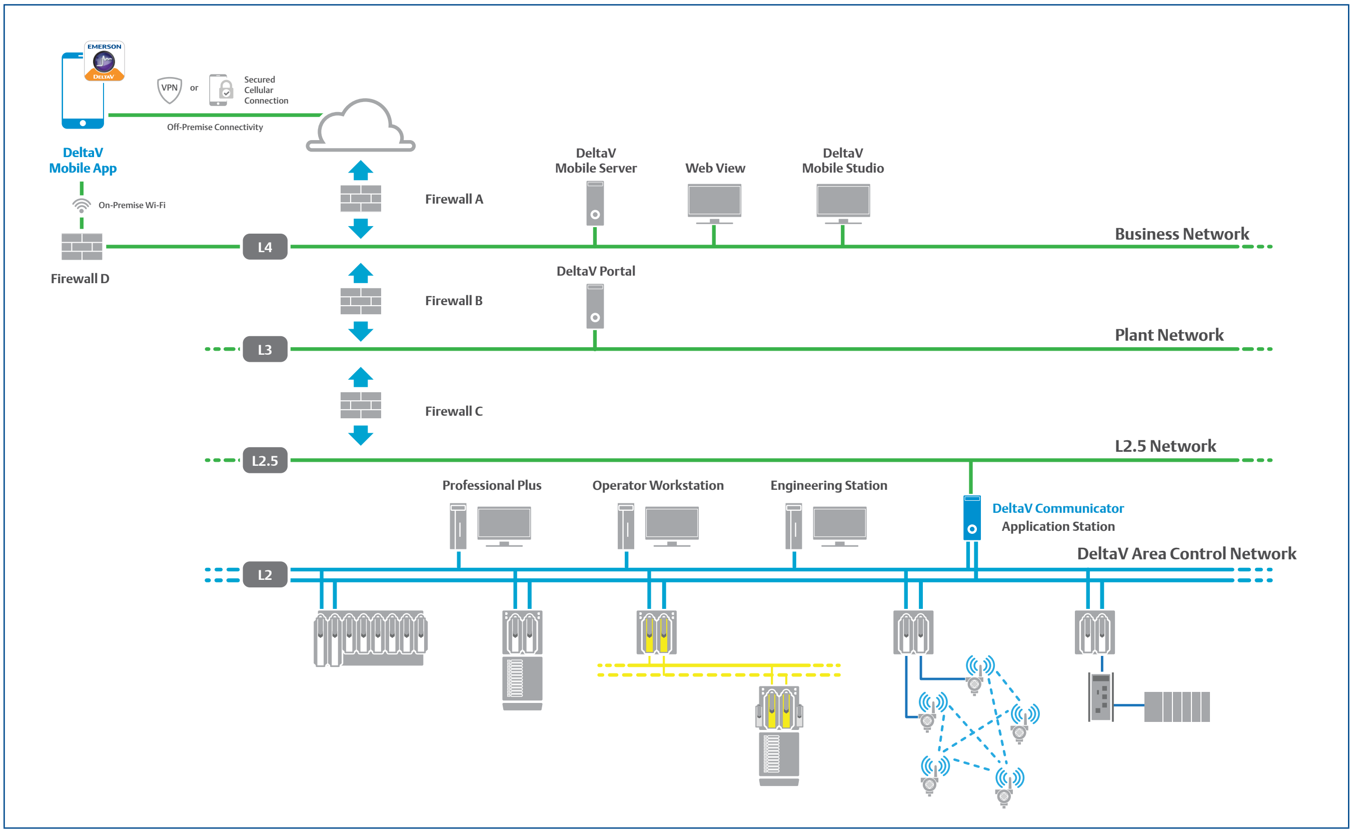
White Paper
May 2020

DeltaV™ Mobile Cybersecurity Brief

This document provides an in-depth overview of cybersecurity considerations for your DeltaV™ Mobile installation.



Introduction

DeltaV™ Mobile provides read-only access to process data and alarms on mobile devices. The solution includes a combination of software and hardware arranged within your existing network.

Network Security

DeltaV Mobile is deployed using multiple network layers, with firewalls segmenting each layer of the network and communication always occurring between adjacent layers. Access to each level in the architecture is isolated by firewalls, necessary Authentication, Authorization, and Accounting (AAA), and layered security.

The **DeltaV Mobile App** connects to the DeltaV Mobile Server to view real-time process values and alarms. On-premise access may be granted via your existing local Wi-Fi using HTTPS protocol over a user-configurable port (default 44155). This connection is encrypted with Transport Layer Security (TLS) supported by Mobile Server's digital certificate. Off-premise access can be granted either using a self-managed Virtual Private Network (VPN) connection to the local network or through Emerson's secure off-premise access solution. The self-managed VPN option is commonly enabled by corporate Information Technology (IT) through Mobile Device Management (MDM) enrollment; this allows company-provided or company-managed devices to access the corporate network resources. As an alternative, Emerson can provide a dedicated reverse proxy solution which enables secure off-premise access without opening another port on the firewall or making changes to your corporate network infrastructure. This secure off-premise access is facilitated through Microsoft Azure Relay™. For more information, refer to our extended whitepaper entitled DeltaV Mobile Cybersecurity Overview and Microsoft's documentation: **https://docs.microsoft.com/en-us/azure/service-bus-relay/relay-what-is-it**.

