**Planning and Installation Guide**
September 2022

# AMS Device Manager

## Version 14.5 Planning and Installation Guide


EMERSON

## Document history

| Date | Description |
|---|---|
| May 2017 | Update, software version 13.5 |
| May 2018 | Update, software version 14.0 |
| October 2019 | Update, software version 14.1.1 |
| September 2020 | Update, software version 14.5 (managed) |
| February 2022 | Update, software version 14.5 (general) |
| September 2022 | Update, software version 14.5 FP1 |

# Contents

# 1 Introduction

This *AMS Device Manager Planning and Installation Guide* contains the following information:

- Chapter 1, Introduction – Provides an overview of AMS Device Manager installation and directs you to the appropriate procedures for installing AMS Device Manager for your setup and circumstances.
- Chapter 2, System requirements – Lists the system requirements for AMS Device Manager, including hardware, software, and security requirements. This chapter also defines additional requirements for system interface networks and sizing considerations when planning your system.
- Chapter 3, Install AMS Device Manager – Describes the procedures for installing AMS Device Manager. This chapter also details AMS Device Manager installation on a DeltaV network.
- Chapter 4, Before using AMS Device Manager – Describes configuration steps needed before using AMS Device Manager.
- Chapter 5, Troubleshoot installation errors – Provides troubleshooting steps you can take if you have problems installing AMS Device Manager.
- Appendix A, DeltaV system interface deployment concepts – Provides architecture diagrams for implementing AMS Device Manager with DeltaV.
- Appendix B, Other deployments – Provides architecture diagrams for implementing AMS Device Manager with supported system interfaces.
- Appendix C, Version compatibility – Provides matrices on AMS Device Manager compatibility with SNAP-ON applications and DeltaV.

**Note**
The information in this manual was current and reviewed as of the printed date. Changes to supported systems and applications may have changed after that date. Consult your local Emerson sales office to verify.

## 1.1 Before you begin

To install and use AMS Device Manager software effectively, you should be familiar with the basic functions and operation of:

- Microsoft Windows
- Your local area network (LAN) configuration and security
- Your communication devices and field devices
- Network components installed on your system

You should also be aware of:

- AMS Device Manager system requirements (see page 13)
- Database backup procedures (see page 7)

- Database restore procedures (see page 8)

**NOTICE**

Do not use the Windows compress feature on the PC drive where AMS Device Manager is installed. AMS Device Manager will be unable to open your database information. Reinstallation of AMS Device Manager will be required.

## 1.2 Configuration Assessment Tool

In preparation for deploying AMS Device View on your network, you should review your PC's Internet Information Services (IIS) configuration to ensure that your system is set up the way you want it. The Center for Internet Security (CIS) provides a tool to automatically check your IIS settings to assess and alert you to possible threat vectors depending on your security configuration needs. You can download this tool from https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/

In addition to the automated checking performed by the CIS-CAT Pro version, Emerson has created several additional XML-based scripts that can be run with this tool. These XML scripts can be found in Tech Support Utilities in the AMS Device View folder on the AMS Device Manager media.

## 1.3 Installation overviews

The following overviews direct you to specific information and procedures required for your type of installation.

### 1.3.1 Install a standalone AMS Device Manager system

A standalone AMS Device Manager system is a Server Plus Station that maintains the AMS Device Manager database, with no associated Client SC Stations.

**Procedure**

1. Read Before you begin.
2. Confirm that your system meets AMS Device Manager requirements on page 13.
3. Do one of the following:
   - For a new installation, follow the Server Plus Station installation steps on page 41.
   - For upgrading from AMS Device Manager 13 or later, see page 36.

### 1.3.2 Install a distributed AMS Device Manager system

A distributed AMS Device Manager system is a client/server deployment of AMS Device Manager Stations. It allows multiple AMS Device Manager Stations access to a common database and all connected devices in the distributed system.

**Procedure**

1. Read Before you begin.
2. Confirm that your system meets AMS Device Manager requirements on page 13.
3. Do one of the following:
   - For a new installation, follow the Server Plus Station and Client SC Station installation steps on page 35.
   - For upgrading from AMS Device Manager 13 or later, see page 36.

### 1.3.3 Install AMS Device Manager on a DeltaV system

**Procedure**

1. Read Before you begin.
2. Confirm that your system meets minimum requirements for a co-deployment (refer to the documentation provided with your DeltaV system).
3. Follow the installation steps on page 57.

## 1.4 Database operations

The following database procedures are essential to successfully install or upgrade to AMS Device Manager 14.5 FP1:

- Back up a database – Do this procedure before upgrading to AMS Device Manager 14.5 FP1.
- Restore a database – Do this procedure after upgrading AMS Device Manager to 14.5 FP1 from version 10.0 to 12.5.

### 1.4.1 Back up a database

**Note**
If performing a database backup on a PC with User Account Control enabled, log in with a Windows administrator user to avoid multiple error messages.

**Procedure**

1. Enter `Database Backup` on the **Start** screen and click **Database Backup**. You can also navigate to the AMS Device Manager folder in Windows.
2. In the **Backup Database** dialog, enter or select the name of the backup file. Select a secure location on your local drive outside the AMS folder.
3. Click **Save**.
4. Enter `Database Verify Repair` on the **Start** screen and click **Database Verify Repair** to check the database for duplicate, missing, and corrupt records.

   **Note**
   For a very large database, the Verify/Repair operation can take a long time.

5. Do one of the following:

- If Database Verify Repair does not return any errors, repeat steps 1 to 3.
- If Database Verify Repair returns any errors, run until there are no more errors and repeat steps 1 to 3.

