad to change the SIP Enable option from **[NO]** to **[YES].**

7

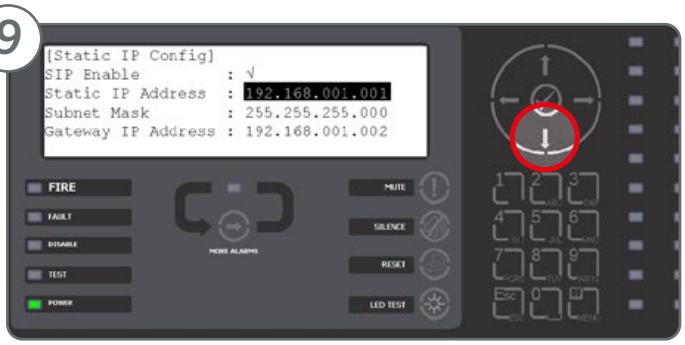


8



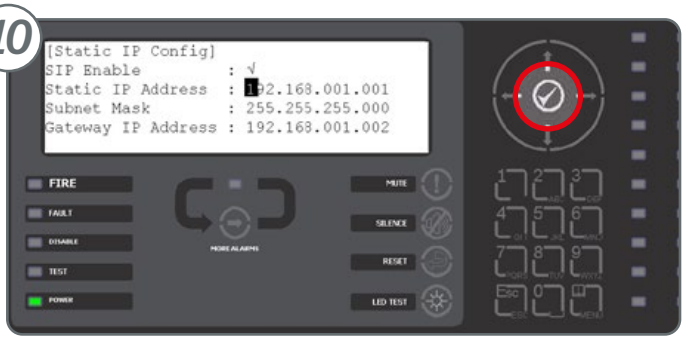
Use the **arrow keys** to scroll down to the **Static IP Address** option.

9



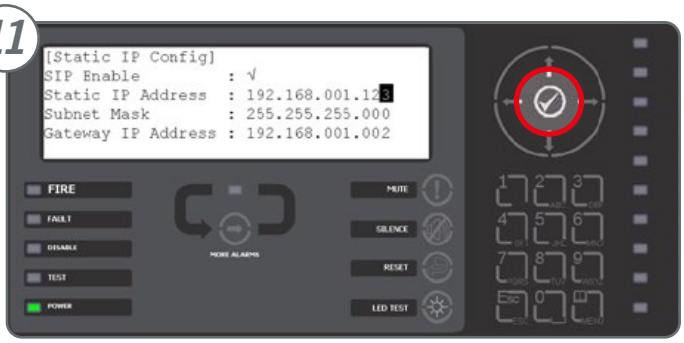
Press the **tick button** to display an **input cursor**.

10



Use the **numeric keypad** to enter your IP address. In this example the IP address 192.168.001.123 is configured.

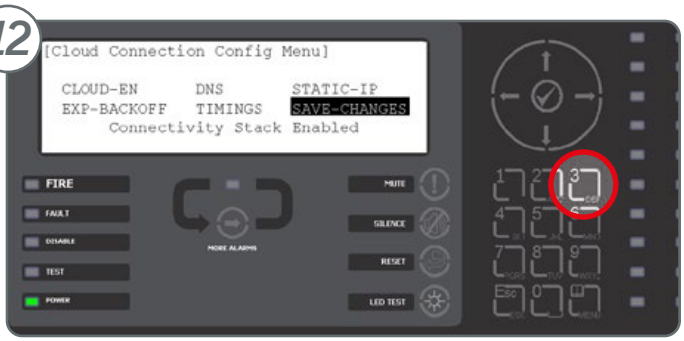
11



Press the **tick button** to accept the static IP address.

