

DeltaV™ Mobile Network Architecture Considerations

This document provides an initial overview of network architecture considerations for your DeltaV™ Mobile installation.



Table of Contents

- Introduction** 3
- Network Topology** 3
- Integration with PK Standalone** 6
- Information Sources** 7
- Mobile Device Connections** 8
 - On-premise 8
 - Off-premise 9
- Notification Options** 10
 - Native mobile push notifications 10
 - Email notifications 11
 - SMS text notifications 12

Introduction

DeltaV Mobile provides operations personnel and managers with access to process and production data from mobile devices. DeltaV Mobile users can monitor real-time process and diagnostic values, along with their historical data in touch-friendly trends. Additionally, users can view personalized lists of alarms and even receive notifications. The mobile application is primarily focused on two views:

1. Watch List: a collection of tags that the user wants to monitor.
2. Alarm List: a collection of alarms based on filter criteria such as process hierarchy, functional classification, priority, and alarm state.

DeltaV Mobile builds on and extends the DeltaV Executive Portal platform. For viewing web-based displays, Internet Explorer is required. In addition to supporting web-based displays on Windows PC or tablets, the overall platform now supports viewing data and alarms on mobile devices. DeltaV Mobile supports iPhone (iOS 9 and above) and Android (Lollipop and above) mobile devices.

DeltaV Systems act as data sources for DeltaV Mobile. To enable these data sources, you must install a software component (DeltaV Communicator) to enable the communication of process data and alarms.

The DeltaV Mobile installation package contains the following:

- DeltaV Mobile Server installation media
- DeltaV Portal installation media
- DeltaV Communicator installation media
- DeltaV Display Export tool
- Software license bundle

This document provides a description of the architecture and deployment options for DeltaV Mobile. It also details mobile device access and notification options.

Network Topology

DeltaV Mobile may be installed as either a 2-tier or a 3-tier topology. The 3-tier topology is shown in Figure 1, and the 2-tier topology is shown in Figure 2. A multi-level topology provides flexibility which may be utilized, as required by site policies, to restrict mobile device access.

The **DeltaV Mobile Server** provides access to data from the actual mobile device app (e.g., iPhone or Android app). It also provides access to the DeltaV Mobile web-based configuration application, **DeltaV Mobile Studio**, which is used to configure DeltaV Mobile watch lists, alarm lists, and notifications.

The **DeltaV Portal** is used to manage connections to one or more DeltaV Systems or OPC sources. It also manages users and licenses.

The lowest layer of the topology is the DeltaV Communicator. The **DeltaV Communicator** is installed on either a DeltaV Application Station or DeltaV Professional Plus. It supports native connections to either the DeltaV Continuous Historian or the DeltaV Advanced Continuous Historian. The DeltaV Communicator provides read-only access to DeltaV real-time process data, historical data, and alarms. A single DeltaV Portal can connect with up to 10 DeltaV Systems. This assumes each DeltaV System has a configuration (.fnx) file size of 1-2GB. More or less than 10 DeltaV System connections can be supported depending on these file sizes.