### 1.4.2 Restore a database

**Notes**

- If you are restoring a database that was created on a different PC and you want to retain the Device Monitor List and Alert Monitor alerts, before you restore the database on the new station, ensure that the names of the PC and system interfaces configured on the new station are the same as the original station.
- If performing a database restore on a PC with User Account Control enabled, log in with a Windows administrator user to avoid multiple error messages.
- Ensure your Windows user has **System** → **Database Utilities** → **Restore Database** permission in AMS Device Manager User Manager. See *AMS Device Manager Books Online* for more information.

**Procedure**

1. Close AMS Device Manager and any related applications (for example, Alert Monitor or Server Plus Connect, if open.
2. Stop all database connections.
3. Right-click the AMS Device Manager Server icon in the Microsoft Windows system tray and select **Stop AMS Device Manager Server** from the context menu.
4. If the database backup file is located on a network drive, copy it to a local drive.
5. Enter `Database Restore` on the **Start** screen and click **Database Restore**.
6. Select the database backup file you want to restore and click **Open**.

## 1.5 Uninstall AMS Device Manager

You must uninstall AMS Device Manager if you are upgrading to the current version from versions 13.0 and lower. You do not need to uninstall the current AMS Device Manager software if you are upgrading from version 13.1.1 or higher. AMS Device Manager must always be uninstalled when co-deployed with a DeltaV system being upgraded. See Operating systems to ensure OS support when upgrading AMS Device Manager.

**Note**

If you have SNAP-ON applications, Web Services, or the AMS Device Manager Calibration Connector application installed, uninstall them before uninstalling AMS Device Manager. If your applications use an external database, you must back up that database before you uninstall the application (if you want to keep the data).

**Procedure**

1. Back up the database (see page 7).
2. Save your license.dat file in a location outside the AMS folder.

3. Right-click the AMS Device Manager Server icon in the Microsoft Windows system tray and select **Stop AMS Device Manager Server** from the context menu.
4. Open the Windows Control Panel and use Programs and Features to remove AMS Device Manager.

# 1.6 Reference documents

After AMS Device Manager is installed, the following user information tools are copied to your PC:

- *AMS Device Manager Books Online*
- *Release Notes*
- *Supported Device List*

## 1.6.1 AMS Device Manager Books Online

*AMS Device Manager Books Online* provides detailed reference and procedural information for using AMS Device Manager. AMS Device Manager Books Online explains the features and functions of AMS Device Manager. You should become familiar with AMS Device Manager Books Online and refer to it regularly as you use AMS Device Manager.

You can access AMS Device Manager Books Online in two ways:

- Click the **Help** menu on the AMS Device Manager toolbar and select **AMS Device Manager Books Online**.
- Enter `Books Online` on the **Start** screen and click **Books Online**.

Use the Contents, Index, or Search tab in the left pane to locate specific topics. You can save shortcuts to frequently used topics and access them on the Favorites tab.

## 1.6.2 Electronic documentation

Two user documents are placed on your station when AMS Device Manager is installed. These documents are available as Portable Document Format (PDF) files, and include the *AMS Device Manager Planning and Installation Guide* and the *Supported Device List*.

You need Adobe Reader to view these files. If you do not have a compatible version of Adobe Reader on your PC already, you can download Adobe Reader from www.adobe.com.

To access an electronic document after Adobe Reader is installed, enter `Installation Guide` or `Supported Device List` on the **Start** screen and click **Installation Guide** or **Supported Device List**.

## 1.6.3 Release Notes

The *Release Notes* provide information about the current release of AMS Device Manager, including supported devices, compatibility issues, and known discrepancies and workarounds.

The Release Notes are provided in text (.TXT) format. You can access the Release Notes in two ways:

- Enter `Release Notes` on the **Start** screen and click **Release Notes**.
- Double-click the `RELNOTES.TXT` file located in the AMS folder after installation or on the AMS Device Manager media

We recommend that you read the Release Notes before using AMS Device Manager.

## 1.6.4 AMS Device View Help

The AMS Device View Help provides detailed reference and procedural information for using AMS Device View. It explains the features and functions of AMS Device View. You can access the AMS Device View Help by selecting  >  from AMS Device View. Use the Search section to find specific topics.

## 1.6.5 Device manuals

Many device manufacturers provide manuals for their devices in PDF format. Run the AMS_PDF_Installer utility to copy relevant manuals to your hard drive. The utility is located in the Device Documentation Installer folder on the AMS Device Manager media.

After installing device manuals, you access them in AMS Device Manager by right-clicking a device and selecting Help from the context menu. If a device manual is available, it opens in Adobe Reader. If no manual exists for the selected device, *AMS Device Manager Books Online* opens. To see a list of device manuals installed on your station, select **Help** → **Device** from the AMS Device Manager toolbar. Double-click a device to open the associated manual.

## 1.6.6 Product data sheets, security guides, and white papers

AMS Device Manager product data sheets provide product descriptions, features, and benefits. Security guides ensure you plan properly to secure communications with AMS Device Manager and related Emerson software. White papers help you understand AMS Device Manager systems and items important to system planning. Please have the data sheets, security guide, and white papers ready for reference when planning a system. For convenience, some product specifications are included in this guide, but this guide is not intended to duplicate security planning, or reproduce product data sheets or white papers. The data sheets and white papers are available on the Emerson website. The security guide is available with a Guardian subscription. See the AMS Device Manager Product Security Guide that applies to this release of AMS Device Manager.

