

## Approaches for Connecting the IMS to the Aircuity Servers

There are a few methods for connecting the Information Management System (IMS) to the Internet for secure data transmission to the Aircuity servers. This data is used to populate IAQ dashboards showing energy savings, opportunities for building optimization and to allow for the proactive monitoring of the Aircuity equipment to ensure peak performance. Aircuity takes data security very seriously and has implemented multiple safeguards to protect customer data and prevent any unauthorized access to the customer's network via the IMS.

**Aircuity's standard offering addresses the key requirements for maintaining system security.**

- ✓ Prevent anyone from accessing the IMS through inbound ports.
- ✓ Prevent anyone from accessing the IMS from the IMS' outbound ports.
- ✓ Encrypt data that is being transferred from IMS to Aircuity servers.



### Secure Data Transfer from IMS to Aircuity Servers

The Aircuity IMS has an integral firewall enabling the regulation of all inbound and outbound traffic. By default *ALL* inbound ports are closed, meaning there is no access to the IMS from ANY inbound requests. Aircuity has shut down all but one outbound port for the Aircuity data transfer. This single port is port 443 and is the standard HTTPS port for all secured data transfer. As Aircuity is using SSL/TLS 256 bit encryption, the data is secure. The outbound Aircuity data through port 443 has been configured to point directly to [api.aircuity.com](https://api.aircuity.com). There are also a set of ports that are open for the sole purpose of obtaining Windows updates. These are outbound only ports and are also pointing directly to the Windows update servers. There is no other possible connection for the IMS.



### Customer's Additional Security

If the IMS is connected to the customer's internal IT network for outbound data transfer, additional firewall settings may be in place. While these can provide extra protection, they may be considered redundant given the robust data security measures already implemented by Aircuity.



### VPN Options *Additional Cost*

For customers seeking an additional layer of security beyond Aircuity's standard measures, a Virtual Private Network (VPN) option is available. The key benefit of a VPN is that it creates an encrypted tunnel for data transmission. This means that not only is the data itself encrypted, but the entire communication channel—including metadata such as network headers—is also protected. When implementing a VPN over the customer's internal network, collaboration with the customer's IT team is required to ensure proper configuration and compatibility on both ends. Alternatively, if a VPN is configured over a wireless connection, all necessary setup is handled by Aircuity, with no action required from the customer.



### Data Security at the Aircuity Server Level

To ensure secure communication between the IMS and the Aircuity Azure-hosted server, we use a custom API key-based authentication mechanism. The API key is dynamically generated on the client side and securely verified by the server before access is granted.

Refer to the [Internet Connectivity Requirements and Specifications](#) for further details.

# Main Approaches to Connecting the IMS to Aircuity Servers

To deliver ongoing support and analytics we offer several secure connectivity approaches designed to meet a range of security requirements. Review and select the one that best aligns with your IT policies.

## APPROACH 1 *best*

Ethernet Drop Connection Provided by Customer

### SECURITY STRATEGIES IMPLEMENTED

IMS has Firewall Configured as Follows:

- All inbound ports closed
- All outbound ports closed except 443
- Port 443 pointed directly to api.myaircuity.com only
- Data transfer employs Transport Layer Security (TLS) with 256-bit encryption
- Customer can implement any additional firewall restrictions and monitoring as desired.

### CHALLENGES AND CONSIDERATIONS

- IT drop planning for the IMS can take time, so discussions should begin early in the process.
- Sometimes IT teams change network settings (IP and gateway settings) without realizing it can cause MyAircuity to lose connection to its servers.
- Usually requires multiple trips or telephone calls with customer IT group to confirm network changes and to update IMS in the field.

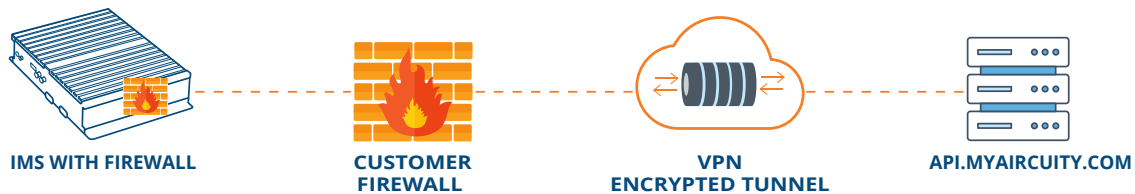
### SUMMARY

- Very secure connection
- No inbound traffic to the IMS exists
- The only outbound traffic is to our API servers
- VPN can be added at additional cost\*

## HARDWIRED CONNECTION PROVIDED BY CUSTOMER



## HARDWIRED CONNECTION PROVIDED BY CUSTOMER THROUGH A VPN (POINT TO SITE)\*



## APPROACH 2 *acceptable*

### 4G LTE Broadband Modem Connection

The wireless router is just a pass through for already secure, encrypted data. All the security measures are covered at the IMS and the api.myaircuity.com servers.