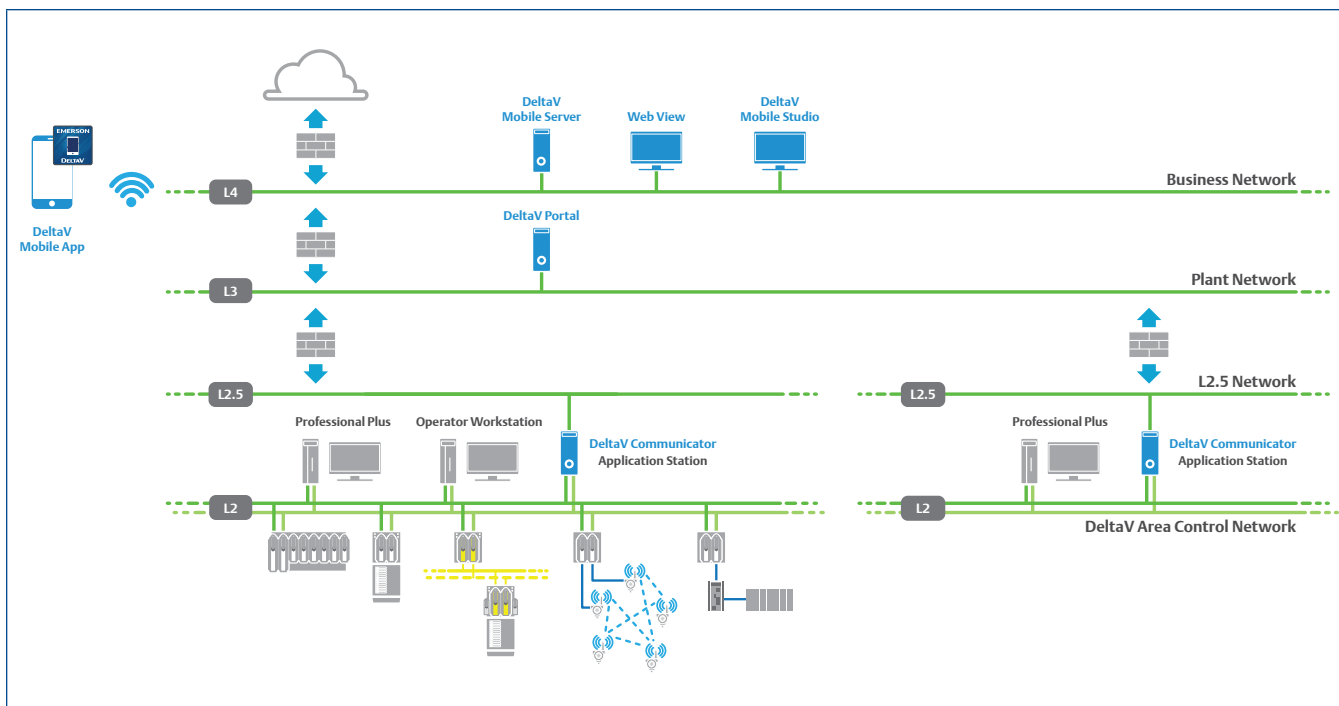


Figure 1. The 3-tier topology installs the DeltaV Mobile Server separately from the DeltaV Portal.

In the 2-tier topology, the DeltaV Mobile Server and the DeltaV Portal are both installed at the same level of the network topology, presumably on the same server, although this is not required.