## 1.6.7 Knowledge Base Articles

The following Knowledge Base Articles (KBA) provide information on specific AMS Device Manager requirements or components:

- KBA NA-0400-0084 *AMS Device Manager Multiplexer System Interface Setup & Troubleshooting Guide*
- KBA NA-0700-0015 *Microsoft Security and Critical Updates*

- KBA NA-0800-0113 *Configuring AMS Device Manager for Cross Domain Functionality*
- KBA NK-1000-0150 *Interoperability of AMS Device Manager Versions with DeltaV*
- KBA NK-1300-0268 *AMS Device Manager Support in Virtual Environments*
- KBA NK-1500-0028 *Computers Must Meet a Supported Installation Scenario When Using AMS Device Manager with DeltaV*
- KBA NK-1500-0051 *Suggested Memory Configuration for SQL Server When Used With AMS Device Manager*
- KBA NK-2100-0182 *Updated AMS Device Manager v14.x System Requirements*
- KBA NK-2200-0080 *Guidelines For Installing A Standard Version Of SQL Server 2019 To Be Used With AMS Device Manager*
- KBA NK-2200-0358 *DeltaV Security Settings Prevent Correct Installation Of AMS Device View*

# 2 System requirements

Each PC in your system must meet minimum software and hardware requirements to ensure successful installation and operation of AMS Device Manager. System interface networks and SNAP-ON applications may have additional requirements.

## 2.1 Sizing considerations

When determining requirements for an AMS Device Manager system, consider the items included in the following tables:

| System Sizing | Supported Maximum | Comments |
|---|---|---|
| Total Tag Count? | 30,000 tags (per system) and 50 networks (per station) | If the system will support more than 3,000 devices, see the requirements on page 22. |
| Wireless Gateway? | 16 Wireless Gateways for each Wireless Interface | Each Wireless Gateway requires an AMS Tag |
| *Wireless*HART Adapters? | 15,000 | Each *Wireless*HART Adapter requires an AMS Tag |
| Total AMS Device Manager stations including the Server Plus? | 132 (Per System) | Although 132 stations are supported, Emerson recommends a maximum of 20 Client SC Stations. |

| Supported System Interfaces | Total Number of Devices Connected per Interface | Comments |
|---|---|---|
| DeltaV | 30,000 (no other interfaces) | When installing AMS Device Manager on a DeltaV system, a licensed AMS Device Manager station (Server Plus or Client SC) must be installed on the ProfessionalPLUS. |
| Wireless Network | 30,000 (no other interfaces), 16 wireless gateways for each Wireless Interface. | |
| Multiplexer Interface | 30,000 (no other interfaces), 31 multiplexers per Multiplexer Interface, up to 255 devices per Multiplexer. | |
| Field Communicator | • You can only connect one AMS Trex unit at a time to an AMS Device Manager station using USB.<br>• You can connect multiple AMS Trex units to an AMS Device Manager station using WiFi. | In an AMS Device Manager distributed system with cross-domain deployment, AMS Trex must be connected to the Server Plus. |

| Supported System Interfaces | Total Number of Devices Connected per Interface | Comments |
|---|---|---|
| HART-IP | 30,000 devices (no other interfaces), 16 gateways per network | |

| Networking Considerations | Supported Maximum | Comments |
|---|---|---|
| Number of Network Domains? | N/A | See *KBA NA-0800-0113* for more information about domains and installing on Domain Controllers. |
| Number of Network Workgroups? | N/A | Restrictions on some ClientSC operations in Workgroups. See Network requirements. |
| Number of Ethernet Serial Hubs? | 50 | |
| Network Firewalls | N/A | Complement firewalls with antivirus software. If AMS Device Manager is installed on a DeltaV workstation, be sure to install an antivirus software according to the specifications of those systems. See AMS Device Manager Product Security Guide for more information. |
| Will Remote Desktop Services or Remote Desktop Session Host be used? (Yes or No) | 5 Concurrent Sessions | See Support for Remote Desktop Services and page 19 for information about supported remote desktop and operating systems. |

# 2.2 Hardware requirements

## 2.2.1 PC processing speed, memory, and disk space

| Application Type | Minimum Requirements |
|---|---|
| Server Plus Station (standalone or distributed system)[1] | Intel Xeon scalable 8-core, 2.4 GHz<br>64 GB RAM<br>100 GB free hard disk space<br>Local SSD SATA hard drive |
| Client SC Station with NO Host Systems (I/O) configured[2] | Intel Core I7, 9th gen, 6-core, 3 GHz<br>16 GB RAM<br>10 GB free hard disk space<br>Local SSD SATA hard drive |
| Client SC Station with Host Systems (I/O) configured | Intel I7 9th gen, 6-core, 3 GHz<br>32 GB RAM<br>10 GB free hard disk space<br>Local SSD SATA hard drive |
| Client SC Station with or without I/O connection with AMS Device View Web Server installed | Intel Core I7, 9th gen, 6-core, 3 GHz<br>32 GB RAM<br>50 GB free hard disk space<br>Local SSD SATA hard drive |
| AMS Device View Web Server (standalone) | Intel Core I7, 9th gen, 6-core, 3 GHz<br>16 GB RAM<br>10 GB free hard disk space<br>Local SSD SATA hard drive |
| Notes: Screen resolution minimum for all stations: SVGA 1024x600 16-bit color | |
| [1]Use SQL Server full version if you have 10GB or greater database, 3,000 devices or more, or you have more than 10 stations. | |
| [2]Modem or calibrator not included in count. | |

## 2.2.2 Serial interfaces

Ethernet serial hubs may be used to add more serial ports when distributing the field devices across multiple AMS Device Manager stations, and are often used when multiple remote systems exist within a plant, and you need to have consolidated information available in a single location such as a maintenance office. Installing Ethernet serial hubs lets virtual COM ports be added to the AMS Device Manager PC and can significantly reduce the required length of the RS-485 network wiring. The HART Multiplexer Interface and documenting calibrators can be used over the existing plant Ethernet.

