Johnson Controls

OpenBlue
Enterprise Manager

OpenBlue Enterprise Manager Security and IT Guide

Digital Solutions
www.johnsoncontrols.com

LIT-12012593
Release 4.0
2021-11-29

Contents

Introduction

This document is intended for building automation system (BAS) and IT professionals.

Engage appropriate network security professionals to ensure that the computer that hosts the Site Director is a secure host for Internet access. Network security is an important issue. Typically, your IT organization must approve configurations that expose networks to the Internet. Be sure to read and understand IT Compliance documentation for your site. Use care when you perform steps on OpenBlue system components because you may require system restarts that conflict with compliance requirements. For example, upgrading an ADS/ADX/ODS requires the computer to be offline for a period of time. Similarly, installing new software on the ADS/ADX/ODS may require a computer restart.

Figure 1: Cloud hosted solution Metasys via ADS/ADX

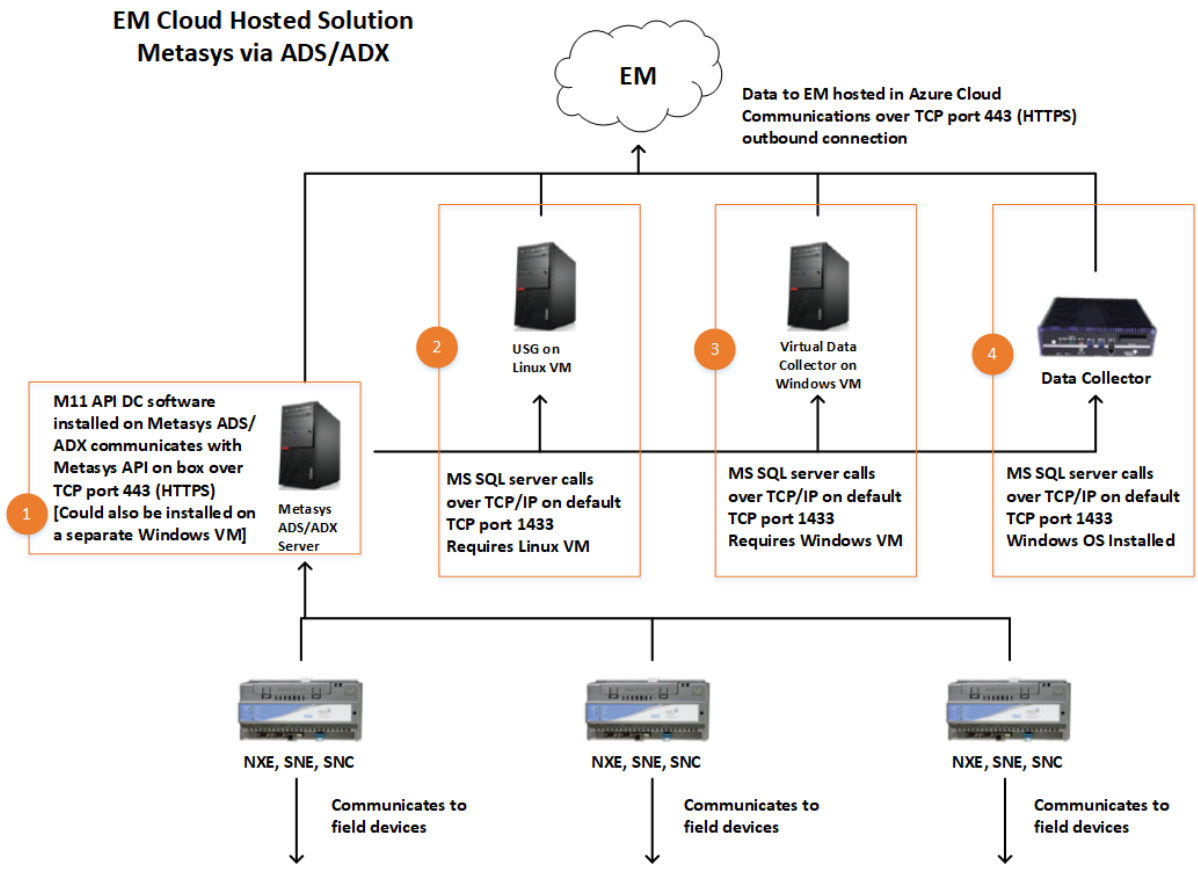


Figure 2: Cloud hosted solution Metasys via BACnet IP

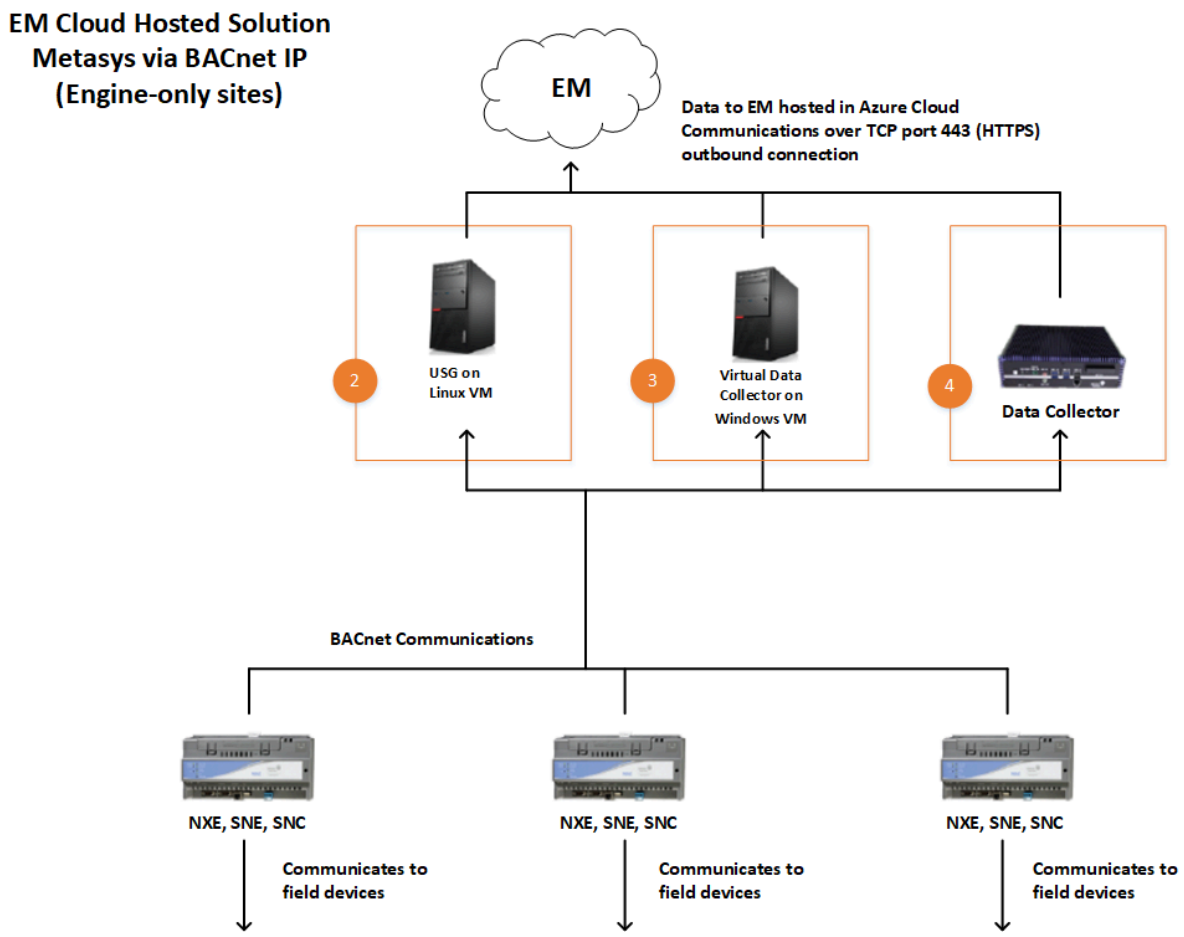


Figure 3: Cloud hosted solution BACnet meters

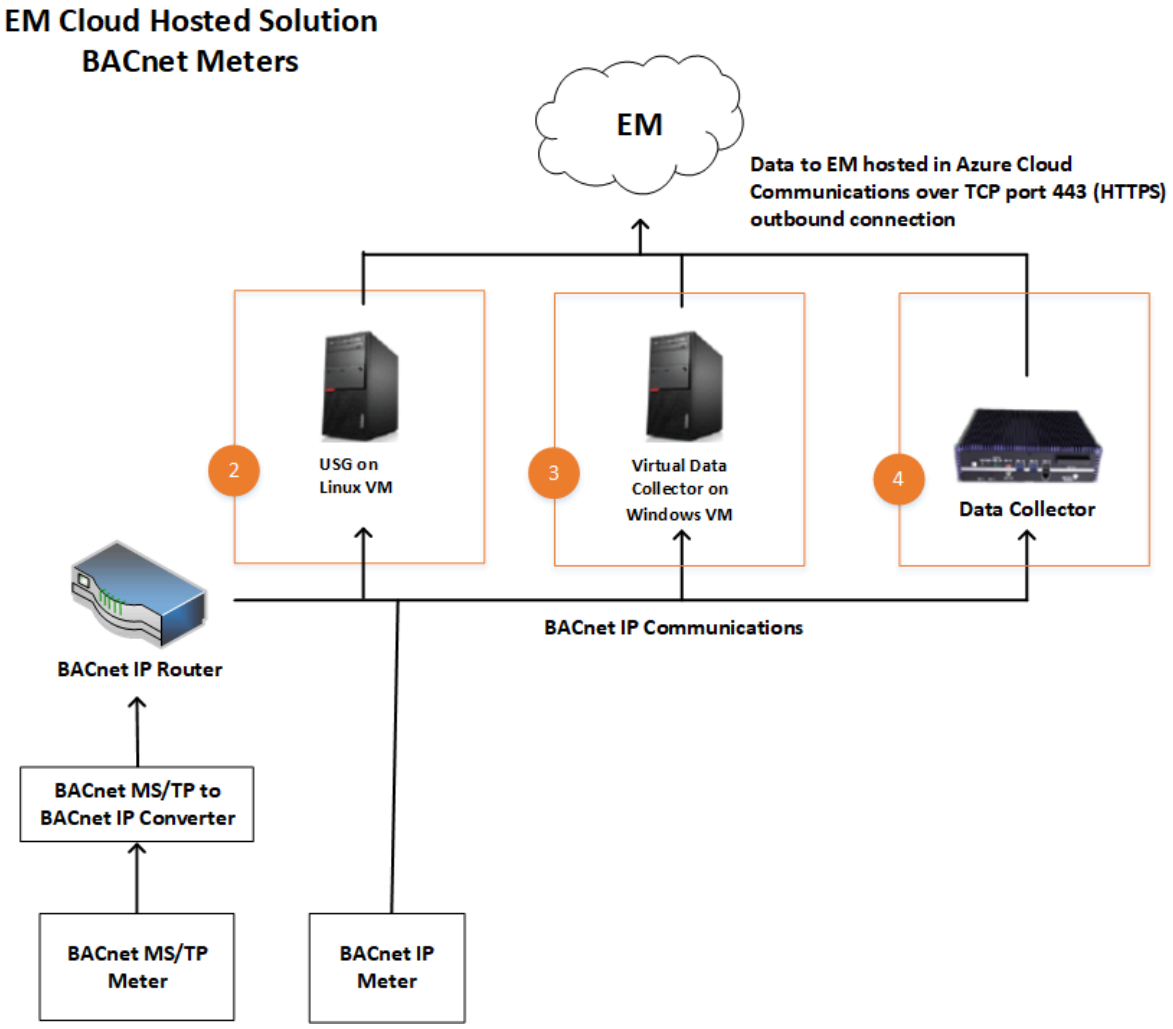
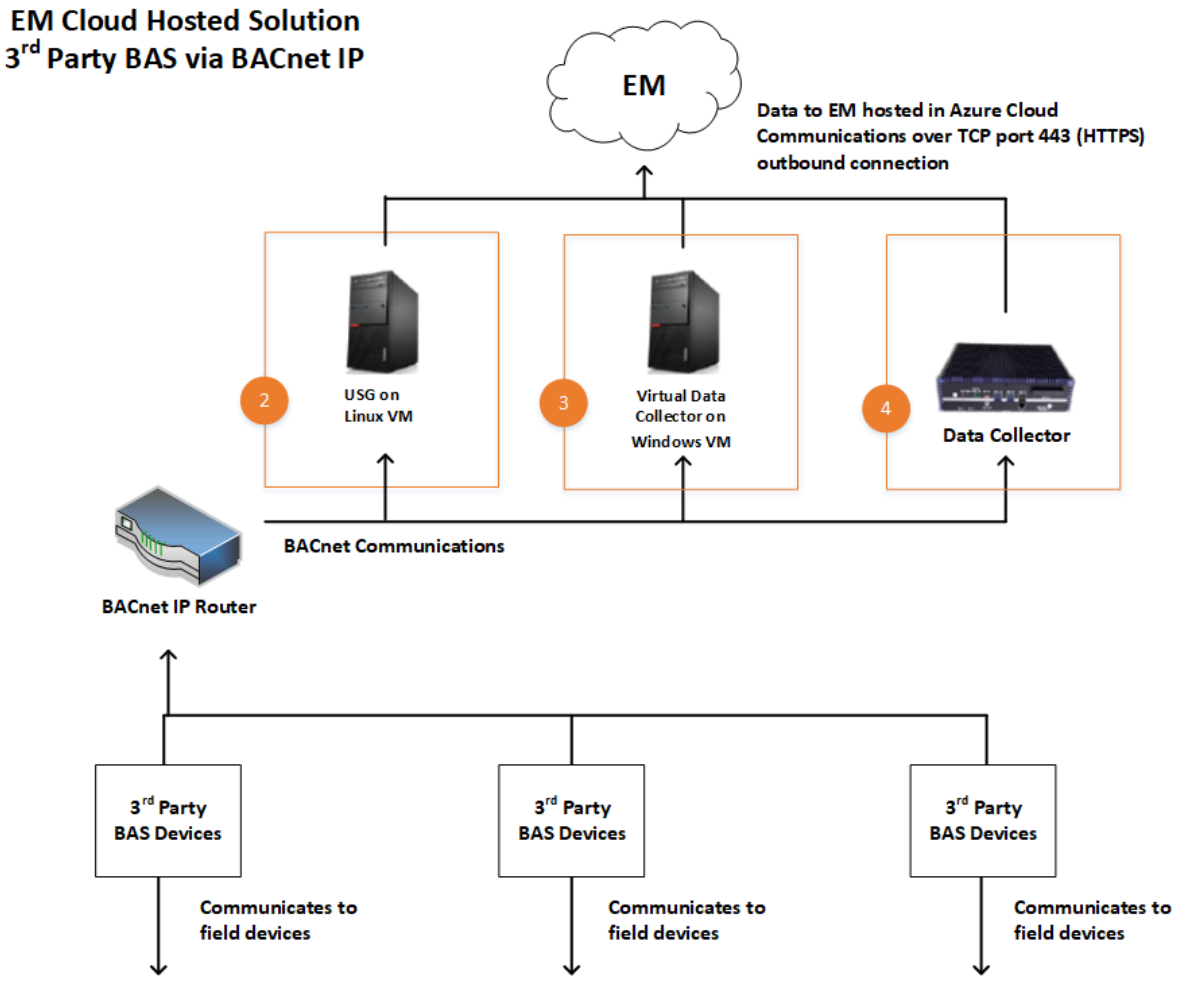


