DeltaV™ Mobile Security Manual

This manual is Emerson confidential and intended for use only by customers, employees, Impact Partners, and others who are responsible for providing security services to Emerson systems and products. It may be provided to potential customers as required to evaluate DeltaV security implementation. It does not require an NDA for distribution.

This manual must not be posted on public websites or redistributed, except as noted above, without permission from Emerson.

Table of Contents

Introduction

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

For details on the architecture and deployment options, refer to a separate white paper entitled DeltaV Mobile Architecture Considerations. This manual assumes the split architecture, as depicted on the coversheet. An alternative collapsed architecture is also supported but not presented here. All security concepts presented are applicable to both options, but network security will inevitably have differences in implementation.

For details on the DeltaV Mobile solution, refer to the DeltaV Mobile Product Data Sheet.

Purpose

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

Glossary

Table 1. Glossary of Terms

Term	Definition
Confidentiality	Assurance that the entity receiving is the intended recipient (encrypt/decrypt)
Authentication	Proof that the entity is whom they claim to be (public/private key)
Integrity	Verification that no unauthorized modification of data has occurred (digital signatures)
Nonrepudiation	Assurance that the entity sending information cannot deny participation (digital signature)
Public key (digital) certificate	A certificate is a computer-generated object that ties the subscriber's identification with the subscriber's public key in a trusted relationship. The certificate contains a number of data elements like identification information, the name of the Certificate Authority (CA) issuing the certificate the name of the subscriber, and the subscriber's public key. The CA digitally signs all of the data elements in the certificate to bind the information to the subscriber in a form that can be verified by third (relying) parties that want to make use of the information in the certificate.
Certification Authority (CA)	The CA is a trusted entity responsible for identifying and authenticating entities and creating the digital certificates that bind the entities to the public key presented to the CA.
Active Directory Federation Services (AD FS)	Active Directory Federation Services provides simplified, secured identity federation and Web single sign-on (SSO) and access control across a wide variety of applications including Office 365, cloud-based SaaS applications, and applications on the corporate network. ■ For the IT organization, it enables you to provide sign on and access control to both modern and legacy applications, on premise and in the cloud, based on the same set of credentials and policies. ■ For the user, it provides seamless sign on using the same familiar account credentials. ■ For the developer, it provides an easy way to authenticate users whose identities live in the organizational directory so that you can focus your efforts on your application, not authentication or identity.

Network Security

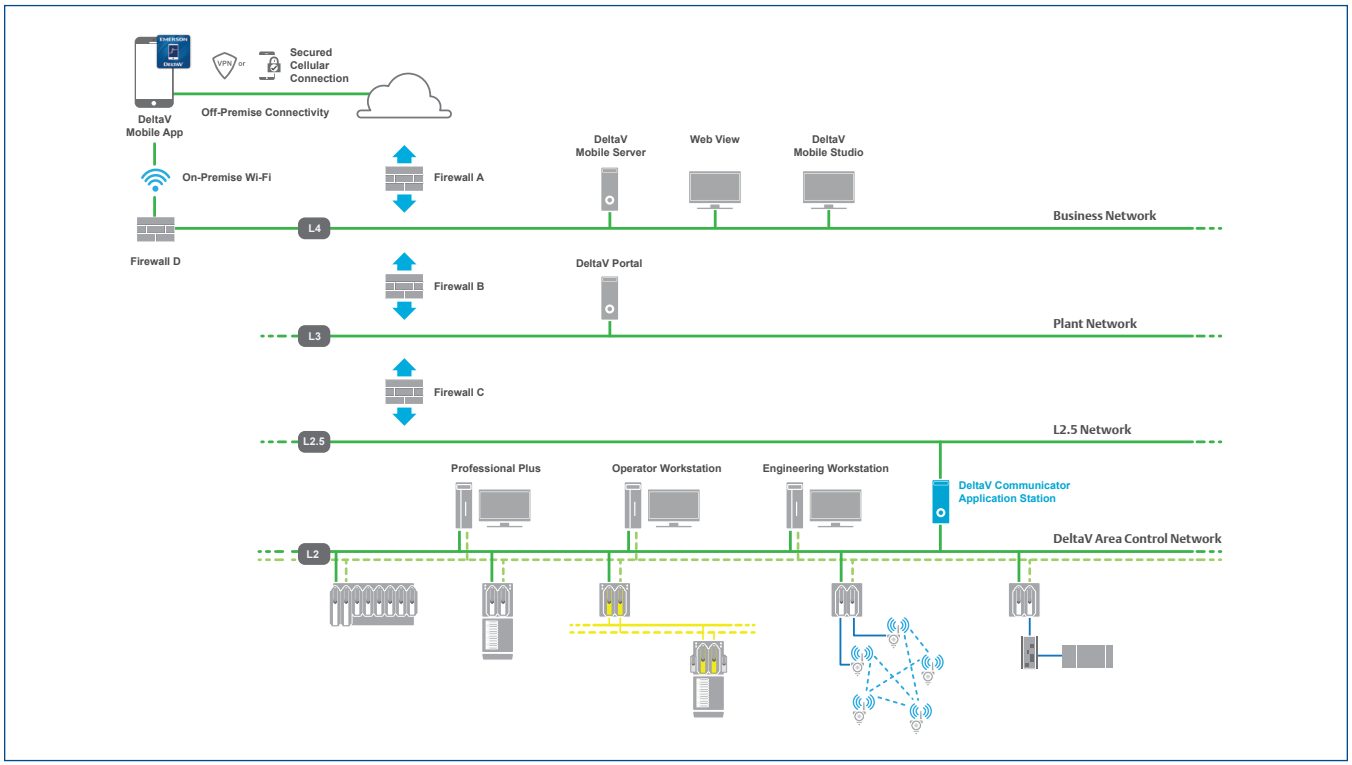


Figure 1. *DeltaV Mobile Network Topology.*

Network Topology

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 and Authorization-Audit (AAA), and layered security.

DeltaV Mobile notifications can be sent to users via email, SMS text messages, or mobile push notifications. For email or SMS text messages, an SMTP email server may be used, which utilizes port 25 by default, as indicated in Table 02. To receive mobile push notifications, an outbound connection must be permitted to Microsoft's Azure Notification Hub (no Wi-Fi or VPN required). The end user does not need an Azure account, and no customer data is stored in Azure. In order for public SMTP for Office365 to work, port 587 needs to be unblocked for the following address: smtp.office365.com.

Additional advice when using Office365 SMTP:

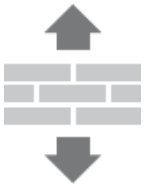
1. SMTP Auth must be enabled in order for the sending to Office365 to work. Reference on how to enable SMTP and SMTP Auth on the specific account:
   https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission
2. Office365 SMTP may not work properly in all cases if multi-factor authentication is enabled for the account.
   a. User level settings:
   https://support.microsoft.com/en-us/account-billing/turning-two-step-verification-on-or-off-for-your-microsoft-account-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca

b. Enterprise-level settings:

https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication

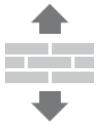
3. Refer to the “smtp.office365.com” section of the following page for additional rules that may need to be placed on the firewall:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

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	Off-Premise Access relay	HTTPS	Outbound 443
	DeltaV Mobile Server	Azure Notification Hub	HTTPS	Outbound 443
	SMTP Email Server	Recipients’ email server	SMTP	Outbound 25 (default) (Outbound 587 for Office 365 SMTP)

The DeltaV Mobile App connects via your existing local Wi-Fi to the DeltaV Mobile Server on the Business Network (L4) using HTTPS protocol over a user-configurable port (default is port 44155). This connection is encrypted with Transport Layer Security (TLS) supported by Mobile Server’s digital certificate. Off-site access can be granted using the Emerson-provided Off-Premise Access capability through outbound port 443 from the DeltaV Mobile Server. Alternatively, off-site access can be granted using a secure VPN connection to the local network.