- An RS-232 serial interface is required for a serial HART multiplexer network or documenting calibrator.
- A serial port with a dedicated interrupt is required for a serial HART modem.

- The use of serial ports on virtual PCs is NOT supported.

### 2.2.3 USB interfaces

- A USB port and USB HART modem drivers are required to use a USB HART modem. See the *Release Notes* for a list of supported modems.
- A USB port is required to connect and pair an AMS Trex Device Communicator to an AMS Device Manager station. A device cannot be connected to a Trex unit when the USB is plugged in.
- The use of USB ports on VMWare and Hyper-V virtual PCs is supported.
- Some Smart Calibrators may use a USB connection. See Documenting Calibrators section for details.

## 2.3 Network requirements

- If you are installing AMS Device Manager on a domain, and it is not the domain controller, you will first need to install software on the domain controller. This installation can be found in the Domain Controller Setup folder on the AMS Device Manager media. See Installing AMS Device Manager on domain controllers for details.
- AMS Device Manager is designed to operate on an Ethernet network running TCP/IP.
- Mobile AMS Device Manager stations are allowed to connect wirelessly using wireless plant network technology. Some communications slowdown can be expected with wireless networking.
- AMS Device Manager has restrictions on certain operations on ClientSC stations in a workgroup environment. Operations that should be performed on the ServerPlus in a workgroup environment include creating user configurations or transferring user configurations to AMS Trex, and provisioning wireless devices from a Wireless Gateway configured on one station to a Wireless Gateway configured on another.
- AMS Device Manager supports deployment within a single domain or workgroup or across multiple domains or workgroups. For more information, refer to *KBA NA-0800-0113*.
- AMS Device Manager does not support deployment between a network workgroup and a network domain.
- Named IP services (how PCs identify each other on a network) must be functioning correctly for stations in an AMS Device Manager distributed system to communicate.
- All stations must be connected to the network before beginning AMS Device Manager installation. This ensures that all stations can access the AMS Device Manager database. All stations' computer names should be recorded (see page 48).
- All stations' PC clocks must be synchronized (many third-party tools are available for this purpose). Clock synchronization is important because the date and time of an event recorded in the database is based on the clock in the PC that generated that event.
- If using workgroups rather than a DNS network, PC names must be manually added to the host table of each PC in the distributed network.

For information about working with network firewalls, see page 61.

**Note**
Consult with your IT department about security issues and any other network operation issues or special requirements for your network.

## 2.3.1 AMS Trex

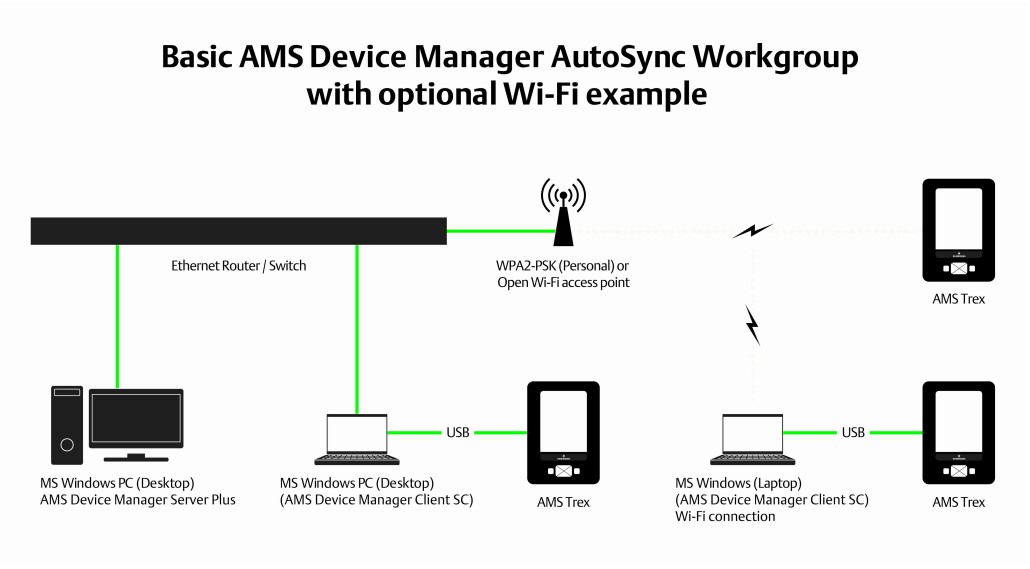
The AMS Trex Device Communicator uses the Field Communicator license, and can communicate with AMS Device Manager on USB or Wireless. You can connect only one concurrent AMS Trex unit at a time to any AMS Device Manager station using USB. You can connect multiple AMS Trex units to any AMS Device Manager station using WiFi.

If you connect to an Enterprise WiFi network, you will need domain user credentials to connect a Trex unit to the network. In an AMS Device Manager distributed system with cross-domain deployment, AMS Trex must be connected to the Server Plus.