Table 1. Inbound connections required from mobile devices to DeltaV Mobile Server.

Firewall D	Level 4 Node	Wi-Fi node	Protocol	Port
⇕	DeltaV Mobile Server	Mobile Devices	HTTPS	44155*

*Note: * user-configurable port.*

DeltaV Mobile notifications can be sent to users via email, SMS text messages, or mobile push notifications. For email or SMS text messages, a SMTP email server may be used, which utilizes port 25 by default, as indicated in Table 2.

To receive mobile push notifications, an outbound connection must be permitted to Microsoft's Azure Notification Hub (no Wi-Fi or VPN is required for mobile devices to receive push notifications). The end user does not need an Azure account, and no customer data is stored in Azure. Optionally, when enabling secure off-premise access (without VPN) the same outbound port 443 is used.

Table 2. Firewall connections required for notifications to mobile devices or Emerson-provided Off-Premise Access without VPN

Firewall A - Level 4+	Level 4 Node	WWW	Protocol	Port
⇕	DeltaV Mobile Server	Azure Notification Hub Azure Relay	HTTPS	Outbound 443
	SMTP Email Server	Recipients' email server	SMTP	Outbound 25 (default)

On the Business Network (Level 4), the **DeltaV Mobile Server** handles mobile session authentication and serves data to the mobile device, which can be registered within your existing Mobile Device Management (MDM) solution and authenticated using your existing Active Directory credentials. **DeltaV Mobile Studio** is a browser-based HTML5 application for registering devices, configuring mobile lists, and setting notification preferences. Clients launch DeltaV Mobile Studio by connecting to the DeltaV Mobile Server through an encrytped TLS connection, using the same inbound port as the mobile device (default 44155).

On the Plant Network (Level 3), the **DeltaV Portal** provides the intermediate connection between the data in the DeltaV System and the DeltaV Mobile Server. Connectivity between the DeltaV Mobile Server and the DeltaV Portal is restricted to be initiated by lower-level (higher trust) DeltaV Portal and encrypted with TLS which is supported by Mobile Server's digital certificate. To view read-only graphics on Internet Explorer, **Web View** clients initiate a session with DeltaV Portal, using TLS encryption supported by DeltaV Portal's digital certificate.

Table 3. Firewall connections required for data transfer from the DeltaV Portal to the DeltaV Mobile Server and Web View.

Firewall B - L3 to L4	Level 3 Node	Level 4 Node	Protocol	Port
	DeltaV Portal	DeltaV Mobile Server	TCP	28130 (inbound to Mobile Server)
	DeltaV Portal	Web View	TCP	58022 (inbound to Portal)
	DeltaV Portal	Web View	HTTPS	443 (inbound to Portal)
	DeltaV Portal	Web View	TCP	3000 (inbound to Portal)

On the Process Control Network (Level 2), the **DeltaV Communicator** is a software application designed to run on your DeltaV Application Station, serving up read-only data for the DeltaV Portal. The DeltaV Portal can connect to multiple DeltaV Systems and other OPC data sources.

Table 4. Firewall connections required for DeltaV Portal information sources.

Firewall C - L2 to L3	Level 2 Node	Level 3 Node	Protocol	Port
	DeltaV Communicator	DeltaV Portal	TCP	58012 (inbound to Communicator)
	DeltaV Communicator	DeltaV Portal	HTTP	58080 (inbound to Communicator)
	OPC data source	DeltaV Portal	OPC DA, OPC HDA	135 (initial request port)

The DeltaV Portal can also connect to non-DeltaV OPC data sources by using OPC Classic (OPC DA for real-time data and OPC HDA for historical data). If a firewall is utilized when connecting to these sources, the port 135 is the initial request port for OPC Classic. The negotiated port can extend across a wide range of ports. This can be automatically managed by the Emerson Smart Firewall.

User Authentication

Users on mobile devices must pass two-factor authentication before they are allowed to connect. As a first factor, the user must be authenticated either locally by the Mobile Server, or preferably through Active Directory™ in a domain. DeltaV Mobile users do not need an additional Active Directory account; they can use their existing enterprise login. As a second factor, the mobile devices must be registered with the DeltaV Mobile Server and are subsequently validated against a device whitelist by their Mobile Device ID.

Once the user has been authenticated and the mobile device has been validated, the mobile app is ready to transfer data. All transferred data is TLS encrypted using a certificate that is provided by the DeltaV Mobile Server. The use of certificates to secure communication is discussed in more detail in the separate white paper entitled "Digital Certificates 2for Web-Based DeltaV Applications".

The principles and features followed in design and implementation of this product are presented for your consideration of cybersecurity risks. Applying these principles and features does not guarantee that your DeltaV system is secure from cyberattacks, intrusion attempts, or other undesired actions. Users are solely and completely responsible for their control system security, practices, and processes.

Emerson
North America, Latin America:
☎ **+**1 800 833 8314 or
☎ **+**1 512 832 3774

Asia Pacific:
☎ +65 6777 8211

Europe, Middle East:
☎ +41 41 768 6111

🌐 **www.emerson.com/deltav**

EMERSON™