ALERTON

VAV IP Controller

SECURITY GUIDE

DISCLAIMER

While we have engaged in efforts to assure the accuracy of this document, Alerton is not responsible for any damages, including consequential damages arising from the application or use of the information contained herein. The information and specifications published here are current at the time of publication and are subject to change without notice. For the latest product specifications please visit our website or contact our corporate office.

Alerton

715 Peachtree Street NE

Atlanta, Georgia 30308

www.alerton.com

INTRODUCTION

This guide contains information on the safe installation and configuration of an Alerton VAV IP controllers, as well as safety-related information on operation, maintenance and decommissioning.
(Models: **VAVi-7u5-IP**, **VAVi-7u5-IP-BLE, VAVi-0-IP**).

Please take some time to read and understand all relevant installation, configuration and operating manuals and ensure that you regularly obtain the latest versions.

Related Security documents

The table below shows the relationships of other Alerton security manuals:

Document	Description
Compass Dealer Security Guide (LT-SEC-DG-CMPS)	Provides security-related instructions for planning, installing, and configuring a compass system. The intended audience is an Alerton dealer.
Compass End-User Security Guide (LT-SEC-EUG-CMPS)	Provides security-related instructions for maintaining and decommissioning a compass system. The intended audience is the compass system owner and end-user.
ACM Dealer Security Guide (LT-SEC-DG-ACM)	Provides security-related instructions for planning, installing, and configuring an ACM. The intended audience is an Alerton dealer.
ACM End User Security Guide (LT-SEC-EUG-ACM)	Provides security-related instructions for maintaining and decommissioning an ACM. The intended audience is the compass system owner and end-user.
VIP Dealer Security Guide (31-00300)	Provides security-related instructions for planning, installing, and configuring an VIP. The intended audience is an Alerton dealer.
VIP End User Security Guide (31-00301)	Provides security-related instructions for maintaining and decommissioning an VIP. The intended audience is the compass system owner and end-user.

SYSTEM DELIVERY

This section includes information on activities that need to happen when the Building Management System (BAS) is delivered to the system owner.

Documentation contains security information

The documentation package delivered with your system should include the following:

- Manual
- VAV settings, including network parameters.
- Network settings, especially network configurations that provide isolation between the BAS/BACnet Network and other networks.
- Firewall settings, such as ports that are allowed through, especially ones that are essential to maintaining the designed security protections.
- Physical security controls, such as a locked cabinet or equipment room, that restricts physical access to VAV Controllers.

Ensure device packaging is in good state.

Inspect that the packaging of the VAV module is intact and not opened, know that it has not been tampered with in enroute.