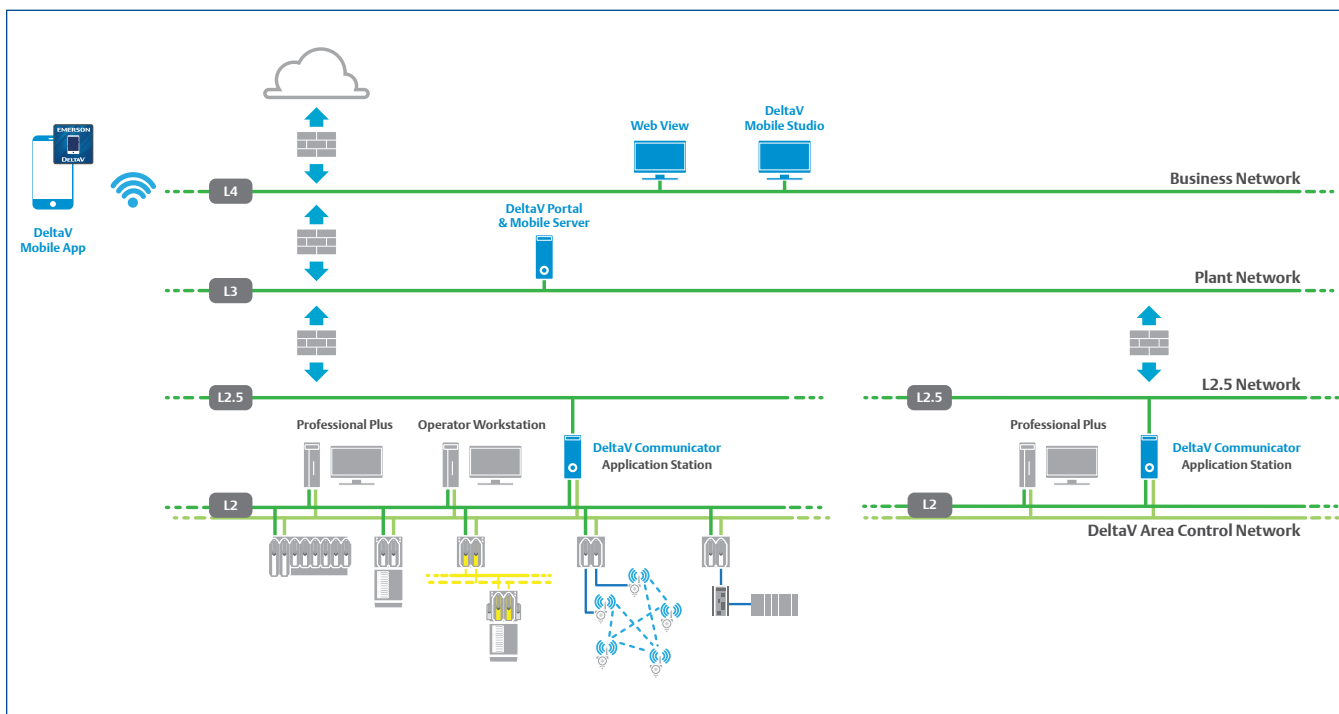


Figure 2. DeltaV Mobile 2-tier topology combines the DeltaV Mobile Server and DeltaV Portal on the same network level.

As a third option, DeltaV Portal can be co-deployed with the DeltaV Communicator when connecting to one DeltaV System, on either a DeltaV Application Station or DeltaV Professional Plus, provided that the Operating System requirements are met (e.g., Server 2016). This option is depicted in Figure 3.

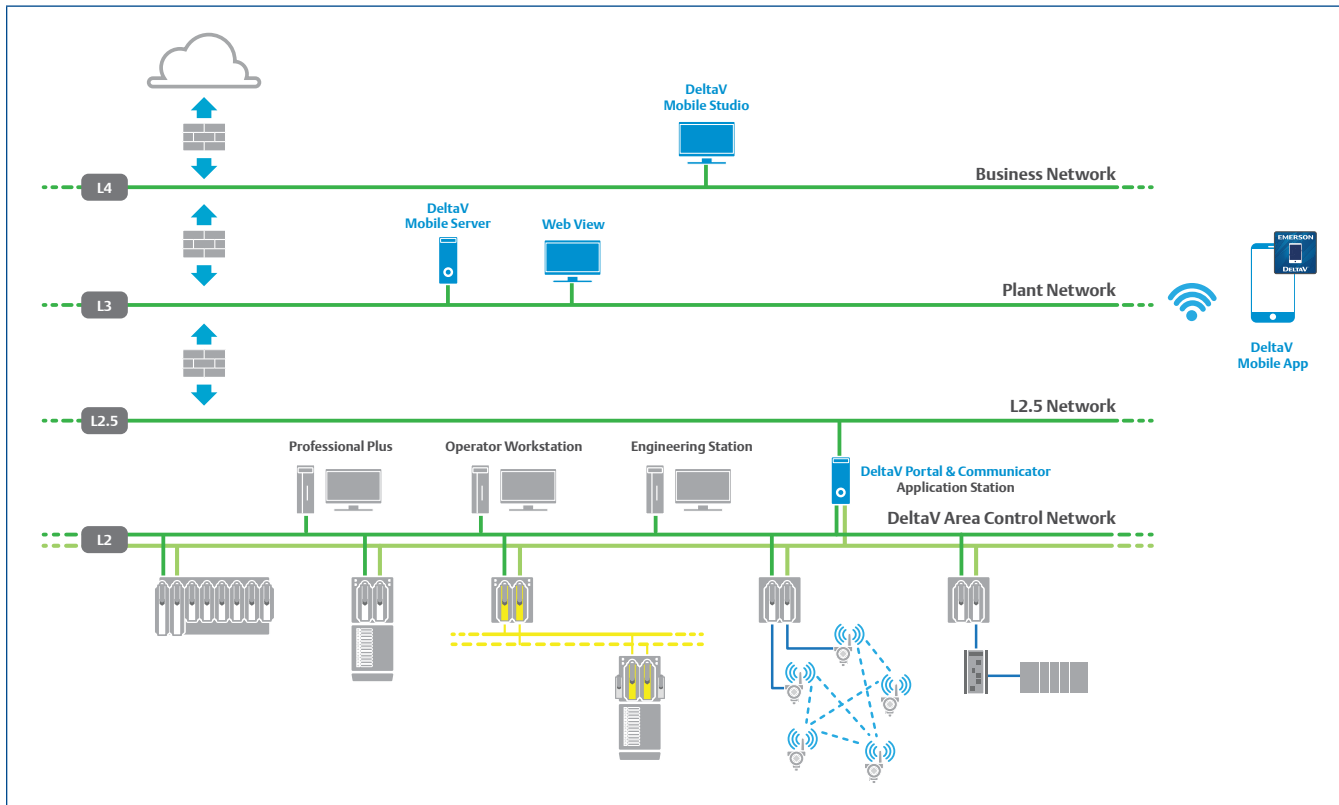


Figure 3. A third DeltaV Mobile supported architecture for DeltaV v13.3.1 and newer.