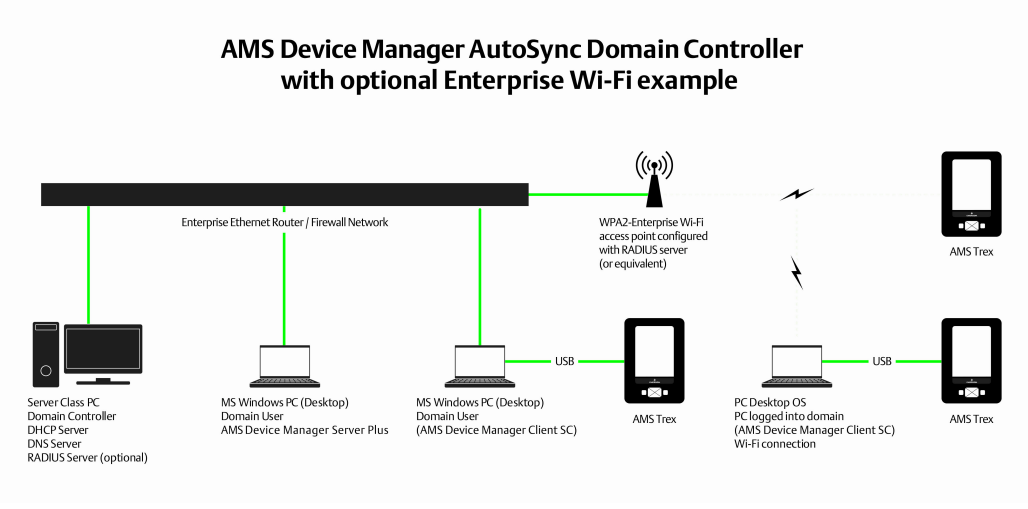
WiFi Protected Access-Enterprise (WPA-Enterprise) is a wireless security mechanism designed for small to large enterprise wireless networks. It is an enhancement to the WPA security protocol with advanced authentication and encryption.

WPA-Enterprise uses the Remote Authentication Dial-in User Service (RADIUS) protocol to manage user authentication.

**Figure 2-1: AMS Trex connection points in a workgroup**



## Figure 2-2: AMS Trex connection points in a domain



# 2.4 Software requirements

## 2.4.1 Operating systems

AMS Device Manager supports the following Windows operating systems:

**Note**
The AMS Device View web server requires server-class Windows operating systems.

| Operating System | Version |
|---|---|
| Windows Server 2016 | Standard |
| Windows Server 2019 | Standard |
| Windows Server 2022 | Standard and IoT editions |
| Windows 10 (not supported for AMS Device View web server) | Professional, Enterprise, Enterprise LTSB, LTSC and IoT editions |
| Windows 11 (not supported for AMS Device View web server) | Professional, Enterprise, Enterprise LTSB, LTSC and IoT editions |

**Notes**

- Only 64-bit versions of the operating systems are supported.
- Desktops, laptops, and tablets with touchscreens are supported on Windows 10 and Windows 11.
- AMS Device Manager and associated SNAP-ON applications may not be 64-bit applications but will be able to run on a 64-bit OS with full functionality.
- Intermixing of the supported operating systems is supported.
- A Server operating system and server-class PC (for example, Dell PowerEdge) are recommended if the database is expected to be greater than 10 GB due to the SQL Server version required (see page 22); or if AMS Device Manager is installed on a DeltaV ProfessionalPLUS Station, Application Station, or Maintenance Station and Batch Historian or VCAT will be used.
- The correct operating system service pack (SP) must be installed on your PC before installing AMS Device Manager. If your PC does not have the correct SP installed, or you are unsure, contact your network administrator.
- See Change Windows Firewall settings for additional operating system configuration considerations.
- AMS Device Manager also supports localized versions of the listed operating systems.

## 2.4.2 Virtualizations

AMS Device Manager is supported on VMWare and Hyper-V virtual PCs.

AMS Device Manager requires a local, dedicated processor, memory, and hard drive for virtual machines.

**Note**
All support for virtual PC setup and functionality must come from VMWare or Microsoft support.

**Supported features:**

- All Ethernet connectivity. This will include but not be limited to:

  - Ethernet Serial Hubs
  - DeltaV systems
  - Wireless HART networks
  - HART-IP networks
  - Other system interfaces that may use Ethernet connectivity
- Smart Calibrators with USB connections
- Supported USB HART modems (Bluetooth HART modems are not currently supported in a virtual environment)

**Note**
No physical serial connections will be supported on any AMS Device Manager station that is installed on a virtual PC. This includes, but is not limited to: serial HART modems, RS232 to RS485 converters, and Bluetooth HART modems. For more information regarding AMS Device Manager installed as a Standalone system, please contact your Emerson sales office or the Global Service Center.

## 2.4.3 Operating system patches and service packs

Newly released Microsoft critical updates and service packs are installed and tested in the AMS Device Manager development labs on supported operating systems. Service pack releases from Microsoft are less frequent but involve many more changes to the operating system. Full support for a new service pack is usually on the next major product release; however early versions of service packs are installed when they are made available from Microsoft, and should an issue be detected, the action we take is very similar to that of critical updates. For more information, see *KBA NA-0700-0015 Microsoft Security and Critical Updates*.

In addition, users can take advantage of the Guardian Support service and website, which provides fixes, patches and KBAs based on their unique system configuration. For more information, visit https://www.emerson.com/en-us/catalog/ams-guardiansupportdevicemanager.

## 2.4.4 Support for Remote Desktop Services

Remote Desktop Services (RDS) is the platform of choice for building virtualization solutions for every end customer need, including delivering individual virtualized applications, providing secure mobile and remote desktop access, and providing end users the ability to run their applications and desktops from the cloud. To use AMS Device Manager 14.5 FP1 in a Remote Desktop Services environment, do the following:

- Set up Remote Desktop Services.
- If you are using a Remote Desktop Session Host, install it before AMS Device Manager. A Remote Desktop Session Host requires a license.
- Remote Desktop Services is limited to 5 concurrent sessions when AMS Device Manager is installed on Windows server-class computers.
- Ensure that Remote Desktop Services is NOT set to **Relaxed Security**.