SYSTEM OVERVIEW

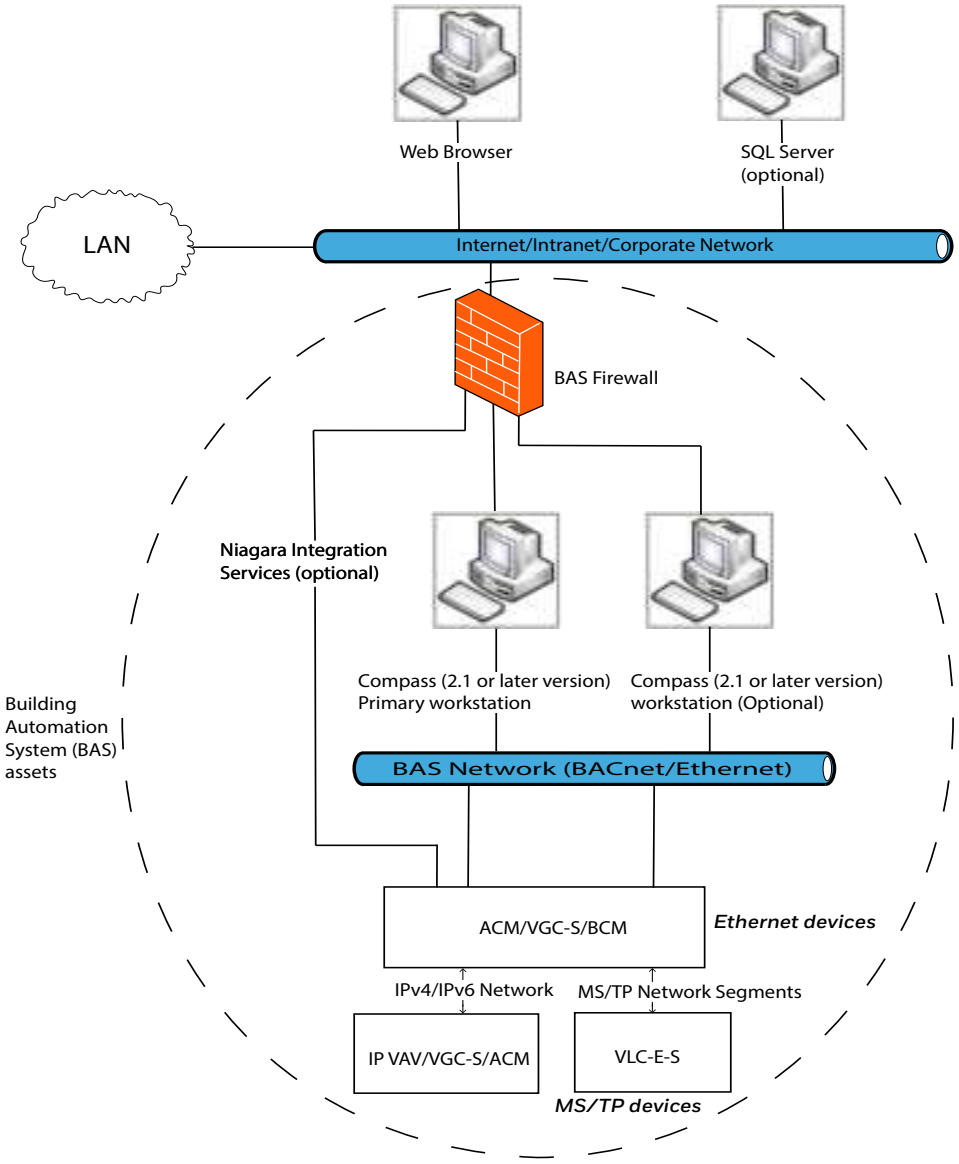

Fig. 1 Graphical description of recommended network topology in a global scope

The key elements of the system overview are:

Internet/Intranet/Corporate Network: This is a simplified, logical network representation of all networks outside the building automation system (BAS) scope. It may provide access to the BAS management interfaces (e.g., the compass primary workstation web user interface) but must give access to the internet so that compass computers can check for and download operating system and virus scanner updates unless another means to do this is provided.

BAS Network: This network is used solely for BAS protocols, which consists of BACnet/IP, BACnet/ Ethernet, and any protocols that a VAV might use. This network must not be the same network as the internet/intranet/corporate network..

BMS Firewall: To provide additional separation and protection to the BAS, use a firewall between the internet/intranet/corporate network and any BAS device that connects to it, such as the compass primary workstation, compass workstations, and VAV controllers.

Compass Primary Workstation: The compass primary workstation is a computer running software. It requires two network connections – one for connecting to the management web user interface through a web browser (usually on the Internet/intranet/corporate network) and another for connecting to the BAS network.

Web Browser: Compass software provides a web-based management interface that is accessed through a web browser not dependent of a connection to the internet.

Compass Workstation (optional): If access to the compass primary workstation's thick client interface is not allowed, then install a compass workstation on a separate computer to access thick client functionality. For example, if the compass primary workstation is run in a virtual machine as a service or console access to it is not permitted.

SQL Server (optional): Compass software can be configured to use an external SQL server.

PLANNING AND INSTALLATION

This section includes information for planning and performing a VAV installation.

Physical equipment

It is essential to discuss physical security of VAV controllers with your customer when planning a system installation. This discussion should assess the security needs of all Alerton VAV IP's components as well as the requirements of the system owner and provide suggestions for best practices if the system owner does not have requirements of their own.

Controlling physical access to Compass workstations, VAV controllers, and network equipment is a fundamental security control that must be implemented on all installations. This can range from locating all mentioned network equipment and controllers in locked rooms or cabinets to using an active access control system that logs access. (As for any log, an access log is only effective if it is monitored and audited regularly).

Compass Planning and Installation

Compass planning and installation security information can be found in the Compass Dealer Security Guide (LT-SEC-DG-CMPS).