Integration with PK Standalone

DeltaV Mobile can also integrate with the DeltaV PK Standalone Operator Panel. Simply deploy the DeltaV Communicator on your Operator Panel, and connect this to a DeltaV Portal. This allows users to receive notifications and view real-time process values and trends from the Standalone PK controller to their mobile devices.

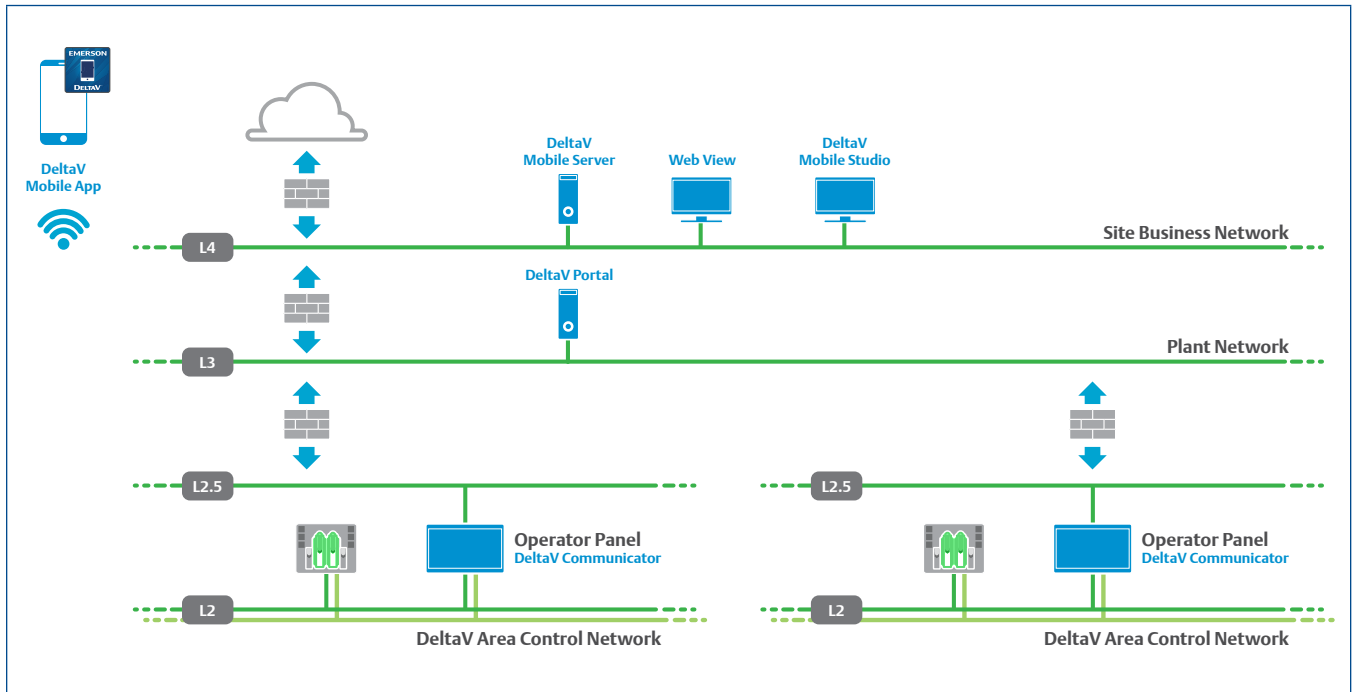


Figure 4. This architecture diagram depicts how DeltaV Mobile can connect to standalone PK controllers.

Information Sources

DeltaV Portal supports multiple information sources, including DeltaV Systems and OPC Servers. The DeltaV System information source delivers alarms, real-time process values, and historical process values to the DeltaV Mobile platform. Currently, the DeltaV Portal supports up to ten DeltaV System information sources.