Table 3. Inbound connections required from mobile devices to DeltaV Mobile Server

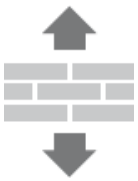
Firewall D	Level 4 Node	Wi-Fi node	Protocol	Port
	DeltaV Mobile Server	Mobile Devices	HTTPS	Inbound 44155*

*Note: * user-configurable port.*

On the Business Network (Level4) business network (Level 4), the DeltaV Mobile Server handles mobile session authentication and serves to the mobile device, which can be registered within your existing Mobile Device Management (MDM) solution and authenticated using your existing Active Directory credentials. Web View provides browser-based viewing of process displays and KPIs. Web View connections to the DeltaV Portal are encrypted with TLS which is supported by DeltaV Portal’s digital certificate. Similarly, DeltaV Mobile Studio is a browser-based HTML5 application for registering devices and configuring DeltaV Mobile users, watch lists, and alarm lists through an encrypted TLS connection with the DeltaV Mobile Server. All these assets can be members of the existing enterprise domain on Level 4.

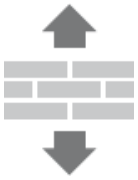
On the plant network (Level 3), the DeltaV Portal provides the intermediate connection between the data in the DeltaV System and the DeltaV Mobile Server. It can connect to multiple DeltaV Systems and other OPC data sources. Connectivity between the DeltaV Mobile Server and the DeltaV Portal is initiated by lower-level (higher trust) DeltaV Portal and encrypted with TLS which is supported by Mobile Server’s digital certificate. Conversely, encrypted Web View sessions are initiated by the Web View client requesting a session from the DeltaV Portal.

Table 4. Firewall connections required for data transfer from DeltaV Portal to 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 Server)
	DeltaV Portal	Web View	HTTPS	443 (inbound to Portal Server)
	DeltaV Portal	Web View	TCP	3000 (inbound to Portal Server)

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 5. 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)

OPC Classic Data Sources

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).

The Classic OPC data source type (which connects to an OPC Classic Server) uses DCOM. As such, when a firewall exists between the DeltaV Portal and the Classic OPC data source, you must open all ports as needed for DCOM communication. Classic OPC uses the following ports:

- Port 135 - used for initial connection negotiation (establishes the port to be used for the transaction).
- Ports between 1024 to 65535 - these are the possible ports reserved for DCOM.

This can be automatically managed by the Emerson Smart Firewall. If using an alternative firewall capable of monitoring port 135 for DCOM connection negotiation, configure a rule on the firewall to open the port based on that negotiation.
If your firewall is not capable of monitoring port 135 for DCOM connection negotiation, you must open all ports needed.
You can restrict the ports in the default range available to DCOM through the Windows operating system. The exact procedure varies based on the Windows operating system; therefore, refer to Windows Help for instructions.

Off-premise access

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.

Option 1: Emerson licensed secure off-premise access using a standard cellular connection

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™.

Key points:

a. The DeltaV Mobile Server can remain on-premise, and only requires an outbound connection via port 443 as defined in Table 3 above.

b. During setup, a private hyperlink is generated and shared with DeltaV Mobile users. This hyperlink allows the mobile device to communicate with a private instance of Azure Relay, instead of directly addressing the DeltaV Mobile Server on a private network.

c. Each DeltaV Mobile Server will connect to its own private instance of Azure Relay. Connections will not be co-mingled between customers.

d. Azure Relay does not store your DeltaV database or live process values. Rather, it acts as a reverse proxy to relay the communication traffic.

Option 2: self-managed VPN off-premise access

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 phones to access the corporate network resources. Emerson does not validate or recommend a specific VPN vendor for this connection. In this scenario, enabling VPN on a mobile device allows the device to communicate directly with an on-premise DeltaV Mobile Server.

Authentication and Authorization

Two-Factor Authentications

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 for Web-Based DeltaV Applications".

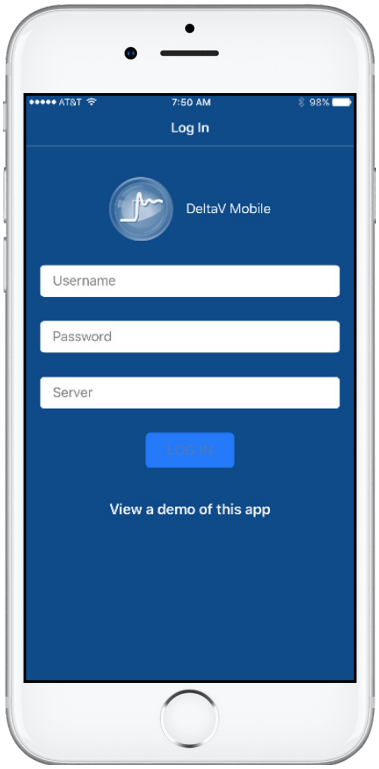


Figure 2. *DeltaV Mobile Log In screen.*

Device Registration

This section discusses the steps involved for device registration. Mobile device registration is a one-time process for the lifetime of the mobile device. The process would need to be repeated if the device is restored to factory settings.

Users are defined and permissions are granted in the **DeltaV Portal User Manager** to indicate that a user has permission to access DeltaV Mobile. The process of adding users is covered in a separate configuration document. The steps in the mobile device registration process are:

1. The user downloads the DeltaV Mobile app from the Apple App store or the Google Play store.
2. The user opens the DeltaV Mobile app and enters login credentials.
3. The user taps “Log In”.
4. The mobile app looks up the Device ID in the keychain for iOS devices. If this doesn’t exist, the mobile app generates one and stores it in the device’s keychain.
5. The mobile app sends the username, password, and Device ID to the DeltaV Mobile Server using encrypted TLS communication.
6. The DeltaV Mobile Server checks the username and password against the site’s Active Directory.
7. The DeltaV Mobile Server checks that the user is a DeltaV Mobile user. Permissions for the user are granted by a system administrator in the DeltaV Portal User Manager (detailed in a separate configuration document).
8. The DeltaV Mobile Server checks that the user’s device is registered to them. If the user is not registered to this device, a status is returned to the app indicating that the device is not registered for that user.

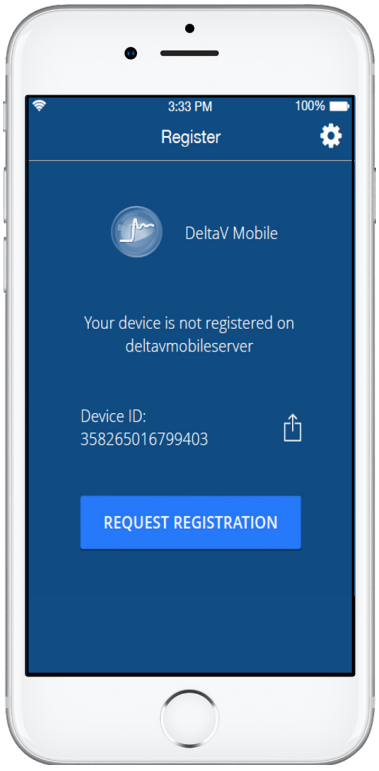


Figure 3. *Mobile device registration.*

9. The mobile app goes to the device registration screen where the user can request registration.
10. After the user requests registration, a user with “Can Configure/Can Administer” privileges can login to DeltaV Mobile Studio using a web browser to accept the device registration request, which maps the Device ID associated with the User ID and completes the device registration process. Details on DeltaV Mobile Studio security and encryption are provided in Section “DeltaV Mobile Security Overview”.
11. The user can now complete the login sequence. Once the device is registered and the user successfully logs in, this username, password, and server information are cached on the mobile device’s key chain in order to support single sign-on (SSO). The password expiration length is managed by the site’s Active Directory Domain Services (ADDS).

    At this point, mobile devices can now use DeltaV Mobile to view data. All transferred data is 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 DeltaV Mobile Security Overview”.

User Authentication and Authorization Sequence

The DeltaV Mobile authorization framework is based on AD FS 2016. OAuth 2.0 and OpenID Connect scenarios make use of the following components to make this possible:

- Active Directory Authentication Library (AD AL): collection of client libraries that facilitate collecting user credentials, creating and submitting token requests and retrieving resulting tokens.
- OWIN (Open Web Interface for .NET) middleware: Set of server-side libraries for protecting web applications and Web APIs with OpenID Connect and OAuth 2.0.

The authentication and authorization sequence support enabling multi-factor authentication between endpoints (i.e client and server components) and accessing control mechanisms to authorize users on the server components. The sequence for authorizing users is shown below in Figure 4.

The sequence works as follows:

1. The DeltaV Mobile client application makes a request to the authorization server in the DeltaV Mobile Server. This request over HTTPS includes the Device ID, domain, username, password for the user account, and the application ID URI for the web API. If the user hasn't already signed in or the user authentication with the provided credentials have failed, the user is prompted to sign in again.