VAV IP Connect Communications Bus and Microset

It is required that physical security access to the VAV IP Connect communications bus and wall module bus wiring be accomplished by:

1. installing wiring in physically inaccessible locations that restricts physical access to the VAV IP Connect communications bus.
2. Or installing wire in conduit.

This required physical security access protection is important to prevent security threats to the control system. Failure to protect the VAV IP Connect communication bus and Microset bus can lead to critical security issues. For example, data loss or corruption could result due to not following the required protection for the VAV IP Connect communication bus.

VAV IP Modbus Connections Communication Bus Best practices

Security of the bus also means that the bus is electrically reliable for communications. It is important the bus is installed with one wire type consistent throughout the whole gateway to controller connection as to eliminate reflections from bus wire impedance mismatches. Shielded wire is not recommended for normal installations.

Recommended VAV Installation Configuration

The following section illustrates the recommended VAV installation configuration. Note that the VAV has a built-in two- port Ethernet switch. The diagram below (Figure 2.) uses the switch functionality to daisy-chain multiple VAV controllers.

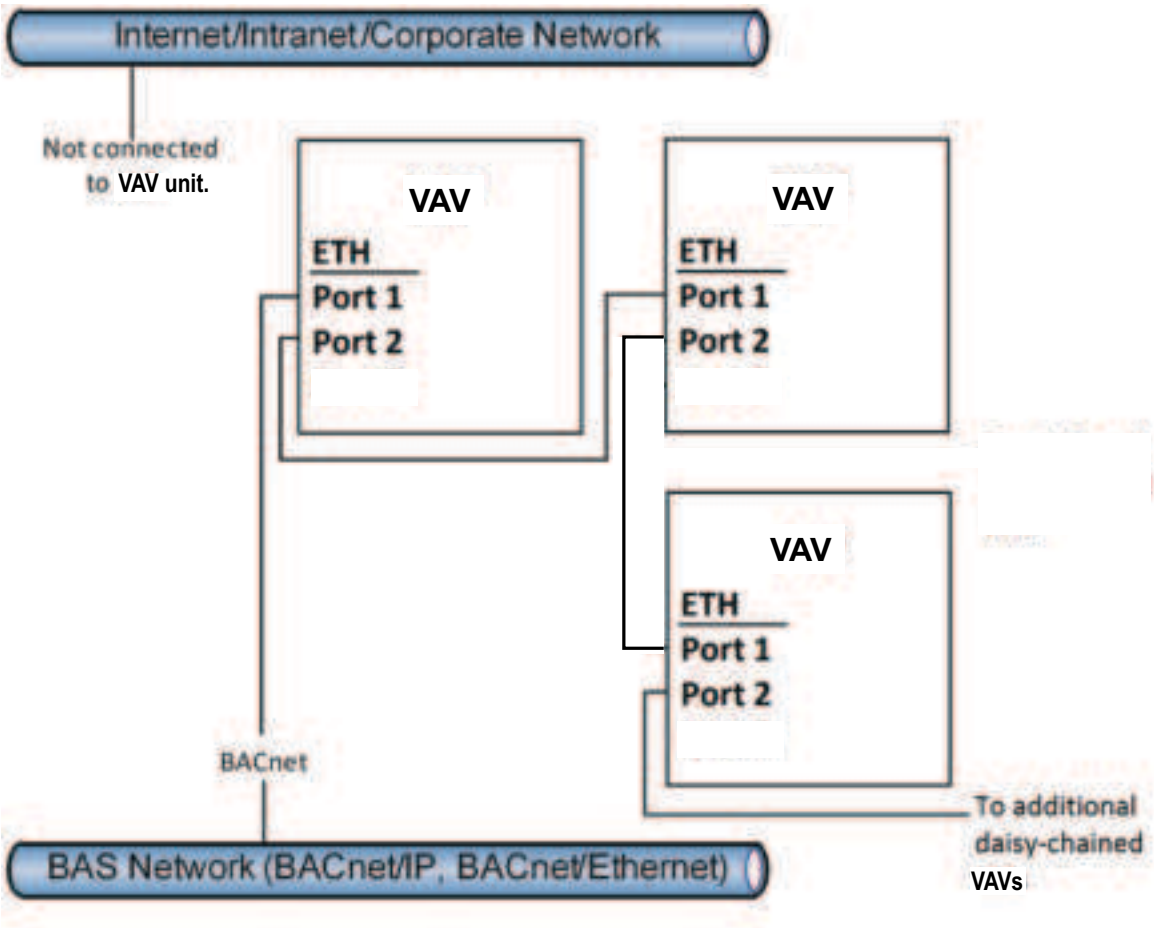

Fig. 2 Graphical description of the recommended IP VAV connection in daisy chain.