**Notes**

- Do not attempt to install AMS Device Manager on a PC accessed through a Remote Desktop Services session; this is not a supported installation method and may produce undesirable results.
- If multiple users are running AMS Device Manager on a Remote Desktop Session Host, and one of the users runs Terminate Servers, the AMS Device Manager application and AMS Device Manager Servers shut down for all users.
- In a Remote Desktop Services environment, SNAP-ON applications may be limited to only one session at any given time.
- If you are installing a Client SC Station on a licensed Remote Desktop Session Host, a Client SC Station license is required for each licensed session.

Contact Microsoft for Remote Desktop Services licensing information. Questions about AMS Device Manager licensing requirements should be directed to your local Emerson sales office.

## 2.4.5 Web browsers

AMS Device Manager supports the following web browsers:

- Microsoft Edge version 97 or higher
- Google Chrome version 97 or higher

When using Google Chrome or Microsoft Edge as a browser for AMS Device View on a PC without AMS Device Manager, you need to download an extension to allow the feature to work properly. https://chrome.google.com/webstore/detail/clickonce-for-google-chro/kekahkplibinaibelipdcikofmedafmb?hl=en-US If using AMS Device View on a PC without internet access, you need to use Microsoft Edge.

AMS Device View also supports Safari Mobile (iOS 14.0 or newer only).

## 2.4.6 AMS Device Manager Web Services

AMS Device Manager Web Services provide the ability to import AMS Device Manager data, in XML format, into business applications such as Microsoft Excel. In addition, Computerized Maintenance Management Systems (CMMS) and Enterprise Resource Planning (ERP) systems can use AMS Device Manager Web Services to retrieve data from AMS Device Manager.

Microsoft Internet Information Services (IIS) and AMS Device Manager 14.5 FP1 Server Plus Station software must be installed on your system before you can install AMS Device Manager Web Services. AMS Device Manager Web Services is not supported on Client SC Stations. If you do not have IIS installed, contact your IT department for assistance.

The following components will need to be enabled for proper operation.

- ASP.NET
- .NET Extensibility
- Request Filtering
- ISAPI

- ISAPI Extensions

**Notes**

- Some control systems do not allow IIS to be installed on the same PC. Check your control system documentation to determine IIS compatibility.
- If you want to install AMS Device Manager Web Services on a DeltaV station, it must be a DeltaV Application or ProfessionalPLUS station.
- You need local administrator permission to install AMS Device Manager Web Services.

## 2.4.7 .NET Framework

If not found on the PC, AMS Device Manager installs the following .NET Framework components

- Microsoft .NET Framework 4.6.1, 4.8
- (for AMS Device View) Microsoft .NET Core 2.2.0 – Windows Server Hosting (includes ASP .NET)

## 2.4.8 Database

AMS Device Manager 14.5 FP1 uses a named instance, Emerson2019, of SQL Server 2019 for its database. The ODBC version 17.9 component is also installed if not present. The size of your database determines which edition of SQL Server you must use:

- *If your database is less than 10 GB*, you can use SQL Server 2019 Express. The AMS Device Manager 14.5 FP1 setup installs this version automatically.
- *If your database is greater than 10 GB* or will be at some future time, we recommended that you install a full version of SQL Server before you install AMS Device Manager.
- If the AMS Device Manager system will support more than 3000 AMS Tags, or have more than 10 AMS Device Manager stations, a full version of SQL Server is recommended regardless of database size.

A full version of SQL Server 2019 must be purchased separately (if you do not already have it).

**Notes**

- Contact Microsoft for more information about appropriate licensing for a full installation of SQL Server
- Additional SQL Server licenses are required when using Client SC Stations. Contact Microsoft for more information.
- The AMS Device Manager database must be located in the `AMS\DB` folder on a local partition of the AMS Device Manager Server Plus Station. Any other location is not supported.

The AMS Device Manager installation program installs SQL Server on your PC as follows:

- If SQL Server 2019 is not installed, the AMS Device Manager 14.5 FP1 installation program will create an Emerson2019 named instance. It will also install and configure SQL Server 2019 Reporting Services Express edition.

- If an instance of SQL Server 2019 is installed, but not the Emerson2019 named instance, the AMS Device Manager 14.5 FP1 installation program will create the Emerson2019 named instance.
- If the SQL Server 2019 Emerson2019 named instance is already installed, the AMS Device Manager 14.5 FP1 installation program will continue with the next part of the installation.
- If you have previously installed a full version of SQL Server 2019, you should create the Emerson2019 named instance before installing AMS Device Manager 14.5 FP1 (refer to your SQL Server documentation). Otherwise, the AMS Device Manager installation will install SQL Server 2019 Express.

### 2.4.9 Microsoft Office

The following Microsoft Office applications are supported:

- Microsoft Word 2013, 2016, 2019 (for Drawings and Notes)
- Microsoft Excel 2013, 2016, 2019 (for Bulk Transfer)
- Microsoft Office 365 (for Drawings and Notes, Bulk Transfer)

**Note**
All stations in a distributed system must use the same application and version for entering Drawings/Notes.

## 2.5 Windows security requirements

### 2.5.1 AMS Device Manager installation

You need Windows system administrator rights to install and configure AMS Device Manager. You also need to review the important security information specified in the "AMS Product Security Guide". Contact Emerson Technical Support for access to this document on Guardian. The document applies to AMS Device Manager and many other AMS-branded products, and provides guidance on what you and your network team need to do to ensure secure installation and operation. TLS 1.2 is required to be enabled. Contact your network administrator for more information.

If AMS Device Manager is being installed on a domain, and will be accessing a domain controller (to support an AMSServiceUser Windows account providing access for all AMS stations on the domain, for instance), you will need to be a member of the domain administrator group to install AMS Device Manager. When installing AMS Device Manager 14.5 FP1 on a domain, follow the steps in Installing AMS Device Manager on domain controllers.

