

Aircuity System Internet Connectivity Requirements and Specifications

General

The Aircuity Facility Monitoring System (FMS) includes an integrated air sampling/data communications backbone with multiple sub-nets. The FMS uses a Windows-based Information Management System (IMS) and provides Internet connectivity between the FMS and MyAircuity.com, hosted by Microsoft Azure cloud service.

Internet connectivity provides the communication path for the remote historical storage of environmental data, the generation of trend graphs and automatic notification of any system failures. Lack of Internet connectivity prevents these system functions.

Every 15 minutes (user configurable and dependent upon an active Internet connection) the IMS transfers all spooled environmental data to the client's account on MyAircuity.com via a secure TCP/IP connection. All traffic is outbound from the IMS.

Encryption

Aircuity employs Transport Layer Security (TLS) with 256-bit encryption to transfer environmental data to Aircuity's servers on Azure cloud. If an active Internet connection is not available for some period of time, the IMS will spool all data and transmit a larger size file once the Internet connection is restored.

A password protected, VeriSign® SSL encrypted, web-based user interface and data management system shall store collected environmental data along with key building characteristics to produce trend graphs and building evaluation reports.

IP Address and Port Requirements

The IMS system operates with restricted outbound port access, with all outbound ports closed except for those explicitly required for essential services. The following firewall rules have been applied:

1. **Blocked All Outbound Connections:** All outbound connections for Domain, Public, and Private profiles have been blocked by default, ensuring no external communication. Subsequent rules selectively open necessary ports for specific applications.
2. **Windows Updates:** Outbound traffic for Windows updates is allowed on TCP ports 80, 443, and 49152-65535, but only for the svchost.exe process to ensure critical updates are received securely from Microsoft.
3. **BACnet Communication:** Inbound/Outbound traffic to local/remote ports 47808 is allowed for BACnet communication, enabling proper data exchange for system monitoring.
4. **Aircuity IMS Manager:** Outbound access is granted on TCP port 443 to a specific Azure IP (40.84.147.78) for secure communication specifically between the IMS Manager software (Ims.Manager.Console.exe) and api.myaircuity.com which is Aircuity's REST service endpoints on Azure Cloud.

These changes significantly restrict outbound traffic, ensuring that only necessary applications and services can communicate with external systems. The IMS can now safely connect to specific trusted domains and IP addresses for updates and remote access while minimizing security risks.

For Systems Configured to Only Connect with api.myaircuity.com: Port 5938 is highly recommended

Port 5938 is used by Aircuity support staff for remote diagnostics and maintenance of the IMS. The application used for this purpose is called TeamViewer which works with an encryption method based on RSA public/private key exchange and AES (256 Bit) session encoding. This technology is used in a comparable form for https/SSL and can be considered completely safe by today's security standards. Team Viewer's security statement may be furnished upon request.

The IMS IP address can be either static or Dynamic Host Control Protocol (DHCP). By default, the IMS ships ready for DHCP but can be readily modified by an Aircuity trained service technician to use an owner specified static IP address.

BACnet® Port (if applicable) IP Address Requirements

If the IMS is connected to a BACnet network the BACnet interface must be configured with a static IP address. Note: IP Address, Subnet Mask and Default Gateway must be configured. DNS is not required.

If the BACnet network has access to the Internet, the IMS may use its BACnet interface for both MyAircuity.com and BACnet network connections. The DNS IP address on the BACnet interface must be valid to support the connection to MyAircuity.com. If the BACnet network does not have access to the Internet, the IMS's primary LAN connection must be used to support the data transfer and analytic functionality on MyAircuity.com.

Optional Virtual Private Network (VPN) Connection

In an effort to provide additional security measures, Aircuity can support connectivity utilizing a secure (IPsec), encrypted (3DES) site-to-site virtual private network (VPN) connection.

Implementation requires client-side router/firewall configuration to support VPN connectivity with Aircuity's servers on Azure cloud. Additional hardware may be required.

A site-to-site VPN gateway connection is used to connect your on-premises network to Aircuity's servers on Azure cloud over an IPsec/IKEv2 VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

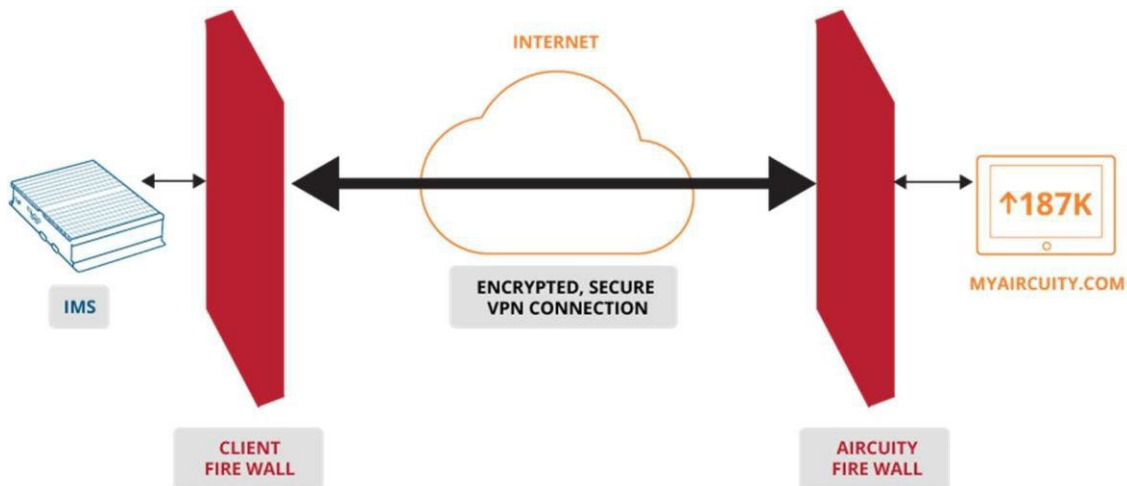


Figure 1: Aircuity /Client VPN Connection

At a minimum we will need the customer's VPN devices to use IKE Version 2 and should be VTI (Virtual Tunnel Interfaces) based. Please read below which describes the new VPN connectivity parameters we must work with to make a secure site to site connection with Aircuity.