Segregate and Protect Networks

Alerton recommends the following to secure and protect networks:

Use a separate dedicated physical network (e.g., separate wires) or virtual network (e.g. VLANs) for BACnet communication. This must be a separate network from the Internet/intranet/corporate network, a firewall can be used with special considerations.

Apply a tamper-evident sticker over the VAV access panel.

If a customer needs additional assurance that the physical access protecting a VAV has not been entered, install a tamper-evident seal or sticker over the access point, or use a door switch on the panel connected to an input of the VAV to provide an alarm.

Documentation

Documentation is essential in capturing design and configuring information required to maintain a secure system.

Document physical devices and configurations, including key security-related information.

All documentation on devices and configurations must include security-related information to establish and maintain the intended security controls. For example, if changes are made to the default services or ports on the VAV, then document these so that the settings can be restored at some point in the future.

Make sure important files for configuration and operation of the VAV unit are stored and safeguarded. Edition or replacement of the files shall be controlled by adding, at least, one layer of security where machine admin log information like admin user and password is required.

Some of these critical files are:

- PointData.mdb: used for Bacnet object configuration.
- DDC.vsdx or DDC.bd9 and its variants: used for the application logic.
- Trendlogbuilder.xlsx or calendarbuilder.xlsx: used to create trendlogs and calendars.
- DCF file: this file is used for configuration of the device.

Document external systems, especially interaction between the VAV and its related systems

The BAS commonly requires or utilizes external systems functionally, such as existing network infrastructure, VPN access, virtual machine hosts, and firewalls. If the BAS requires those systems to be configured in a certain way for security, such as a firewall allowing or denying specific ports or a network allowing access to specific systems, you must document this information. If these systems need to be restored at some point in the future, e.g., due to equipment failure, or changes need to be made to the external systems, e.g., upgrading a firewall, having documented this information will help you restore to the previous security level.

CONFIGURING A VAV

This section contains information for configuring a VAV.

Control traffic from other subnets

It is recommended to always disable traffic to/from other subnets. For security reasons, traffic to/from other subnets is by default disabled, preventing devices from other subnets from reaching this device.

Fig. 3 Ethernet Configuration

Create and maintain a baseline of Controller Configurations

Create and maintain a baseline of VAV configurations properly configured for security. Ensure that this baseline also includes DCF files. Do not commit insecure configurations to the baseline to prevent inadvertently applying them in the future. Update any relevant documentation when configurations change.

Change Default Passwords.

There is no default password for Backup/Restore/Restart. Users who do not set up passwords for these features are effectively disabled.

Even with good password strength requirements, there are some passwords that are stronger than others. It is important to educate users on password strength. Password strength requirements are not sufficient to ensure that strong passwords are used. For example, Password10 satisfies all the requirements, but is a weak and easily hackable password.

BLE Password Configuration

If not in use it is always advice to disable BLE communications from the DCF.

BLE Configuration allows an 8-character PIN password that is used for pairing authorization and further communication, a strong password is recommended since unauthorized access could result in the modification of critical values used on airflow calculations and provoke harm to the system and other connected controllers.
See installation and operation guide for Alerton VAV for more instructions on how to configure the BLE password.

Changing the backup and Restore/Restart/Control Passwords

To change the backup or restore/restart/control passwords, use Compass to edit the VAV configuration.