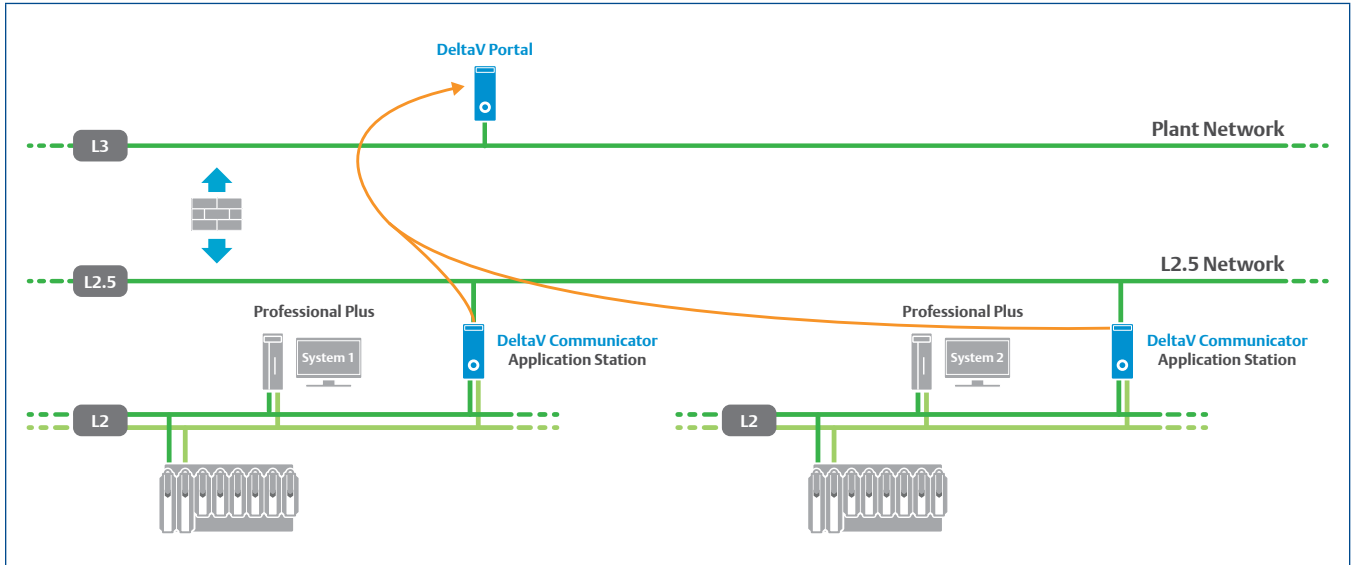


Figure 5. Multiple DeltaV System information sources combine into one DeltaV Portal.

Supported OPC information sources include real-time OPC DA and historical OPC HDA servers. With these information sources, you can expand your DeltaV Mobile platform to consolidate relevant information across multiple vendor systems and sources of data.

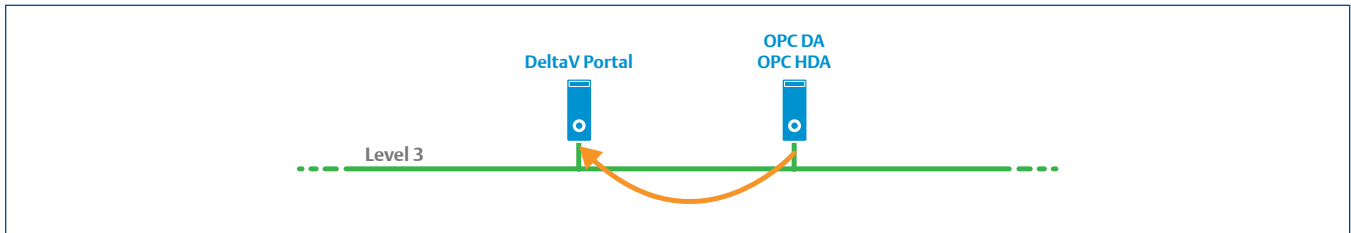


Figure 6. DeltaV Portal can accept OPC DA and OPC HDA information sources.

Mobile Device Connections

Mobile devices must connect to the DeltaV Mobile Server to view alarms and process values. This connection uses HTTPS over a user-configurable port (default port 44155).

On-premise

On-premise access is achieved using a local Wi-Fi network. No direct internet (WWW) connection is required.



Figure 7. On-premise mobile connection in a 3-tier topology, either by direct Wi-Fi access to the Level 4 network or through a Firewall.

In a two-tier topology, the local Wi-Fi can be established at either Level 3 or Level 4 of the network.