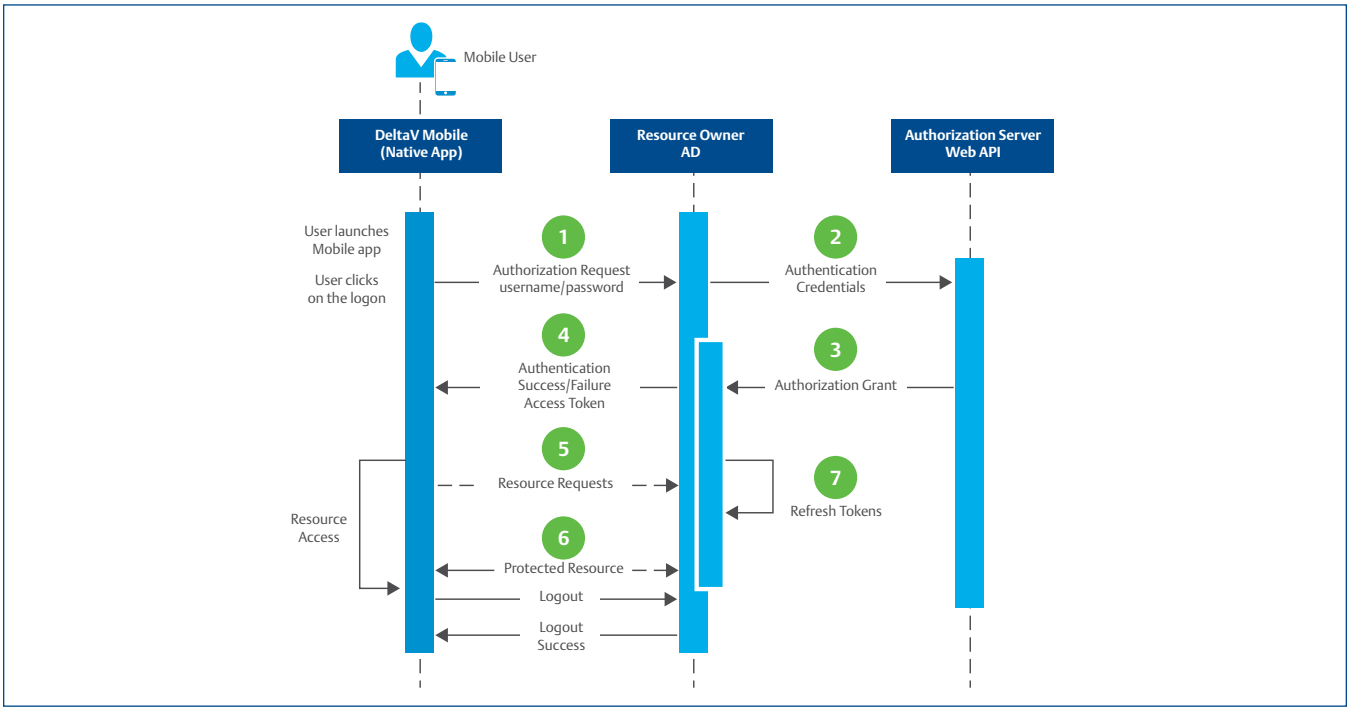


Figure 4. *DeltaV Mobile authentication sequence.*

2. The Authorization Server, which is also part of the DeltaV Mobile Server, authenticates the user against the Active Directory (AD).
3. Upon successful authentication, the AD issues an authorization code response back to the Web API resulting in an access token being generated for the user.
4. The Web API responds back to the DeltaV Mobile client application with the resulting access token over HTTPS. In the scenario that the authentication has failed, an appropriate error message is reported back to the user.
5. Over HTTPS, the DeltaV Mobile client application continues to make resource requests to the Web API until the user logs out from the application.
6. The Web API then validates the access token, and if validation is successful, returns the desired resource.
7. If the application has a valid access token, it can be used, refreshed, or renewed without prompting the user to sign in again. The Web API relies on the token refresh timers to keep the access token validated and active. When the access token expires, subsequent resource requests for the user will fail and the Web API will render an error message to the DeltaV Mobile client application. At that time, the user will be redirected to the Log In screen and prompted to authenticate again, which results in a new access token.

Watch Lists and Alarm Lists for Mobile Devices

Configuration of the mobile device watchlist and alarm lists is provided through a web-based HTML5 application called DeltaV Mobile Studio. These lists are cached on the DeltaV Mobile Server. The data for these lists originates from DeltaV Portal. DeltaV Mobile Studio communicates to the DeltaV Mobile Server using HTTPS over a user-configurable port, using TLS encryption. Access to the web interface uses HTTPS built on SHA2 web certificates, which can be self-signed or imported from a commercial Certificate Authority (CA). Similar to mobile devices, access privileges to DeltaV Mobile Studio can be controlled using DeltaV Portal User Manager.

Once the connection has been established, the DeltaV Portal collects data from the DeltaV Communicator and publishes data to the DeltaV Mobile Server. An example of a DeltaV Mobile watch list is shown below.

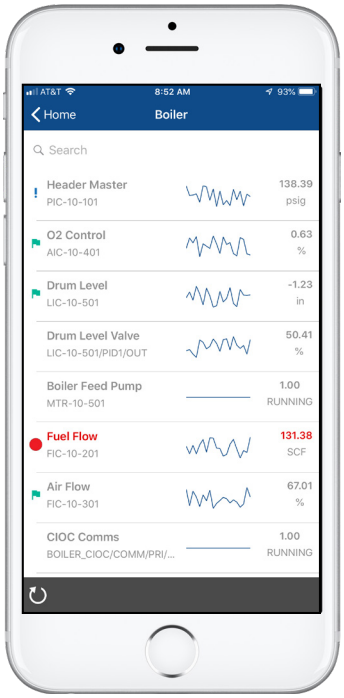


Figure 5. *Example of a DeltaV Mobile Watch List.*

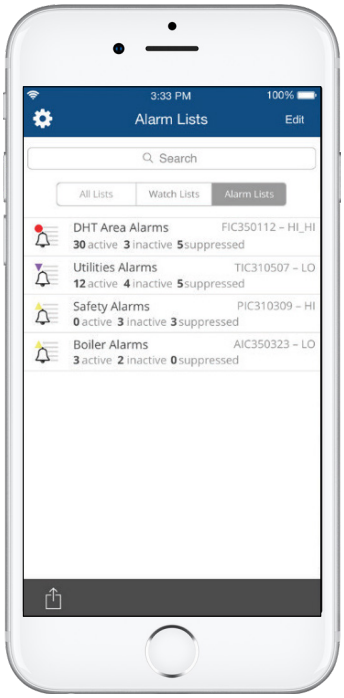


Figure 6. *Example of a DeltaV Mobile Alarm List.*

Least-Privilege Service Accounts

DeltaV Portal and DeltaV Mobile Server require Windows service accounts and user logins. The installation follows the principle of least-privilege access. Users logging into the DeltaV Portal or DeltaV Mobile Server should be authenticated to the site's Active Directory prior to being allowed access. A Workgroup environment is also supported. However, in Workgroup environments, local accounts have to be created in each server machine with the same credentials to allow the communications.

Table 05. Windows Service Accounts for DeltaV Portal and DeltaV Mobile Server.

Node	User	Type	Member of Groups
DeltaV Portal	EmersonService	Windows Service	Administrators EmServices Users
DeltaV Mobile Server	MobileService	Windows Service	Administrators EmServices Performance Monitor Users Users
DeltaV Communicator (Application Station)	Configurable / Custom	Windows Service, non-interactive DeltaV	DeltaV Operators

The DeltaV Communicator Service integrates with DeltaV on the Application Station. As part of the installation, a non- interactive DeltaV account with basic privileges is created. This account is a member of the Basic Operator group (i.e. a built-in roles-based access group with low privileges). If the account already exists, then the account is converted to non-interactive. This account should not be assigned any DeltaV keys (i.e. additional privileges).

Security Hardening

Operating System Hardening

Multiple Windows operating systems are supported for the DeltaV Portal and DeltaV Mobile Server. It is recommended that the DeltaV Portal and DeltaV Mobile Server run on hardened operating systems.