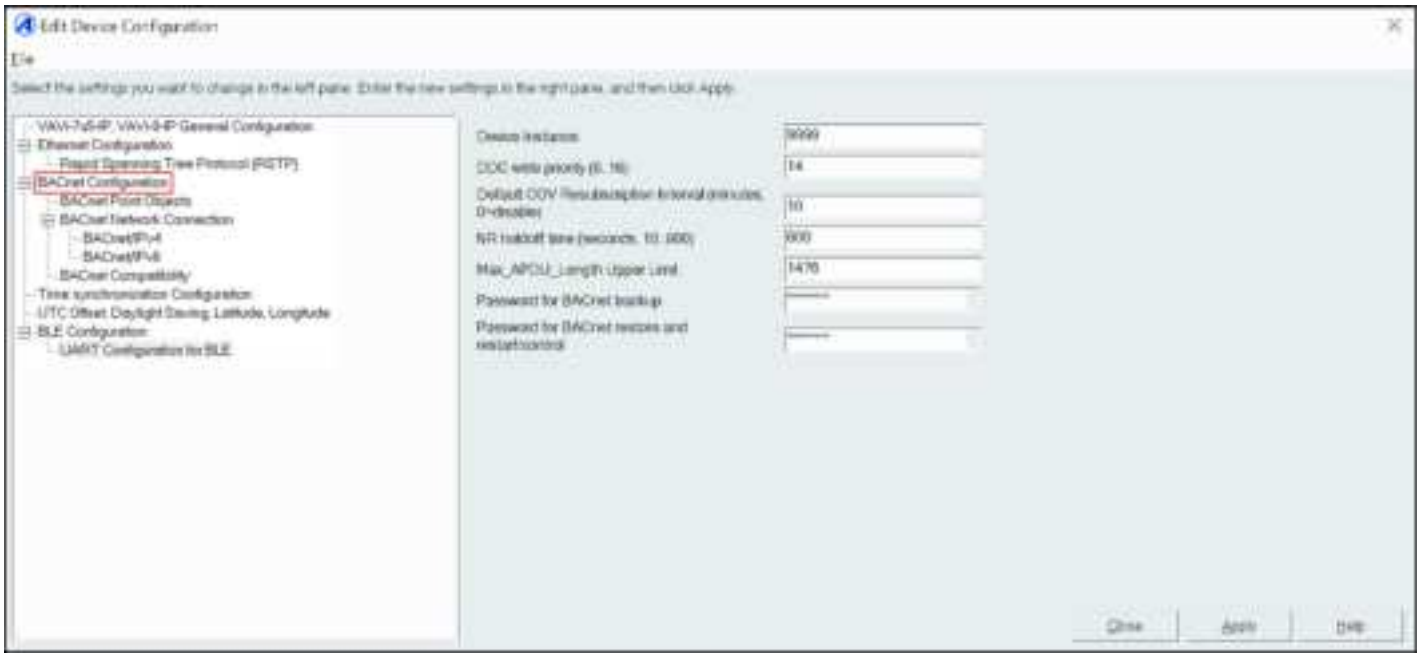

Fig. 4 BACnet Configuration

One password specifically for BACnet Backup and another password for Restore/Restart/Control. Both passwords are stored as hashed values in the DCF.

> **IMPORTANT!** The backup/restore/restart/control password should differ from passwords used for any other purpose. It is OK to use the same backup/restore/restart/control password for multiple devices, provided the password is safe. It should not be the same password used for user login to any service, including the VAV configuration screens.

Compass Configurations

Compass security considerations for its configurations is detailed in Compass 2.1 End User – section: “Installation, Configuration and system delivery”.

Basic security measure to consider:

- Compass must be configured to use HTTPS even on a private network.
- Extra care must be taken to protect the SQL server system if configured.

About Microset Field Service Mode

It is highly recommended that a connected Microset 4 device has a configured password to prevent unsupervised access to field service mode which in normal circumstances allows technicians to query and adjust key operating setting of the system and without prevention could allow unsupervised actions with potentially harmful consequences.

Also Microset 4 device has the capacity to not allow Field Service mode after the airflow balancing process has being finished.

For Microset 4 detailed information and instructions see Microset 4 Installation & Operations Guide - Service Mode section.

For (Legacy) Microset 2 (which does not count with a password feature) it is recommended to secure the file that contains steps involved in getting access to this mode, these instructions are in the file named Field-Service-and-Balance-Modes-from-LTBT-TM-MSET2-rev0003.

Considerations for the BAS firewall

These next considerations assume that the installation process has follow the network recommended configuration guidelines stated Fig. 2, located in “Recommended VAV Installation Configuration” section in which we are using a firewall to isolate the BAS network from the internet or the corporate network.

Important points regarding UDP port.

- This port is used for data transmission by every BAS unit in the network.
- It is highly recommended that the default port value for UDP (47808) is changed, this is important for automatic cyberattacks prevention.
- An installed firewall that successfully isolates the BAS network should not allow UDP traffic flow to the internet/intranet or any other network. Failure in ensuring this could mean that any unsupervised personnel connected to the non-isolated network would have access to unencrypted BacNet messages by connecting a sniffer.