**Note**
Microsoft SQL Server 2019 Reporting Services is not allowed on a Windows domain controller due to Microsoft Windows restrictions, so Bulk Transfer reports will not work.

The Certificate Manager utility helps automate the process of managing secure communications among the AMS Device Manager and (if installed) AMS Device View components on your system. Depending on your deployment of System Interfaces, you

will need to run Certificate Manager on the Server Plus station, and all stations with a configured system interface, and copy certificates to the appropriate stations. Certificate Manager will display the state of certificates on the station. See Configure and secure a Distributed System and *AMS Device Manager Books Online* for more details.

## 2.5.2 AMS Device Manager users

During installation, the **AMSDeviceManager** Windows user group is created and given access to the AMS folder, subfolders, and files. When an administrator adds existing Windows users in the AMS Device Manager User Manager utility on local or domain PCs (see *AMS Device Manager Books Online*), these users are automatically added to the AMSDeviceManager Windows user group. However, they may not be able to use all AMS Device Manager features until permissions are assigned to them in User Manager.

For AMS Device Manager stations on a workgroup, Windows users added in the User Manager utility must be manually added to the AMSDeviceManager Windows user group using the Windows Control Panel on the Client SC Stations.

The installation creates a share of the AMS folder. It also allows connected Client SC Stations to use the Drawings/Notes feature of AMS Device Manager. If your situation makes this security configuration undesirable, consult your operating system documentation or your system administrator.

## 2.5.3 AMS Service User

A Windows user account called **AMSServiceUser** is automatically created on each AMS Device Manager station and added to the **AMSDeviceManager** Windows user group. The **AMSServiceUser** account is not created if it exists on the domain controller where AMS Device Manager stations are connected. The local or domain **AMSServiceUser** accounts are also added to the **AMSDeviceManager** Windows user group on all AMS Device Manager stations during installation.

The AMS Device Manager installation prompts you to enter the AMS system password for this created user. Make sure the password you enter meets your OS password complexity requirements, and remember this password for subsequent installations which require it, such as AMS Web Services.

**Note**
If you are installing an AMS Device Manager distributed system on domain controller PCs or a mix of domain controllers and non-domain controller PCs, do all the domain controller installations first (see page 54). When installing on a DeltaV Professional Plus with an IDDC, the AMSServiceUser account is installed on the IDDC, not on the Professional Plus.

This user account runs some of the AMS Device Manager services. If your AMS Device Manager system is located on a network that requires periodic changing of passwords, the AMSServiceUser account password can be changed using the `AMSPasswordUtility.exe` utility from the `AMS\Bin` folder on each AMS Device Manager station. You should only run the utility after all AMS Device Manager stations have been installed. Do not use the Windows User Accounts or AMS User Manager to modify this user, or change this password as AMS Device Manager will no longer function.

**Note**
If the AMS Device Manager Calibration Connector application (see page 58) is installed when you change the password for the **AMSServiceUser**, you must also change the password for AmsCalibrationConnectorWS properties. This requires a change in the Windows Services console of your workstation. If you are unsure how to do this, contact your IT department.

### 2.5.4 AMS Device View security requirements

You need Windows system administrator rights to install and configure the AMS Device View web server. Contact your network administrator if there are other network security requirements before installation.

To access and use AMS Device View, Windows users must be:

- members of the AMSDeviceManager Windows group
- enabled in AMS Device Manager User Manager

And have the following permissions in AMS Device Manager User Manager:

- Device Read. Also, if not using a Read-Only server:
- Device Write, to associate a device with a project, remove a device, or mark a device as complete
- Manage Alert Configurations, to disable alerts in AMS Device View
- System Settings Write, to rename, delete, or complete a project

Users with Plant Location restrictions can only view devices in their assigned area. See *AMS Device Manager Books Online* for more information on AMS Device Manager security.

## 2.6 Requirements for system interfaces

Requirements for system interfaces are in addition to the hardware and software requirements for AMS Device Manager.

### 2.6.1 HART modems

HART modems let AMS Device Manager communicate with HART devices using a PC serial port, PC USB port, or Bluetooth connectivity. Serial and USB HART modems attach directly to a PC or laptop computer. Bluetooth HART modems require a self-contained power source as well as a Bluetooth-ready workstation PC. The PC can have Bluetooth capability built-in or use a Bluetooth adapter and Microsoft Bluetooth software components. HART modems are not supported with USB to RS-232 converters or with Ethernet converters.

You must configure AMS Device Manager to send and receive data to and from the PC serial communications port or USB port (USB HART modem software is required). If a Bluetooth HART modem is used, you must prepare the PC for its use. Contact your IT department for assistance. HART modems also allow multidropping up to 16 HART devices.

The following modems are supported:

- Microflex MicroLink USB HART Modem
- P&F External Serial HART Modem
- P&F USB HART Modem
- P&F USB HART Modem w/PowerXpress
- P&F Bluetooth Viator Modem (Windows 10 only)

**Notes**

- If your USB or Bluetooth HART modem manufacturer provided supporting driver software, install it before configuring the modem for use with AMS Device Manager.
- Bluetooth is not natively supported on Windows Server 2016.
- Installing a HART Modem in Network Configuration requires Windows Administrators group permissions.

## 2.6.2 Documenting calibrators

With the optional Calibration Assistant SNAP-ON application, a documenting calibrator can be used to automate the collection of device calibration data.