For the DeltaV Communicator (and by exception for the DeltaV Portal when it is installed on a supported DeltaV workstation), Emerson prescribes and applies security hardening recommendations for the operating system in Knowledge Based Articles (KBAs) for DeltaV. These hardening recommendations align with CIS Benchmarks. In the case that DeltaV Portal or DeltaV Mobile Server is installed on an operating system that does not match a supported DeltaV operating system (e.g. Microsoft Server 2012), Emerson has not published specific security hardening guidelines and the user is recommended to follow CIS Benchmarks.

Alternatively, operating systems can be hardened following the site's best practices.

Password Complexity Requirements

Require passwords to meet the following complexity standards:

1. Must have at least one uppercase letter
2. Must have at least one lower case letter
3. Must have at least one number
4. Must have at least one special character
5. Minimum of 8 characters in length

Table 6 - Required Password Policy settings

Property	Value
Minimum password length	8 Characters
Password must meet complexity requirements	Enabled

Manually set the password policy to machines where the user credentials for mobile studio access resides (for non DeltaV node type only and not necessarily the portal machine).

DeltaV Mobile Setup

Node Type: DeltaV Node / Non DeltaV Node (most use)

Deployment:

- Two Tier – non DeltaV, portal and server in one machine
- Three Tier – non DeltaV portal and server are on separated machines
- One Box – DeltaV; variations of install:
  - Portal and communicator on Application Station or Professional Plus (not recommended)
  - Portal, Server and Communicator on Application Station or Professional Plus (not recommended)

For One box deployment (DeltaV node type) there is no need to apply the lockout threshold as it should be handled by the DeltaV settings already.

For Workgroup

Apply this to the machine where the user credentials reside (not necessarily the portal machine).

1. Go to **"Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy"**.
2. Set the password policy *(see settings from Table 6).*

For Domain

Apply this to the machine where the user credentials reside – in this case the domain controller

1. Navigate to Start – Administrative Tools – Group Policy Management.
2. Expand the relevant domain node. Right click Default Domain Policy and select Edit from the drop-down list.
3. Group Policy Management Editor opens.
   Navigate to Computer Configuration\Policies \Windows Settings \Security Settings \Account Policies \Password Policy.
4. Set the password policy *(see settings from Table 6).*

Account Lockout Threshold

Table 7 - Recommended Account Lockout Threshold Settings

Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Manually apply threshold to machines where the user credentials for mobile studio access resides (for non DeltaV node type only).

DeltaV Mobile Setup

Node Type: DeltaV Node / Non DeltaV Node (most use)

Deployment:

- Two Tier – non DeltaV, portal and server in one machine
- Three Tier – non DeltaV portal and server are on separated machines
- One Box – DeltaV; variations of install:
  - Portal and communicator on Application Station or Professional Plus (not recommended)
  - Portal, Server and Communicator on Application Station or Professional Plus (not recommended)

For One box deployment (DeltaV node type) - there is no need to apply the lockout threshold as it should be handled by the DeltaV settings already.

For Workgroup

Apply this to the machine where the user credentials reside (not necessarily the portal machine)

1) Go to **“Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy”**

2) Set the Account Lockout Threshold *(see settings from Table 7)*

For Domain

Apply this to the machine where the user credentials reside – in this case the domain controller

1) Navigate to Start – Administrative Tools – Group Policy Management.

2) Expand the relevant domain node. Right click Default Domain Policy and select Edit from the drop-down list.

3) Group Policy Management Editor opens. Navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy where three lockout policy settings listed.

4) To set the Account Lockout Threshold policy setting, right click it and select Properties from the drop-down list

5) Set the Account Lockout Threshold *(see settings from Table 7)*

Windows Updates and Security Patches

It is important that the site follow Microsoft security update recommendations to apply the latest Windows updates and security patches.

For the DeltaV Communicator residing on a DeltaV Application Station, Emerson tests and approves monthly Windows security updates which can be downloaded from Emerson through the Guardian Support Portal.

For the DeltaV Portal and DeltaV Mobile Server, it is recommended to align with the site's corporate standards to simplify and align patching responsibilities.

Internet Information Services (IIS)

Internet Information Services is used for Web View with DeltaV Portal. DeltaV Portal is fully compliant with CIS Benchmarks for Microsoft IIS 10 v1.0.0, released March 31, 2017.

SQL Server 2016

DeltaV Portal and DeltaV Mobile Server have implemented hardening recommendations for SQL Server following CIS Benchmarks for Microsoft SQL Server 2016 v1.0.0, released August 11, 2017.

Manually set the SQL Server port the machines that the DeltaV Mobile Server and Portal resides.

DeltaV Mobile Setup

Node Type: in most cases a Non DeltaV node

Deployment:

- Two Tier – non DeltaV, portal and server in one machine
- Three Tier – non DeltaV portal and server are on separated machines
- One Box – DeltaV; variations of install:
  - Portal and communicator on Application Station or Proplus (not recommended)
  - Portal, Server and Communicator on Application Station or Proplus (not recommended)

For Workgroup and Domain

Apply this to the machine where the DeltaV Mobile Server and Portal resides.

1. Open SQL Server Configuration Manager
2. On the left pane select **Protocols for MOBILEPORTCONFIG** under **SQL Server Network Configuration**.
3. On the right pane, right click on the **TCP/IP** and select **Properties**.
4. If it is not Enabled, enable it by setting the **Enable** property to **Yes** on the **Protocol** tab of the Properties window.
5. Navigate to the **IP Addresses** tab.
6. Under **IPAll**, set the TCP Port to your desired port. The port must not be used by other applications on your machine.
7. Press Apply when done.

Malware Protection

Antivirus and/or whitelisting software is highly recommended on the DeltaV Communicator (DeltaV Application Station), DeltaV Portal, and the DeltaV Mobile Server.

For the DeltaV Communicator residing on a DeltaV Application Station, the antivirus and whitelisting solutions approved for DeltaV Systems are recommended.

For the DeltaV Portal and DeltaV Mobile Server, it is recommended to align with the site's corporate standards to simplify and align the software management and patching responsibilities.

Backup and Recovery

It is recommended to perform regular backups and develop a recovery procedure to restore from these backups. DeltaV Mobile supports backup and recovery mechanisms to import and export server certificates. Real-time failover can also be applied when the nodes appear to be compromised.

Host-Based Firewalls

Host-based firewalls (also known as host-based intrusion prevention or HIPS) are highly recommended. Emerson recommends using Microsoft Windows Firewall enabled on the DeltaV Communicator DeltaV Portal and DeltaV Mobile Server. For the DeltaV Communicator, Emerson only approves the use of Windows Firewall on the Level 2.5 network of the DeltaV Application Station; do not enable the Windows Firewall for your Level 2 DeltaV Area Control Network.

Mobile Device Management

Emerson recommends that all mobile devices are managed by the asset owner's Mobile Device Management (MDM).

Figure 7. *Windows account lockout policy.*

DeltaV Mobile Studio

DeltaV Mobile Studio is an HTML5 web application which requires users to authenticate for access. Brute force attacks at logging into the web application can be prevented by enabling Windows account lockout policies. It is important to remember that by default, Windows account lockout policies are “Not Defined”. Figure 6 provides some recommended settings for your Windows account lock policy on DeltaV Mobile Server to protect the DeltaV Mobile Studio against brute force attacks.

Web & Phone Certificates

Certificate Management

Self-Signed Certificates

During installation, an option to generate and use a Self-Signed Certificates is provided for testing and commissioning of DeltaV Mobile. Self-Signed Certificates poses security risks and is not recommended for production use. Self-Signed Certificates can be generated by anyone and clients such as a browser can’t reliably validate the authenticity of such certificates. This can be an avenue for attacks such as Man in the Middle.