Important points regarding NTP port.

- This port is used for Time Synchronization from Network Time Server.
- It is not critical to manually change the port default value (100).
- NTP data flow should not be allowed to flow through the BAS firewall, failure in ensuring this could mean that any unsupervised personnel connected to the non-isolated network would have access to unencrypted NTP messages by connecting a sniffer or potentially injecting malicious messages to the network.
- It is recommended that the NTP server is on the same subnet.

The following table summarize information stated above:

Table 1 Configuration BAS Fairwall

Default Port/Protocol	Purpose	Change from Default?	Allow Through BAS Firewall?
47808/UDP	BACnet/IPv4 network connection	Yes	No
47808/UDPv6	BACnet/IPv6 Network connection	Yes	No
100/NTP Server	Time Synchronization from Network Time Server.	No	No

SECURITY RECOMMENDATIONS FOR USE OF A VAV

Monitor physical access controls.

Monitor the physical access control of the IP VAV, such as monitoring the room where the IP VAV is installed, installing a sensor on the cabinet, or instituting a process for checking out the key to the cabinet where the IP VAV is mounted. Monitor for unauthorized access.

Monitor Paired BLE Mobile Device.

Monitor the physical access to mobile device, do not save the password on auto loggers, do not leave an open session after finishing working with the mobile device that could allow unauthorized access to the app connected to the controller network.

Monitor network access controls.

Monitor firewalls and any other network access controls for unauthorized changes or access. Consult your specific firewall documentation for more information about its monitoring and logging facilities.

Monitor Compass control access.

End user should monitor the room where the Compass Primary Workstation is located. Supervise login credentials access and the number of permits those behold. Renew passwords and do not leave Compass sessions opened if the logged in session owner is not present.

About DDC Logic considerations and disclaimer.

Preferable, end user, should not send custom DDC applications created by someone else other than an Authorized Alerton Dealer, use and secure the DDC logic delivered along the system, save it in a higher edit administration rights directory and supervise last edit every time there is a need to resend the file to the VAV IP controller.

SECURITY RECOMMENDATIONS FOR MAINTENANCE OF THE VAV

Compass Workstation Maintenance

Make sure Compass Workstation is running up to date virus software and comply with corporate PC security standards as well as having the last Compass version available which could include solutions to already found vulnerabilities and/or updated third party libraries, overall stronger versions in cybersecurity are incrementally delivered. See Compass End-User Security Guide (LT-SEC-EUG-CMPS). Documentation for more information on how updating its libraries and software.

Update to latest ROC

New ROC files are released regularly and may include security fixes and enhancements. If your dealer does not do this as part of a maintenance agreement, you must periodically monitor for updates and apply them.

Updating the VAV ROC in Device Manager

Use the Device Scan feature in Device Manager to scan the network for the VAV and save it to the Device Manager Table. It is an easy way to ensure the VAV is communicating. A device record for the VAV must exist in Device Manager for you to view and change VAV values using Compass. The device record stores set up information about the VAV. An accurate device record is a key to managing DDC, ROC files, and automation features.

Once a device record exists, use Device Manager to send and read data from the VAV. See the Compass Installation and Upgrade Guide for more information about working in Device Manager.

NOTE:
Only add the device record to the Device Manager when the VAV does not already exist in the Device Manager table. If the VAV exists in Device Manager, Do NOT save to table until sending Device Properties. Doing so will delete Device Profile parameters.

- Make sure your Compass installation has the most recent VAV ROC file.
- Use Compass Device Manager to send the ROC file to the VAV. Open Device Manager >select the device(s) > click Send > (check on ROC box) > Send.