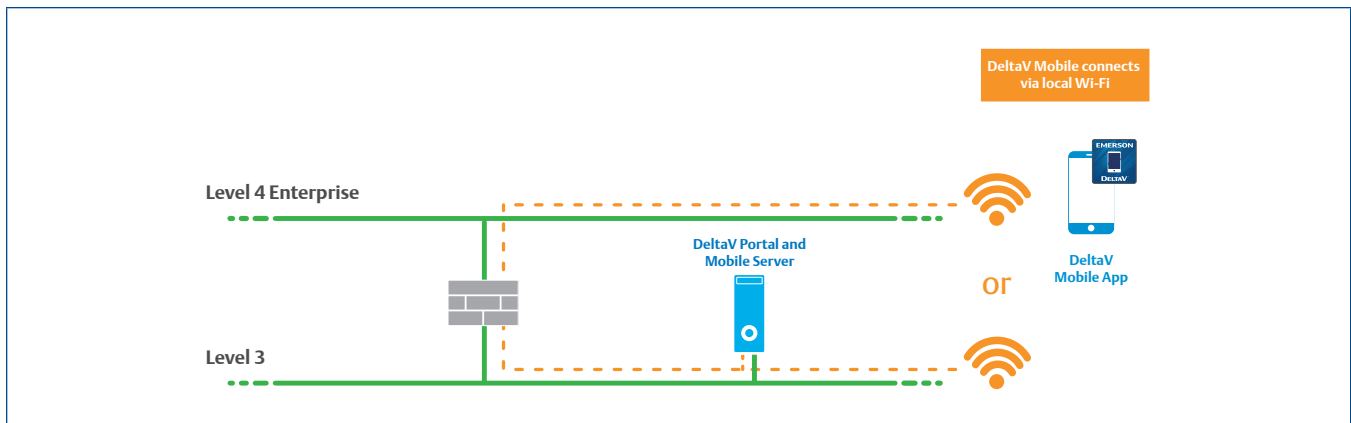


Figure 8. On-premise mobile connection in a 2-tier topology.

Off-premise

Option 1: Licensed off-premise access via cellular network

Emerson can provide off-premise access to DeltaV Mobile over a cellular network, without opening another port on the firewall or making changes to your corporate network infrastructure. The DeltaV Mobile App and your DeltaV Mobile Server communicate securely through a private relay connection. The DeltaV Mobile Server connects outbound to the cloud-based relay service, and all communications through the relay are encrypted. This optional cloud-enabled service does not require end-user management, and your process data remains private on the DeltaV Mobile Server.

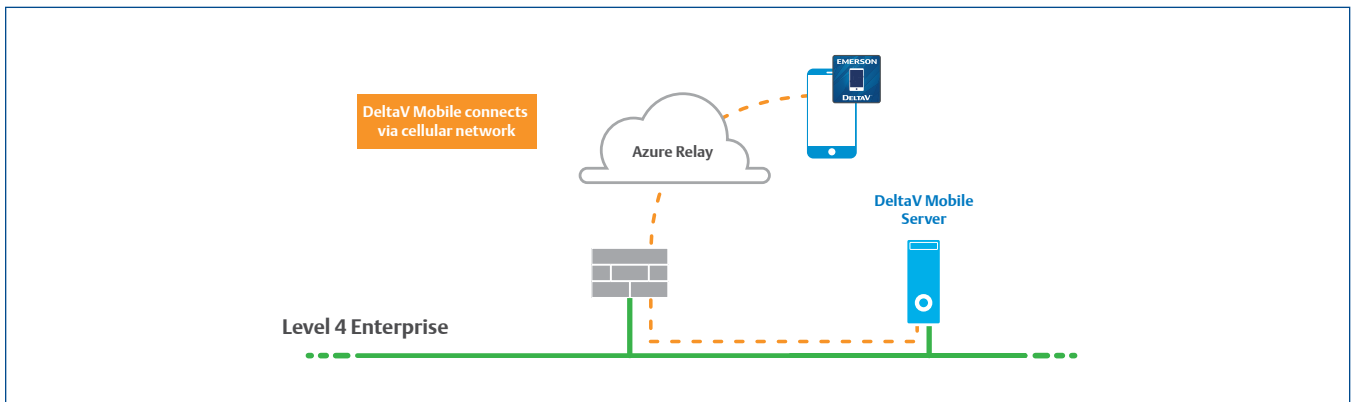


Figure 9. Licensed off-premise access via cellular network.

Option 2: Off-premise access through self-managed Virtual Private Network

Users can also access DeltaV Mobile while off-premise by using a self-managed VPN. The mobile device will need a VPN connection to resolve the DeltaV Mobile Server address.