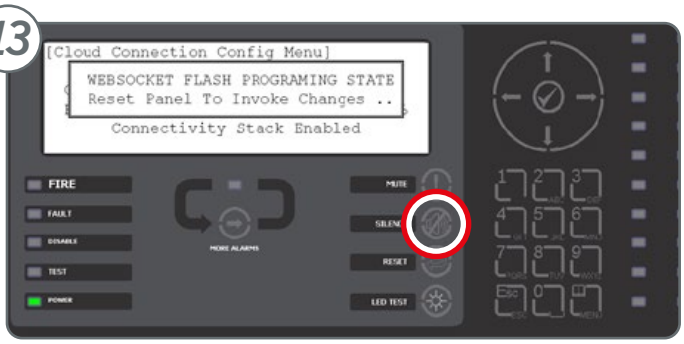
Once the IP address details have been entered, press the ESC button bottom/left of the numeric keypad, and then press **[6]** to select **SAVE CHANGES**.

12



A confirmation message will be displayed.

13



Press **RESET** button on the panel, Then wait for panel to reset and take you back to the main screen. (Repeat steps 1-4).

Information for IT Managers

At the Cloud Menu press [1] to select **CONNECT** (This seems to be automatic (As seen in picture below) but if not select connect)

14

Once connected, the screen will display **STATUS: CONNECTED**.

15

What bandwidth will the connected panel typically use?

The fire system generates very little data under normal working conditions. Data is sent to the cloud, when the status of a device on the fire system changes, for example when a fault registers from a device such as dirty, missing, bad data, or when a device detects smoke, flame or heat.

The typical data usage is in the range of 5-20Mb per day.

How is user sign-in managed?

AdvancedLive provides users with a range of sign-in options. Integration with single sign-on providers is in place for:

- Microsoft
- Google
- LinkedIn

Please speak to our team for information about integrating with other single sign-on providers.

There is also a passwordless sign-in option that delegates the authentication process to the user's corporate email client. The user can enter the email address that was used when they received the invitation to start using AdvancedLive. AdvancedLive sends a time-sensitive, single-use link to the email address. The user clicks on the link in the email which will sign them directly into AdvancedLive.

Tel: +44 (0)345 894 7000 **Email:** enquiries@advancedco.com **Web:** www.advancedco.com

Advanced

Information for IT Managers

Where is the information stored?

AdvancedLive is operated from within the Microsoft Azure cloud. All data is stored in Azure SQL databases.

How is the information store protected?

Communication between the AdvancedLive software and the Azure SQL Database is conducted over a secure TLS connection. All SQL connections since .NET7 are encrypted by default, whereas previously the TLS encryption was disabled by default.

Azure SQL Databases are encrypted at rest.

Connection to the Azure SQL Database is controlled by the Azure server firewall, and only AdvancedLive software instances are permitted to access the Azure SQL Server instance.

Which set of employees have access to our data and how is this controlled?

Access to the entire Azure environment is tightly controlled.

Firstly, no backups or copies of the data are taken from the live Azure environment. Replication, backup, and recovery are handled within the Azure instance, so that no data is transported or exfiltrated from the environment.

Access to the Azure SQL server environment is restricted to individuals within the Advanced digital services team.

Do third parties have access to AdvancedLive data and if so, how is this controlled?

No third parties have access to any data held within AdvancedLive.

How are updates tested and then rolled out to the live system?

All updates to AdvancedLive are run through a comprehensive set of automated tests, and through several stages of deployment before being released for customers to use in the live environment.

Is any encryption applied to the data, both at rest and during transit to end users and between information stores?

Encryption is in place at all data transit endpoints, and at rest.

The Advanced connected panel installed on the fire system connects over a TLS-encrypted channel on port 443 using HTTPS.

All communication between users and the AdvancedLive platform occurs over HTTPS communication between the user's browser on their desktop, laptop, tablet or mobile phone.

AdvancedLive uses the Azure SQL Database as a data store, which employs encryption at rest. Also, communication between AdvancedLive and the Azure SQL database is encrypted using a TLS certificate.