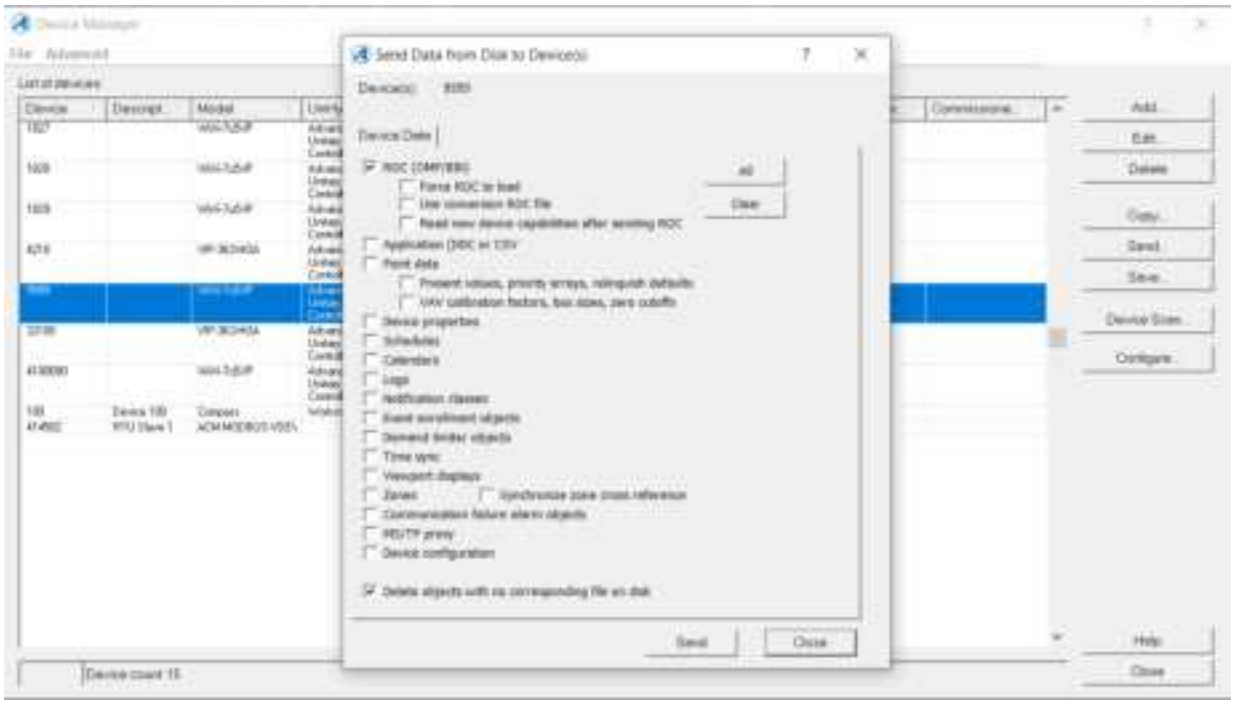

Fig. 5 Send Data from Disk to Device(s)

SECURITY RECOMMENDATIONS FOR DECOMISSIONING OF THE VAV

This section contains information for decommissioning an Alerton VAV IP.

Reset Alerton VAV IP to factory defaults.

Resetting the Alerton VAV IP to factory defaults will erase all data stored in its configuration. For more information on how to reset the VAV IP to factory defaults, see Alerton VAV IP Controller_Installation and Operations Guide_ 31-0531-02.pdf

VAV INSTALLATION SECURITY CHECKLIST

VAV Device Instance:

VAV Description:

VAV Location:

Installer: Date:

Complete the following security tasks for each installed VAV:

(**YES/NO**) Design a secure installation considering both software and hardware vulnerabilities.

(**YES/NO**) Develop a Disaster and Recovery Plan documenting configurations important for the network security and integrity.

(**YES/NO**) Install a firewall between the Building Automation System (BAS) and external network, securely configure both the firewall and network.

(**YES/NO**) Physically secure the VAV and Compass Workstation in a place with restricted access.

(**YES/NO**) Set a password for the next features:

1. Backup password
2. Restore/Restart/Control password.
3. Microset Field Service Mode Password. (if installed)

(**YES/NO**) Disable Microset Communication port if it is not being used.

(**YES/NO**) Provide all required data to the BAS system owner at delivery.

Train end users on documented security maintenance tasks

This manual provides instructions on security maintenance task for the VAV modules, but additional system level tasks also need to be documented. End users should be trained in these tasks:

- IP VAV Firmware Download process.
- Compass Update Process.
- User should be conscious of the right measures to safeguard files mentioned on Documentation section.

Documents should be delivered along the system, but end user can always find these an other documents on https://buildings.honeywell.com

ALERTON

715 Peachtree Street NE
Atlanta, Georgia 30308
www.alerton.com

31-00529-02 I Rev. 08-24