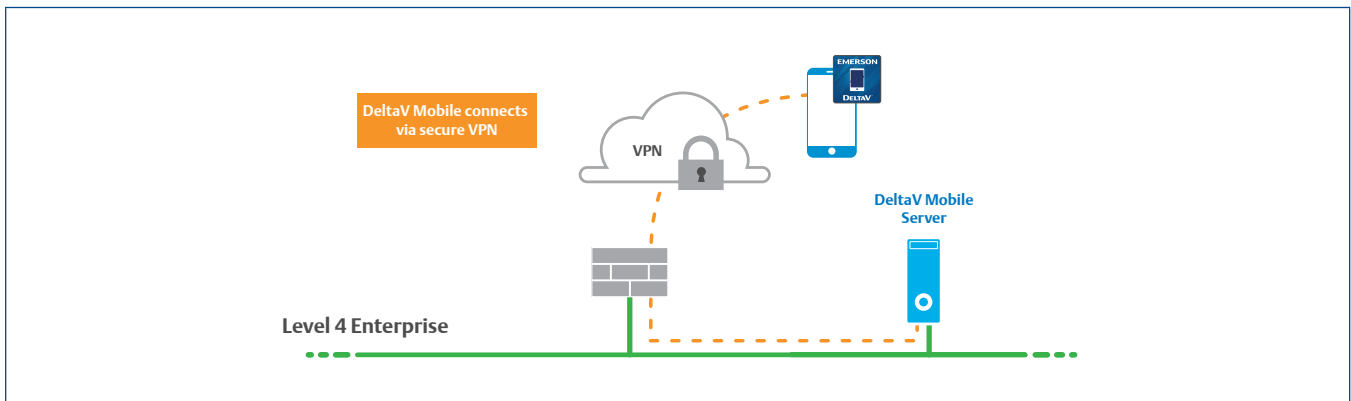


Figure 10. Off-premise mobile connection in a 3-tier topology.

Notification Options

Users can receive three different types of notifications:

- Native mobile push notifications
- SMS text notifications
- Email notifications

The following sections describe each of these notification options in more detail. For simplicity, the 3-tier topology is assumed in the diagrams below, but it is not required.

Native mobile push notifications

To receive mobile push notifications, the Mobile Server must be internet-facing. Mobile push notifications are directed through Microsoft's Azure Notification Hub. No Wi-Fi or VPN is required on the end-user's mobile phone to receive the notification. The end user and customer do not need an Azure account, and no customer data is stored in Azure. For details on Microsoft's security for Azure Notification Hubs, refer to: <https://docs.microsoft.com/en-us/azure/notification-hubs/notification-hubs-push-notification-security>.

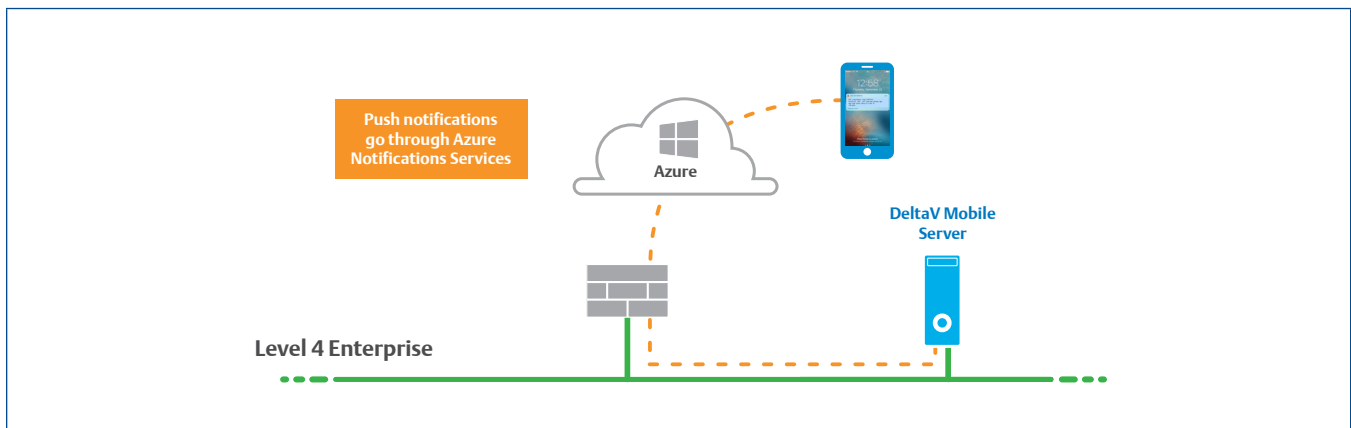


Figure 11. Native mobile push notifications go through Azure Notification Services.