Figure 4: Cloud hosted solution third-party BAS via BACnet IP



Microsoft® Azure security and privacy

Microsoft® makes security and privacy a priority at every step, from code development up to incident response.

Security and privacy are built into the Azure platform. The Security Development Lifecycle (SDL) addresses security at every development phase, from initial planning to launch. Microsoft update Azure continually to make it even more secure. Operational Security Assurance (OSA) is an additional framework that ensures secure operations throughout the lifecycle of the cloud-based service. Azure is the only public cloud platform to offer continuous security-health monitoring.

Security

Microsoft employs rigorous security and technology practices to ensure that Azure is resilient to attack, safeguards user access to the Azure environment, and keeps customer data secure.

Encrypting communications and operation processes:

- For data in transit, Azure uses industry-standard transport protocols between user devices and Microsoft data centers, and within data centers themselves.
- For data at rest, Azure has a wide range of encryption capabilities up to AES-256.

Securing networks:

- Azure has the infrastructure necessary to securely connect virtual machines to one another and to connect on-premises datacenters with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft datacenters with a variety of technologies. Azure Virtual Network extends your on-premises network to the cloud with site-to-site VPN.

Managing threats:

- To protect against online threats, Azure uses Microsoft Anti-Malware for cloud services and virtual machines. Microsoft also employs intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing, data analytics and machine learning tools to mitigate threats to the Azure platform.

Privacy

Microsoft adheres to the world's first code of practice for cloud privacy, ISO/IEC 27018.

With Azure, customers own customer data - that is, all data, including text, sound, video or image files and software, that customers supply to Microsoft with Azure. Customers can access their data at any time and for any reason without assistance from Microsoft. Microsoft does not use customer data or derive information from it for advertising or data mining.

Compliance

Azure conforms to a broad set of international and industry-specific compliance standards, such as ISO 27018, HIPAA, FedRAMP, and SOC 3, as well as country-specific standards like Australia IRAP, UK G-Cloud and Singapore MTCS.

Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls that these standards mandate. As part of Microsoft's commitment to transparency, you can request audit results from these third parties to verify successful implementation of security controls.

OpenBlue Enterprise Manager data center security compliance

OpenBlue Enterprise Manager conforms to the following compliance protocols:

- The Statement on Standards for Attestation Engagements (SSAE) No. 16/Service Organization Controls (SOC) 3. Microsoft Azure SOC Reports can be downloaded: `https://servicetrust.microsoft.com/Documents/ComplianceReports`.
- The Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of the American Institute of Certified Public.
- Accountants (AICPA) in January 2010. SSAE 16 effectively replaces SAS 70 as the authoritative guidance for reporting on service organizations. SSAE 16 was formally issued in April 2010 with an effective date of June 20, 2017.
- SSAE 16 was drafted with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard, International Standards for Assurance Engagements (ISAE) 3402. For more information on SSAE-16, SOC 3, and other reports, please visit `http://www.ssae-16.com`.

Security and network configuration considerations

Security consideration

The OpenBlue Enterprise Manager data collector ships with Windows Defender Anti-virus pre-installed. If you choose to use a different anti-virus solution, you must exclude the following directories:

- `C:\inetpub\wwwroot`
- `C:\Program Files\Johnson Controls\BuildingPlatform`
- `D:\BuildingPlatform`

Router and firewall devices

For the Johnson Controls hosting site to communicate with your Building Automation System (BAS), you must identify and configure all network control devices that segregate access to allow data transmission.

Perimeter control considerations (connections to the cloud)

You must place the OBEM Data Collector in a segment of the customer network that allows outbound Internet access. It is possible to accommodate a variety of options for network placement including, but not limited to, a restricted segment of the network such as a demilitarized zone (DMZ) dedicated to business partner or third-party vendors, or another secure segment of the internal network, such as a virtual local area network (VLAN) segment logically dedicated to the OpenBlue Enterprise Manager data collector.

OpenBlue Enterprise Manager requires the standard web protocol HTTPS for communication between the data collector and the cloud-hosted data center. OpenBlue Enterprise Manager encrypts all customer data with HTTPS. You must configure perimeter routers and firewalls to allow outbound traffic on TCP port 443 from the data collector to the cloud-hosted environment. No other communication ports are necessary for data transmission to the internet.

Johnson Controls uses TeamViewer to provide remote support, monitoring and troubleshooting. You must allow TeamViewer in your network.