DeltaV Mobile Setup

Node Type: in most cases a Non DeltaV node

Deployment:

- Two Tier – non DeltaV, portal and server in one machine.
- Three Tier – non DeltaV portal and server are on separated machines.
- One Box – DeltaV; variations of install:
  - Portal and communicator on Application Station or Proplus (not recommended)
  - Portal, Server and Communicator on Application Station or Proplus (not recommended)

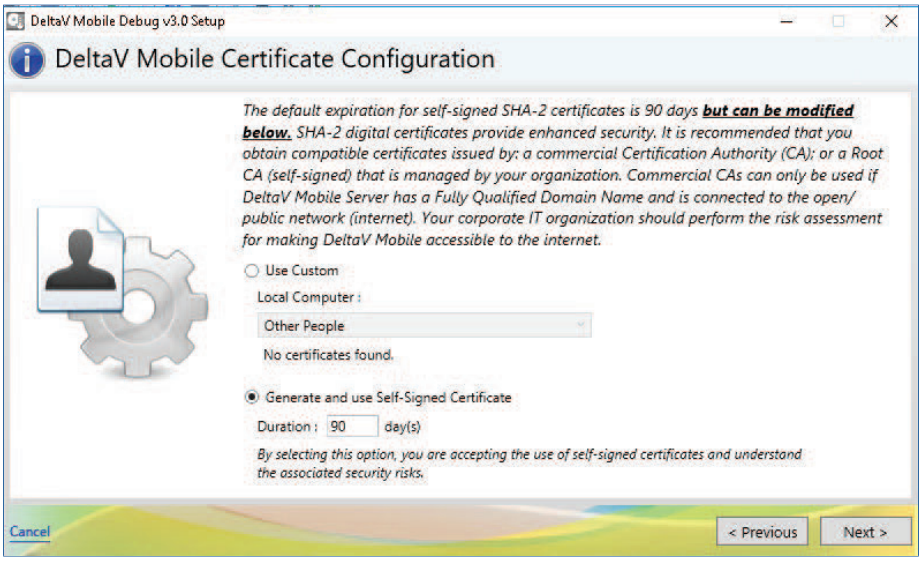


Figure 8. *DeltaV Mobile Certificate configuration.*

Certificates from CA or Root CA

For production, it is recommended to use a certificate signed by a commercial Certification Authority or a Root CA (self-signed) managed by your organization. Refer to the *Digital Certificates for Web-Based DeltaV Applications* whitepaper in Section 1 for the available options in deploying a Certificate Authority. Certificate requirements for DeltaV Mobile are detailed on KBA NK-1700-0153.

Figure 9. *During installation of DeltaV Mobile, it can be configured to use certificates installed on the server.*

Changing Certificates

To change the certificates used by DeltaV Mobile, the tool Certificate Configuration Utility can be used. This tool is included on the DeltaV Mobile installation and can be launched by running **C:\Program Files (x86)\Emerson\DeltaV Mobile\ ConfigCert.exe**.

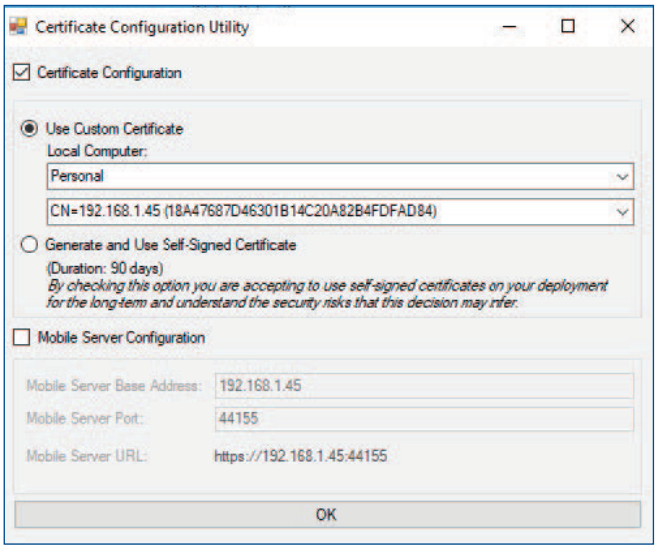
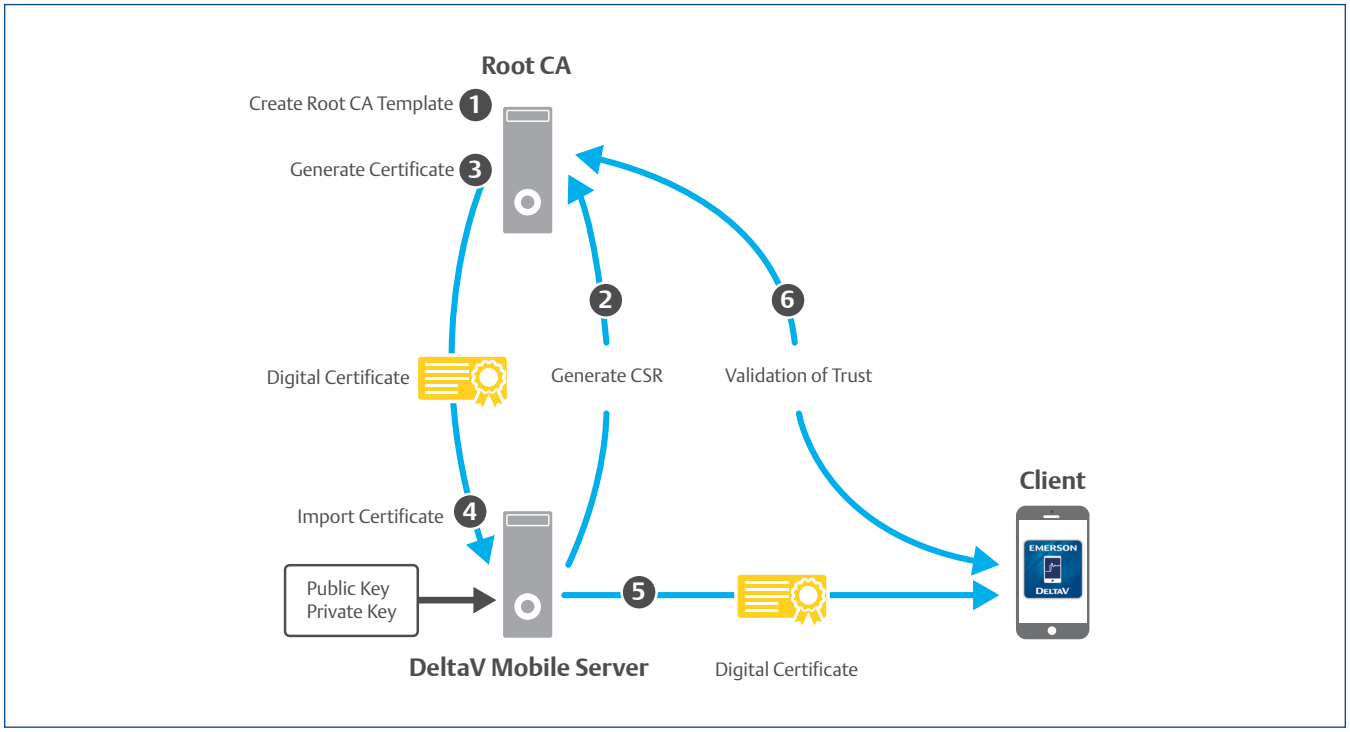


Figure 10. *Certificate Configuration Utility.*

Sample guide on how to create custom certificates for DeltaV Mobile using customer's Root CA.



Notes:

A. Steps provided below are to be used as a guide only.

B. Procedure may vary depending on Site IT's procedures, requirements, and architectures.

Main Steps:

1. Create template for DeltaV Mobile in CA server
2. Generate Certificate Signing Request (CSR) from the Mobile and/or Portal Server using the DeltaV Mobile template
3. Generate the certificate in the CA server based on the CSR
4. Import Certificate in the Mobile and/or Portal Server
5. DeltaV Mobile certificate is provided to client.
6. Certificate trust is validated with CA server

Detailed Steps

1. Create template for DeltaV Mobile in CA Server (The CA Server itself is typically deployed by IT).
   a. In order for the DeltaV Mobile app to work, the template must have the Basic Constraints enabled and must be CA (not End-entity). Typically, the Subordinate Certificate Authority and Root Certificate Authority templates have the CA extension, which is required for DeltaV Mobile. It is possible to use either the Subordinate Certificate Authority and Root Certificate Authority templates to create a separate and dedicated template for DeltaV Mobile.
   b. In addition to default settings of the Subordinate Certificate Authority and Root Certificate Authority templates, the template must have the following requirements:
      i. On Extension tab, ensure Basic Constraints is enabled and is a CA certificate (not end entity).
      ii. On the Private Key tab, on Key Options, ensure key size is 2048 and Make Private Key Exportable setting is selected.
      iii. On the Private Key tab, on Key Type, select Exchange.
      iv. The license validity must not exceed 285 days for iOS compatibility.
      v. Publish the DeltaV Mobile template to the Active Directory Enrollment Policy. This can take over an hour to complete.
2. Generate Certificate Signing Request (CSR) from the Mobile and/or Portal Server using the DeltaV Mobile template.
   a. In the Mobile or Portal Server, open MMC.
   b. Go to File>Add/Remove Snap-in.
   c. Select Certificates and click Add.
   d. Select Computer Account, click Next.
   e. Select Local Computer, click Finish, click OK.
   f. Expand Certificates, go to Personal, right click, select All Tasks>Advanced Operations>Create Custom Request.
   g. On Select Certificate Enrollment Policy, there should be an Active Directory Enrollment Policy under “Configured by your administrator”. Click Next.
   h. Select the DeltaV Mobile template. Note that the template may not appear if Step 1 was not completed correctly.
   i. Click the template’s dropdown arrow and select Properties.
   j. On the Subject tab, under Subject Name> Type, select Common Name. For the Value, type IP address or the hostname/FQDN (e.g. 192.168.0.1 or DVMobileServer or DVMobileServer.Emerson.local) and click Add.
   k. On the Subject tab, under Alternative Name, configure the following and click Add.