Email notifications

The DeltaV Mobile Server does not require an internet connection in this scenario. From the built-in application, Notification Manager on the DeltaV Mobile Server, the user enters the IP Address of the local SMTP server. When the Mobile Server generates a new alert, it publishes this alert along with the required destination email addresses to the SMTP server which then emails this message to the respective end-users. There is no additional configuration required on the local SMTP server.

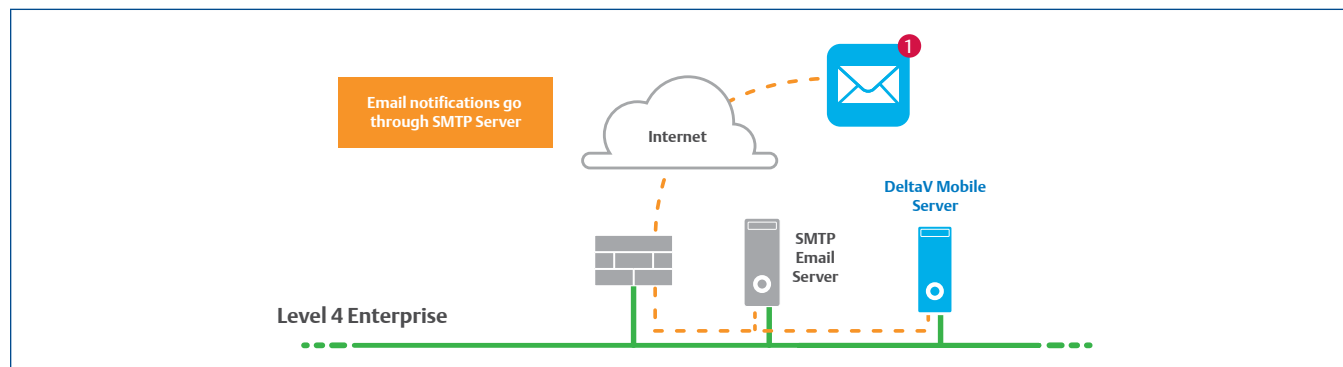


Figure 12. Email notifications are relayed through a local SMTP server.

SMS text notifications

SMS text notifications can also be achieved using a local SMTP server. In this scenario, the destination email address follows this format: number@txt.att.net where number is a 10-digit cellular phone number and txt.att.net is an example of a carrier's SMS to email gateway (i.e., AT&T).

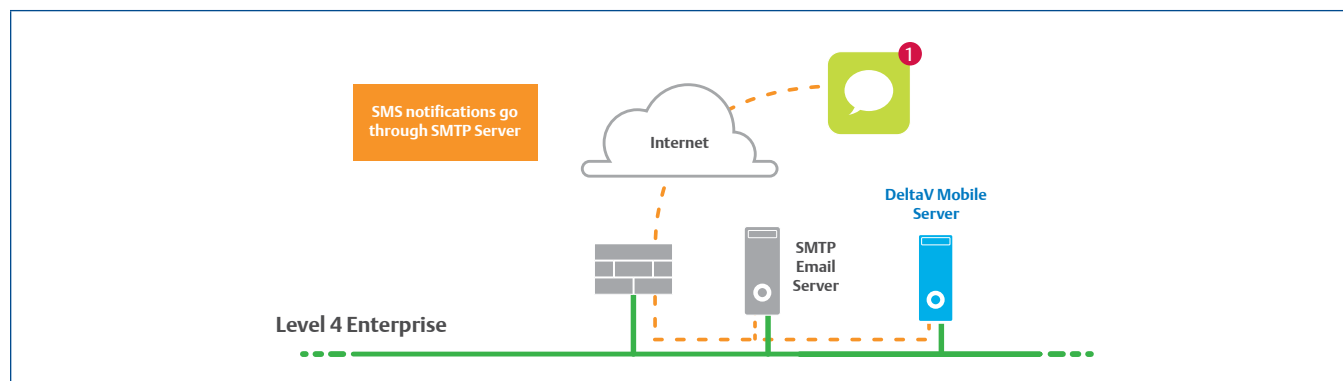


Figure 13. SMS notifications using SMTP server.

The Emerson logo is a trademark and service mark of Emerson Electric Co. The DeltaV logo is a mark of one of the Emerson family of companies. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while diligent efforts were made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.

Contact Us

🌐 www.emerson.com/contactus