Destination IP addresses

OpenBlue Enterprise Manager customers can practice DNS white-listing or granular IP address filtering through network devices (for example, proxies or firewalls) for various reasons.

The OpenBlue Enterprise Manager platform uses the Microsoft Azure webapp, which requires a list of globally dispersed IP address ranges to be available as destinations for the OpenBlue Enterprise Manager data collector communications. Microsoft updates this list periodically due to changes at their data centers. Microsoft maintains additions and deletions in an XML file available at `https://www.microsoft.com/en-us/download/details.aspx?id=41653`. You must enter all addresses in this list. When you troubleshoot connectivity issues of the OpenBlue Enterprise Manager data collector, review the XML file to ensure all the IP address ranges are up to date.

Internal network control considerations (connection to customer ADX)

You must configure any internal network connection between the Johnson Controls ADX or third party BACnet device and the OpenBlue Enterprise Manager data collector to allow data transmission on TCP port 1433 (SQL).

The IT team must open the following Inbound Connection ports to enable the Command and Controls feature:

- **4208**: Publisher/Subscriber feature
- **4210**: Web Socket server feature

ADX name and address changes

The customer is responsible for notifying Johnson Controls of any changes to the ADX computer name. To avoid loss of data in OpenBlue Enterprise Manager, try to use a DNS name in the data collector setup when specifying the database connection to the ADX. If the ADX has a static IP on a network without DNS, you must update the data collector when this address is changed to ensure that there is no loss of data.

Updates and patch management

Updates, including but not limited to operating system, anti-virus and other built-in software, are the responsibility of the customer, as defined by their security and service standards. Johnson Controls is responsible for OpenBlue Enterprise Manager data collector software remotely through TeamViewer.

ⓘ **Note:** Windows Updates is set to off by default. You must apply Windows Updates on a monthly basis to ensure that the data collector software is up-to-date.

OpenBlue Enterprise Manager application access

You must access OpenBlue Enterprise Manager with a secure browser using the standard HTTPS protocol. You must authenticate yourself with a user ID and password.

Password standards

The password for the data collector is set to expire every 42 days by default. When you create a password for the data collector, you must ensure it contains the following password standards:

- Password length must be greater than or equal to 8 characters and lesser than or equal to 25 characters.
- Password must contain alphanumeric characters.
- Password must contain at least 1 upper case character.
- Password must contain at least 1 number.
- Password must contain at least 1 special character.

You must create a strong password. A strong password reduces the risk of a security breach in the data collector.

Logging and monitoring

OpenBlue Enterprise Manager creates log files to record issues that may occur. Johnson Controls staff monitor these log files, monitor OpenBlue Enterprise Manager servers, and support instances of OpenBlue Enterprise Manager with TeamViewer software.

Application logging

Application log information is available within the application user interface for administrators to monitor critical activity.

OpenBlue Enterprise Manager conducts additional application logging behind the scenes of the user interface for troubleshooting purposes. The Johnson Controls Data Center Operations team monitors logs for critical events.

Server monitoring

The Johnson Controls Development Operations team uses IT Brain to monitor server availability and performance. OpenBlue Enterprise Manager sends an automated alert to the team if there is any issue on the server.

Remote support

The Johnson Controls Development Operations team uses TeamViewer to access the OpenBlue Enterprise Manager data collector and provide remote support. TeamViewer uses secure port 443 to communicate and stores all access events in log files.

Related documentation

Table 1: Related Information

For information on	See document
OpenBlue Enterprise Manager	OpenBlue Enterprise Manager Product Bulletin, LIT-12012497
OpenBlue Enterprise Manager data collector	OpenBlue Enterprise Manager Data Collector Product Bulletin, LIT-12012343

Product warranty

This product is covered by a limited warranty, details of which can be found at www.johnsoncontrols.com/buildingswarranty.

Software terms

Use of the software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at www.johnsoncontrols.com/techterms. Your use of this product constitutes an agreement to such terms.

Patents

Patents: https://jcipat.com

Contact information

Contact your local Johnson Controls representative: www.johnsoncontrols.com/locations
Contact Johnson Controls: www.johnsoncontrols.com/contact-us