      IP Address = 192.168.0.1

      DNS Name = 192.168.0.1

      DNS Name = DVMobileServer

      DNS Name = DVMobileServer.Emerson.local

      IP Address = 127.0.0.1

      DNS Name = 127.0.0.1

l. On General Tab, type a Friendly Name to easily identify the certificate.

m. On Extension tab, ensure Basic Constraints is enabled and is a CA certificate (not end entity).

n. On the Private Key tab, on Key Options, ensure key size is 2048 and Make Private Key Exportable setting is selected.

o. On the Private Key tab, on Key Type, select Exchange.

p. Click OK. Click Next.

q. Save the CSR file to a desired location.

3. Generate the certificate in the CA server based on the CSR.

   a. Generate certificate in the CA server using the CSR provided.

   b. This might require a password to be set. It may also include other certificates needed in the certification path.

4. Import Certificate in the Mobile Server and/or Portal Server.

   a. Import certificate into Certificate Store.

      i. In the Mobile or Portal Server, Open MMC.

      ii. Go to File>Add/Remove Snap-in.

      iii. Select Certificates and click Add.

      iv. Select Computer Account, click Next.

      v. Select Local Computer, click Finish, click OK.

      vi. Expand Certificates, go to Personal or Trusted Root Certification Authorities, right click, select All Tasks>Import.

      vii. On Certificate Import Wizard window, click Next.

      viii. Browse for the PFX file and click Next.

      ix. Type the password, select “mark this key as exportable”, select “Include all extended properties”, click Next.

      x. Click next, click Finish. Click OK on the “Import was successful” message.

      xi. Select the certificate, right click, and select Open. Make sure the General tab, shows “You have a private key that corresponds to this certificate” and does not show any error on other tabs. Make sure Basic Constraints is available and is set to CA (Subject Type). Click OK.

   b. Import Certificate using ConfigCert.exe in Mobile and/or Portal server.

      i. Go to C:\Program Files (x86)\Emerson\DeltaV Mobile. Run ConfigCert.exe.

      ii. Select Certificate Configuration, use Custom Certificate, browse for the custom certificate and click OK.

c. Set Web View to use the certificate via IIS in the Portal Server.

   i. Open IIS Manager in the Portal Server, go to ServerName>Sites>Default Web Site. Select Bindings.

   ii. Select https, click Edit.

   iii. Select the Certificate, click OK.

   iv. Click OK. Click Close. Close IIS Manager.

5. DeltaV Mobile certificate is provided to client.

   a. This step occurs automatically when the user logs in via the DeltaV Mobile app.

   b. If the DeltaV Mobile certificate has parent certificates, it may be required to import the parent certificates in the device, if these are not already deployed with mobile device management software.

6. Certificate trust is validated with CA server

   a. This step occurs automatically when the user logs in via the DeltaV Mobile app.

   b. Note that this step assumes as a precondition that the CA server has been added as a trusted certificate authority on the client device (typically deployed by IT through mobile device management).

Secure Communications

The use of web certificates provides the means to encrypt and secure communications using Transport Layer Security (TLS). This is illustrated in Figure 11.

The DeltaV Mobile app to the DeltaV Mobile Server session is encrypted for data privacy and integrity. The security level of the TLS session is regulated by the cipher suites supported by the endpoints and negotiated during TLS session establishment.

It is recommended that the service connectivity relies on the identity validation of the service with a Public CA signed certificate with a verified chain of trust. The IP and port provided by the site's IT department are configured in DeltaV Mobile Server.

Guidelines for configuration, use, and TLS implementation are found in NIST Special Publication 800-52 Revision 1: *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.*

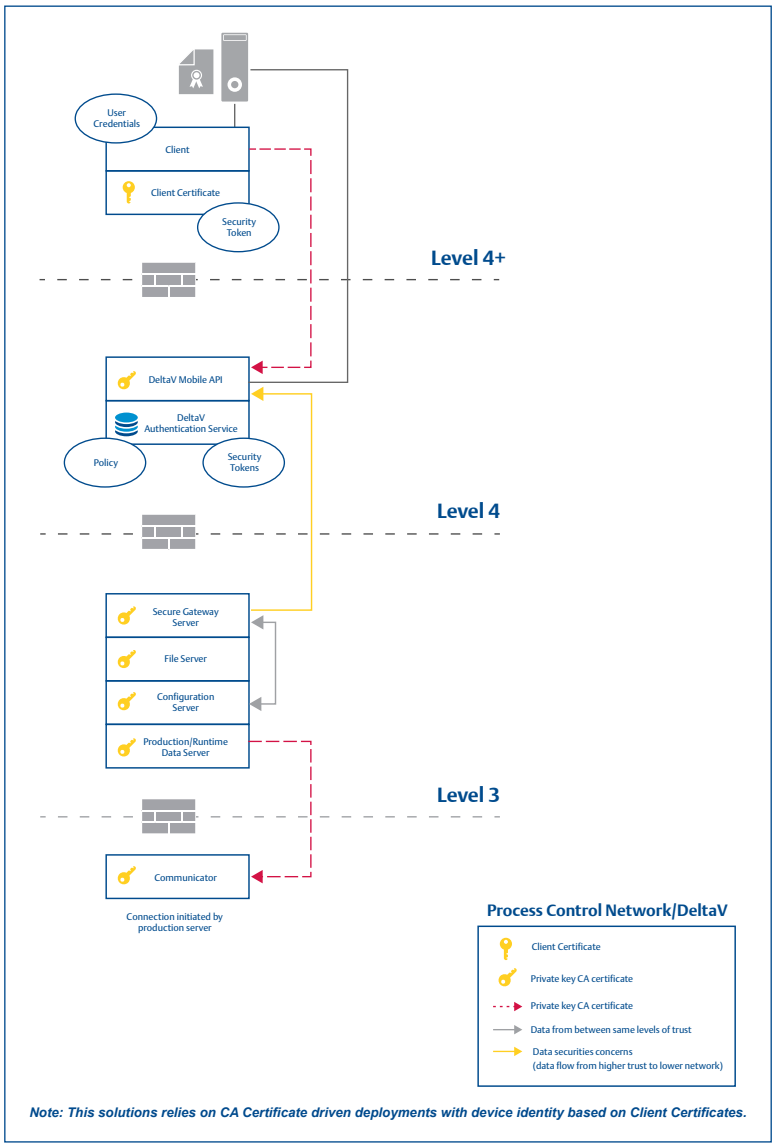


Figure 11. *Encrypted TLS communication using certificates.*

Certificate Installation for Android and IOS

Android

1. Login to the DeltaV Mobile app with valid credentials. A download notice will prompt when the certificate for the server is not yet installed (or has changed). Click “Install”. There might be a security prompt that will be shown, just enter your pin to continue to the installation. The security prompt will appear if the certificate of the server being connected to is not yet installed on the device. Once installed, the prompt won’t appear in succeeding logins. Take note of the Thumbprint for verification.
2. The certificate thumbprint is also shown on the prompt to allow the user to validate the thumbprint of the certificate they are installing. The thumbprint will identify the certificate of the server they are connecting to. Before installing the certificate, it is highly recommended for users to compare the certificate thumbprint shown on their device to the thumbprint of the certificate installed on the Mobile Server.