#### SECURITY STRATEGIES IMPLEMENTED

- Same as APPROACH 1 except;
- No longer running through customer's network

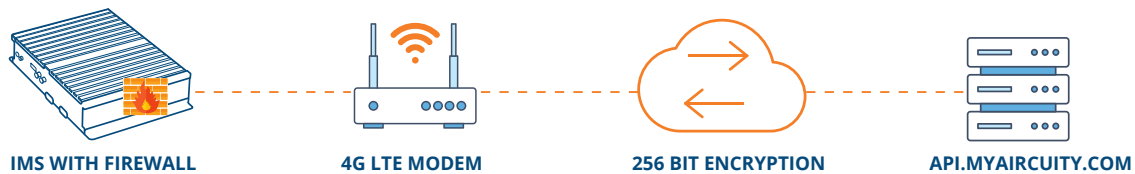
#### CHALLENGES AND CONSIDERATIONS

- While some customers may perceive the lack of direct IT oversight as a security concern, providing detailed Internet connectivity guidelines—with clearly outlined security measures—can help address and alleviate those concerns.
- Must include the additional cost of simple 4G LTE modem and SIM card subscription.

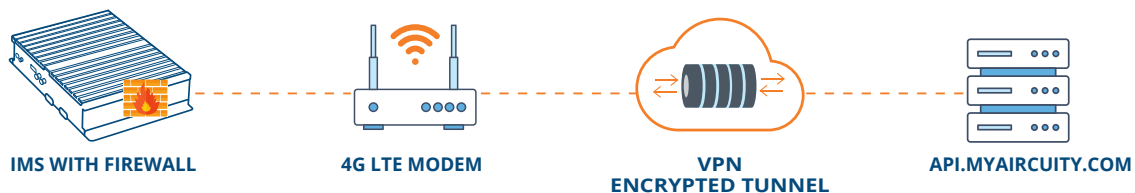
#### SUMMARY

- Very secure connection
- No inbound traffic to the IMS exists
- The only outbound traffic is to our API servers
- VPN can be added at additional cost\*

#### 4G LTE MODEM PURCHASED BY REP



#### 4G LTE MODEM PURCHASED BY REP THROUGH A VPN (POINT TO SITE)\*



### **APPROACH 3** *least preferred* Manual Data Export

If the customer is unable to permit any outbound connection even if it is not on their network, there is a possibility to manually pull the data on a periodic bases and have Aircuity manually upload the data.

#### **SECURITY STRATEGIES IMPLEMENTED**

- Since there is no connection this is the most secure

#### **CHALLENGES AND CONSIDERATIONS**

- Without proactive monitoring, there is no way for our team to be alerted if data uploads are interrupted or if equipment malfunctions occur. This lack of visibility can lead to missed issues that may impact both occupant safety and energy efficiency. In this setup, system oversight relies solely on the Building Management System's (BMS) monitoring capabilities and the technician's scheduled on-site visits, which may not detect issues in real time.

#### **SUMMARY**

- Our goal is to ensure all customers receive the full value of Aircuity's Assurance Services. While alternative connectivity approaches are available, it's important to note that they may limit certain features or reduce the overall service benefits. By clearly outlining these differences, we aim to support you in making an informed decision that best aligns with your operational and security priorities.

## **Checklist**

- ✓ Review security protocols to determine best approach
- ✓ Refer to the Internet Connectivity Requirements for further details
- ✓ Have questions? Contact your local representative or Aircuity Technical Support 1.617.641.8800, opt. 2 techsupport@aircuity.com

### **Security Practices You Can Trust**



- No Inbound Access Required
- Data is Encrypted in Transit and at Rest
- Authentication & Access Controls Safeguard all Communications