1. To establish the VPN connection with Aircuity on Azure, IKEv2 is a requirement. The VPN device should be listed on the following list: [Link to Microsoft.com](#)
2. If you don't see your device listed in the Validated VPN devices table, your device still may work with a Site-to-Site connection. Contact your device manufacturer for additional support and configuration instructions.
3. The tables on Microsoft's site contain the combinations of algorithms and parameters Azure VPN gateways use in default configuration. For route-based VPN gateways created using the Azure Resource Management deployment model, you can specify a custom policy on each individual connection.

Please use the IKEv2 for IKE/IPsec configuration: [Link to Microsoft.com](#)

4. In addition, you must clamp TCP MSS at 1350. Or if your VPN devices do not support MSS clamping, you can alternatively set the MTU on the tunnel interface to 1400 bytes instead.
5. Aircuity Azure environment to connect to the client device.
 - VPN Aircuity Azure Gateway Public IP: 23.98.223.122
 - Virtual Network Aircuity Azure Address Space: 192.168.20.0/22

Important: the client network should not overlap with the Aircuity Azure virtual network Address Space.

6. Information required from the CLIENT:
 - VPN Client Device Public IP.
 - Client Address Space
7. The pre-shared key between Aircuity Azure and the client device should be alphanumeric.

Location on the Network

The IMS can reside directly on the client's network, inside the firewall or within a DMZ as appropriate for the client's security requirements. Please contact Aircuity Technical Support techsupport@aircuity.com to discuss additional configuration options.

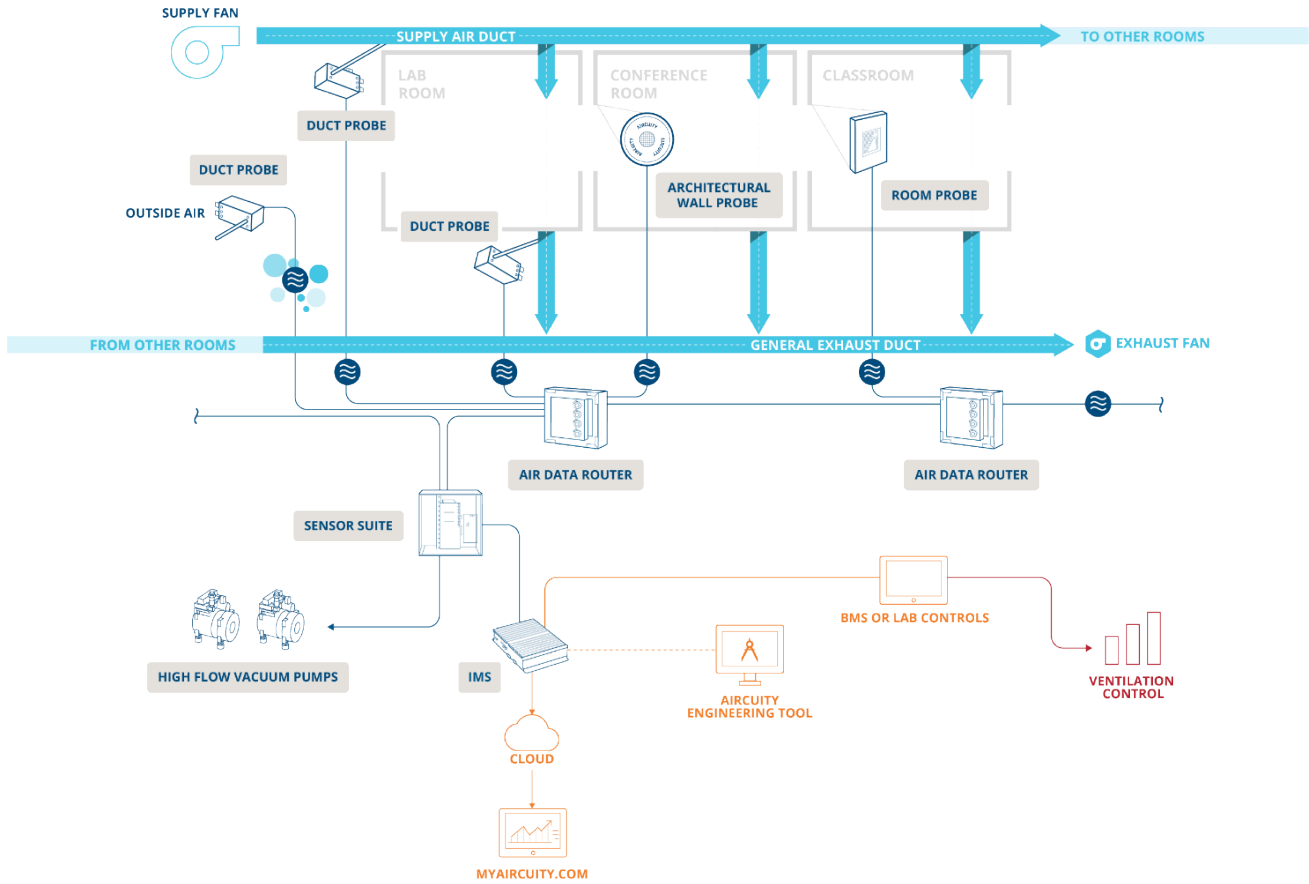


Figure 2: Aircuity Platform