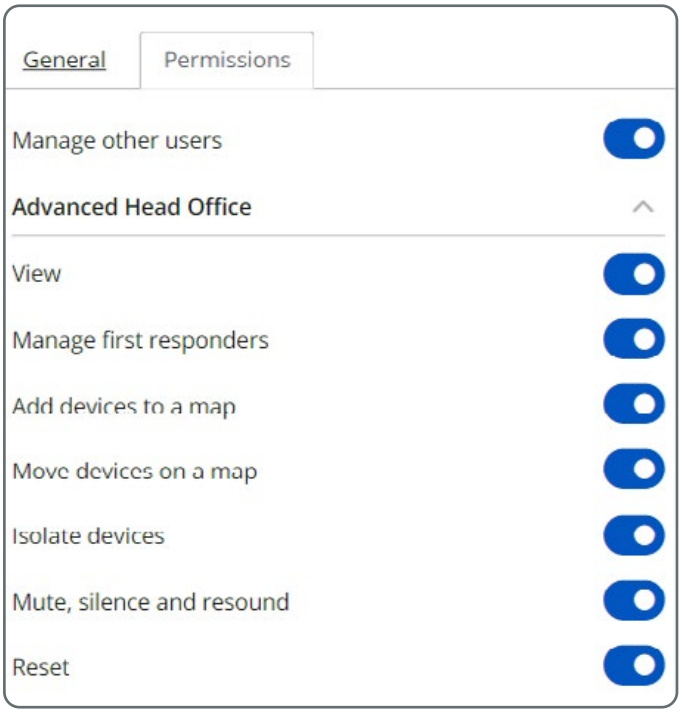
Information for IT Managers

What controls are in place to separate Advanced's data from other customers?

All customer data is logically partitioned. Data access is managed via software controls, and user authorisation rules.

All AdvancedLive API endpoints enforce strict authentication policies. Each policy validates that the current user is authenticated and has sufficient permissions to perform the data request or action that the endpoint governs.

Each user is invited to AdvancedLive by email. By default, an invited user has no permissions, so is unable to view any sites within AdvancedLive, or any management function.



The user can then be granted a number of permissions including managing other users for each site within an organisation. Therefore, it is possible to have users within an organisation who are only able to monitor a single site.

At those sites, the users can be granted permissions to perform functions such as:

- Manage the first responders
- Add devices to maps
- Move devices on a map
- Isolate devices
- Mute, silence or resound the site via panels.

Tel: +44 (0)345 894 7000 **Email:** enquiries@advancedco.com **Web:** www.advancedco.com

Advanced

Information for IT Managers

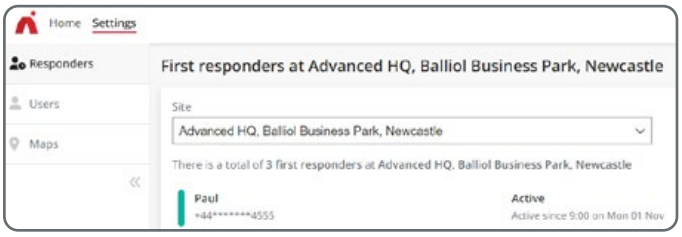
What personal identifiable information is stored within AdvancedLive?

AdvancedLive has been built to capture only the essential personal information required to operate the AdvancedLive service.

First responders

First responders are a set of AdvancedLive users, typically the fire marshals and facilities team members, who respond to a fire alarm to investigate and confirm and then evacuate the building. The first responders are notified about a potential fire via an SMS message. Therefore, AdvancedLive requires the name and mobile phone number of the first responders.

Access to the management of first responders is controlled via user permissions, and the manager is unable to see the first responder's mobile phone number, as this is masked out in the management view.



User information

The only user information stored in AdvancedLive is the name and unique identifier, which in this case is their email address used to receive the AdvancedLive invitation.

User information in audit trails

A powerful feature of AdvancedLive is the comprehensive audit trail which gives users detailed information on fire system events, and actions taken. To ensure that the audit trail is clear, AdvancedLive shows the name of the user who performed the action. To ensure data is secure, a masked version of the mobile telephone number is shown if used.

For example, when a fire incident starts and first responders are notified about the incident, the incident event log shows details of the first responders who have been notified, and which first responders have viewed the incident.

At Advanced, ensuring security and safety is paramount.
If you have any further questions, please get in touch using the details below.

Tel: +44 (0)345 894 7000 **Email:** enquiries@advancedco.com **Web:** www.advancedco.com

Advanced