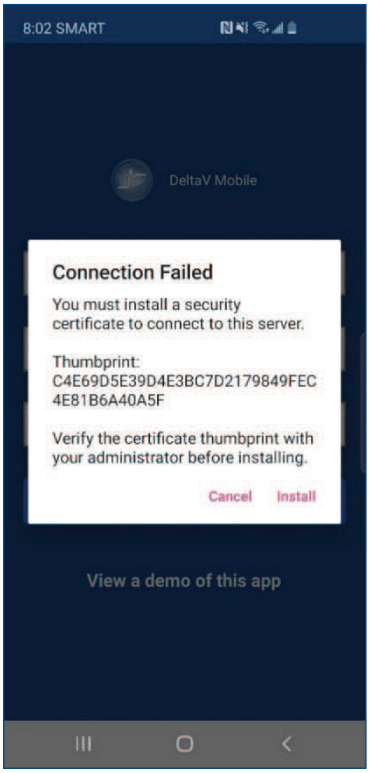


Figure 12. *Install certificate prompt on Android.*

3. The Certificate Installer app will be launched, enter a Certificate name then press ok.

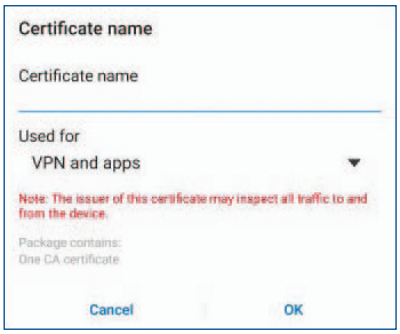


Figure 13. *Install certificate on Android*

4. Navigate back to DeltaV Mobile App then log-in as usual.

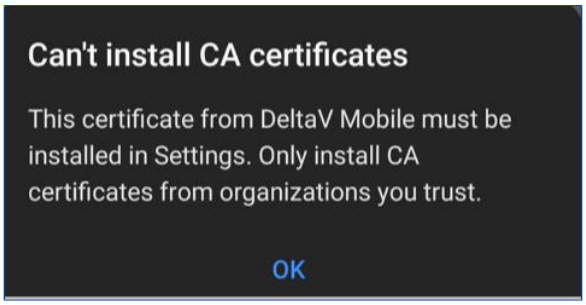


Figure 14. *Error message after trying to install the certificate*

5. Some users may experience an error message. Please note the following steps in the workaround. To work around this issue, copy and manually install the DeltaV Mobile certificates on Android11 devices:
    1. Copy/download the CER certificate to your Android 11 device (e.g. send the CER via email, then open the email in the Android 11 device, and download the CER).
    2. Go to Settings and search for Other Security Settings.
    3. Go to Install from device storage, select CA Certificate, and click Install Anyway.
    4. Enter the PIN, then select the certificate, and select Done.

iOS

1. Login to the DeltaV Mobile app with valid credentials. A download notice will prompt when the certificate for the server is not yet installed (or has changed). Click “Download Certificate”.

   The certificate thumbprint is also shown on the prompt to allow the user to validate the thumbprint of the certificate they are installing. The thumbprint will identify the certificate of the server they are connecting to. Before installing the certificate, it is highly recommended for users to compare the certificate thumbprint shown on their device to the thumbprint of the certificate installed on the Mobile Server.

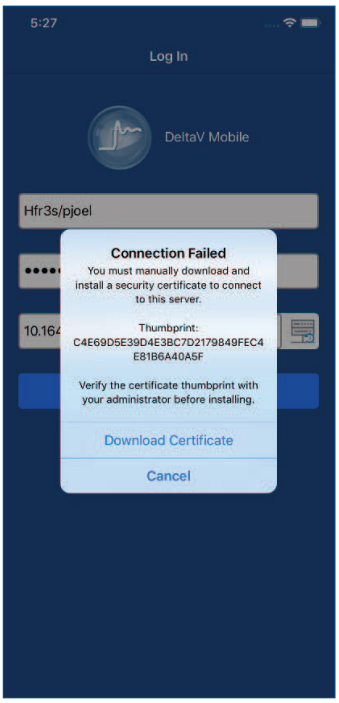


Figure 15. *Install certificate prompt on iOS.*

2. Safari App will open and will prompt you to download the certificate, click Allow. A Profile Downloaded Prompt will be shown.

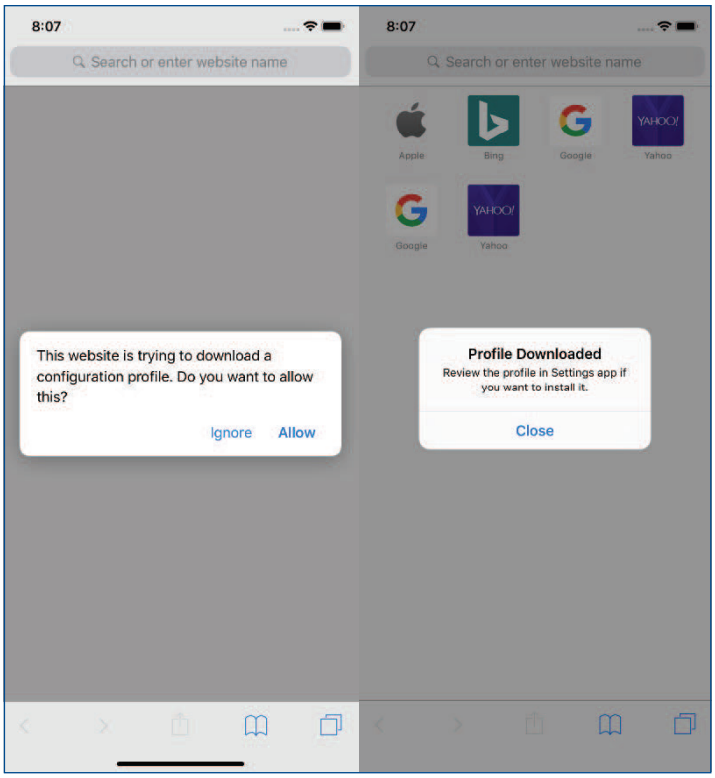


Figure 16. *Download certificate on iOS.*

3. Open the Settings app and click Profile Downloaded.

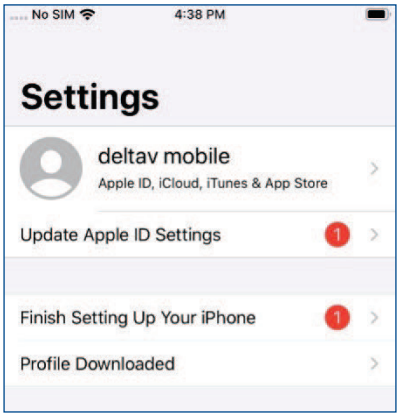


Figure 17. *Check profile on iOS.*

4. On Install Profile, click Install. Note: Authentication prompt might be seen to verify identity. To proceed just enter your pin (depends on the configured authentication on the device).

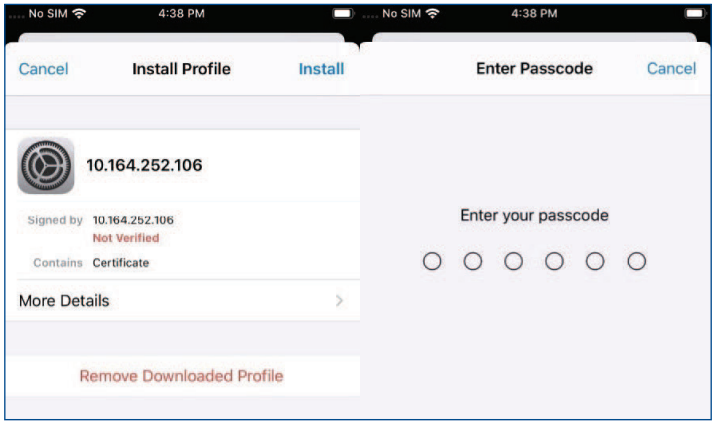


Figure 18. *Install profile page on iOS.*

5. Since we are installing a self-signed certificate, a Warning message will appear. Click install to proceed.

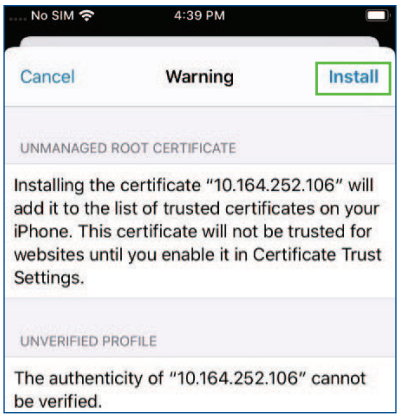


Figure 19. *Install profile warning on iOS.*

6. The profile is already installed, but it is not yet trusted. To trust the certificate, go back to General, and click about.

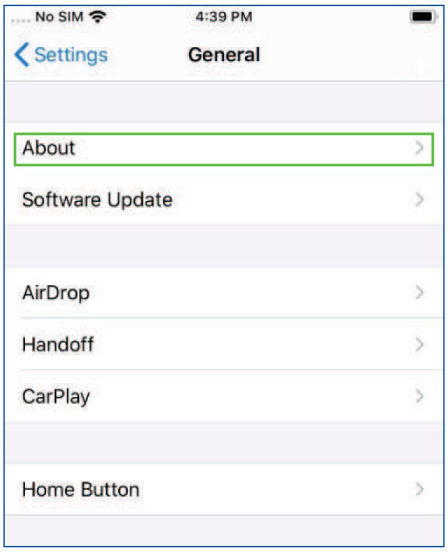


Figure 20. *iOS General page.*

7. Click on Certificate Trust Settings.

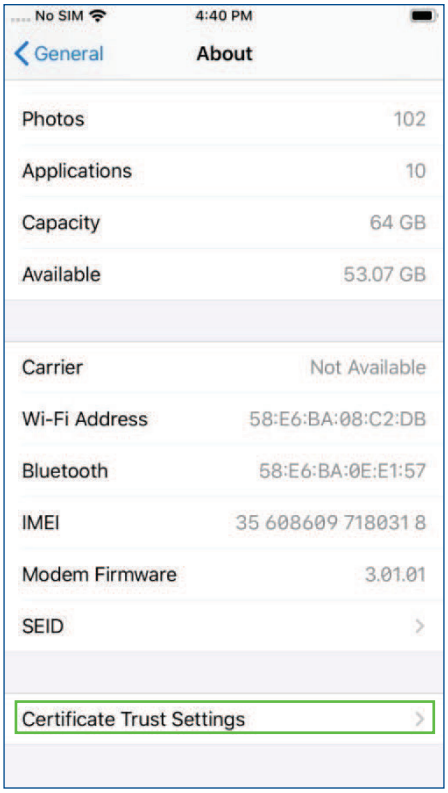


Figure 21. *iOS About page.*

8. On Certificate Trust Settings, toggle the button beside the new certificate installation. Click Continue to proceed.

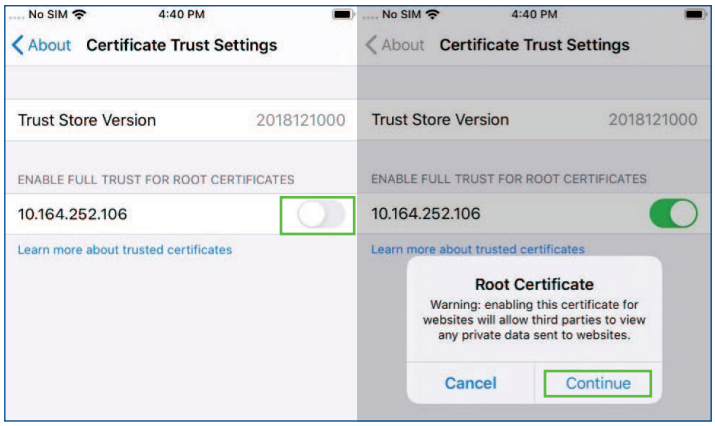


Figure 22. *Trust certificate on iOS.*

9. Navigate back to DeltaV Mobile App then log-in as usual.

Data Security

Protected Transfer of FHX File

DeltaV Mobile uses the export from the DeltaV configuration database (commonly referred to as the FHX file) to populate its database with the module hierarchy, module parameters, alarm parameters, and alarm configuration. The actual control strategy is not required and not imported into DeltaV Mobile. The transfer of the FHX file from the DeltaV Professional Plus workstation can be done manually or automated.

Manual Transfer

When done manually, the file must be placed into the '%ProgramData%\Emerson\Mobile-Imports' directory on the DeltaV Mobile Server. The user then uses DeltaV Mobile Studio to manually initiate an import. Once the import is complete, the FHX file is deleted automatically from the Mobile-Imports directory.

Automated Transfer

Automated and secure transfer of the configuration file (FHX) can be enabled. The FHX file can be automatically exported on a daily basis using DeltaV's built-in utility. Alternatively, the DeltaV Communicator can monitor the FHX file (on the Professional Plus) directly to track changes. The directory to monitor is specified by the user at the time they register their information source.

Data at rest

1. The DeltaV Communicator monitors the supplied path information (directory and information source file name for: write time changes (newer) and file size changes).
2. If a change is detected, a hash of the FHX file is created using SHA384.
3. A temporary .zip file is created.
4. The .zip file is then encrypted using AesManaged (Advanced Encryption Standard (AES) symmetric algorithm) to a second temporary file.

Data in transit

1. A notification is then sent to DeltaV Portal (via DeltaV Portal Info Source) with the hash result and the Key and IV from the encryption.
2. This notification is forwarded to the DeltaV Mobile Server.
3. The DeltaV Mobile Server then begins the process of requesting the transfer of the encrypted file one block at a time.

Data in use

1. Once the file transfer is complete, the .zip file is generated by decrypting the encrypted file, and the FHX is decompressed from the .zip file.
2. The hash of the FHX file is then performed. If valid, the FHX file is imported into the DeltaV Mobile configuration database (SQL Server database).

Data destruction

1. Once the import is complete, the FHX file is deleted from the '%ProgramData%\Emerson\Mobile-Imports\Auto' directory. Access to the '%ProgramData%\Emerson\Mobile-Imports\Auto' directory should be restricted to the "MobileService" and "Administrators" accounts.

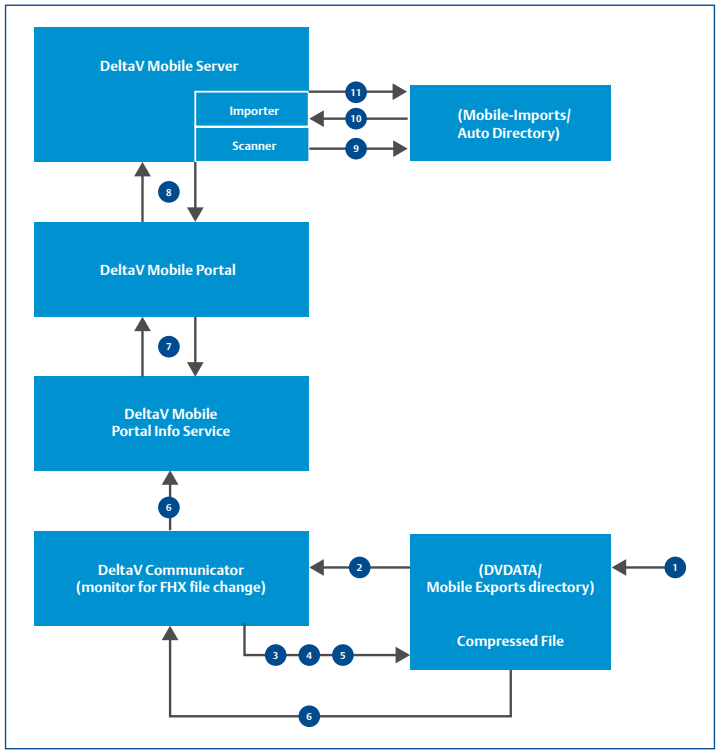


Figure 23. *FHX file transfer.*

Secure Development

Mobile Device Application Security

To secure Emerson's mobile infrastructure, Emerson proactively identifies and remediates mobile application vulnerabilities within the development lifecycle. Emerson has a dedicated, independent Threat and Vulnerability Management Team that performs mobile application security assessments on every release of all Emerson mobile application, including DeltaV Mobile. Tests are based on the Mobile OWASP.

Emerson Information Security has partnered with NowSecure to provide the capability to scan a mobile application at any stage in the development lifecycle to identify and remediate vulnerabilities prior to publishing to application stores. The findings are based on the National Information Assurance Partnership (NIAP).

The Threat and Vulnerability Management Team utilized the automated NowSecure ViaLab platform to test the DeltaV Mobile App for the following:

- Mobile Client
- Network and Web Traffic
- Code Analysis

DeltaV Mobile Security Manual

White Paper
October 2022

Contact Us
www.emerson.com/contactus