When the documenting calibrator is connected to AMS Device Manager, test definitions can be checked out (downloaded) to the calibrator. The calibrator is then attached to the corresponding field device, tests are run, and data is collected. This data can then be checked in (uploaded) to AMS Device Manager for electronic record keeping and report generation.

The following documenting calibrators are supported:

- Fluke 729*, 753, 754*
- Druck DPI615, DPI620 CE/IS/Genii+
- Rosemount P330, P370, T460, T490
- Beamex MC6 (MC6-Ex, MC6-T not supported)
- Transmation 195, 196, 197
- BETA Calibrators (BetaFlex*, BetaGauge II, and MasterCal 922) that support protocol 13 or later.

* The drivers for these calibrators support downloading of switch data. The Windows driver for the 754 must be installed before configuring it to be used with AMS Device Manager. To install drivers for these calibrators, see KBA NK-1400-0206.

A USB port and drivers are required to connect Fluke 753 and Fluke 754 Documenting Process Calibrators.

The Beamex MC6 USB driver, located on the AMS Device Manager install media, must be installed first before using the Beamex MC6 with AMS Device Manager. You must select USB from the Com Port dropdown when configuring the calibrator in Network Configuration.

The Beamex MC6 supports downloading test definitions for fieldbus devices.

See the *AMS Device Manager Supported Device List* to determine if a device supports calibration.

## 2.6.3 DeltaV

A DeltaV control network is an isolated Ethernet local area network (LAN) that provides communication between the controllers and the stations. It uses one or more Ethernet hubs for communication.

DeltaV System Interface station software requirements:

- AMS Device Manager 14.5 FP1 can only be installed on the following DeltaV 13.3.2, 14.LTS, 14.FP1, .FP2 and .FP3, and 15.LTS stations:

| DeltaV Workstations | AMS Device Manager Station Type |
|---|---|
| ProfessionalPLUS Station | Server Plus Station or Client SC Station |
| ProfessionalPLUS as Remote Client Server | Server Plus Station or Client SC Station |
| Local Application Station[1] | Server Plus Station or Client SC Station |
| Remote Application Station | Server Plus Station or Client SC Station |
| Local "Operate" Station<br>— Professional<br>— Operator<br>— Base<br>— Maintenance | Server Plus Station or Client SC Station |
| Operator Station as Remote Client Server | Client SC Station only |
| Remote "Operate" Station<br>— Professional<br>— Operator<br>— Base | Client SC Station only |
| [1]Remote Desktop Services is not supported. | |

- The DeltaV System Interface must be configured on a licensed AMS Device Manager station that is on the DeltaV network.
- AMS Device Manager supports DeltaV version 13.3.2 and later in co-deployed installations only.

For a list of supported DeltaV Controllers with versions of DeltaV, see the DeltaV Software Updates KBAs and Release Notes for each version.

DeltaV supports:

- FOUNDATION fieldbus devices
- Wired HART Rev. 5, Rev. 6, and Rev. 7 devices
- *Wireless*HART Rev. 7 devices
- PROFIBUS DPV1 devices
- PROFIBUS PA devices (supported on DeltaV 13.3.2 or higher with a Series 2+ PROFIBUS DP I/O card and a PROFIBUS DP/PA Coupler on a PROFIBUS DP segment. See PROFIBUS section for supported couplers.)

- HART safety devices connected to DeltaV SIS logic solvers
- HART safety devices connected to DeltaV 13.3.2 or later (SIS) CHARMs logic solvers

DeltaV versions 13.3.2 and later can access devices connected to RS3 and PROVOX I/O systems through the DeltaV Interface for RS3 I/O and DeltaV Interface for PROVOX I/O, respectively. The devices are displayed in the DeltaV network hierarchy in AMS Device Manager. For installation and setup information, refer to the *DeltaV Books Online*.

To receive alerts from devices connected to PROVOX and RS3 Migration Controllers in your DeltaV network hierarchy, you must run a utility to properly set the DeltaV alert capability (see page 62).

The DeltaV password (if not using the default password) must be entered in the AMS Device Manager Network Configuration utility (see *Add a DeltaV network* in *AMS Device Manager Books Online*).

The ValveLink SNAP-ON application is supported for DeltaV and PROVOX I/O cards, but not for RS3 cards.

The DeltaV System Interface supports ValveLink Diagnostics. Analog output modules configured for HART are required on the DeltaV station for communication with HART FIELDVUE digital valve controllers. FOUNDATION fieldbus FIELDVUE digital valve controllers need only be commissioned and ports downloaded.

### 2.6.4 HART-IP

The HART-IP System Interface lets you use AMS Device Manager to view and configure wired and wireless devices connected to HART-IP gateways. The following HART-IP gateways are supported:

- Triconex CX v11.5
- HIMA HIMax v 5
- Honeywell OneWireless WDMX, WDMY v R240, R300, R310, R320
- Phoenix Contact Ethernet HART Multiplexer including:
  - GW PL ETH/BASIC-BUS, v 2702321)
  - GW PL ETH/UNI-BUS, v 2702233)
- Softing smartLink HW-DP v 2.0, SW-HT v 1.20 and higher

Other gateways may be supported. See NK-2200-0374 AMS Device Manager V14.5 FP1 Release Information. Contact your HART-IP manufacturer for any gateway-specific firmware or software needed to connect to AMS Device Manager.

### 2.6.5 HART Multiplexer Network

The HART Multiplexer System Interface lets you use AMS Device Manager to communicate with HART devices through a HART multiplexer. HART multiplexers can link many installed HART field devices to an AMS Device Manager station, providing the capability to remotely configure, troubleshoot, and monitor those devices. A typical HART multiplexer network enables one PC COM port to communicate with up to 63 addressable HART multiplexers.

AMS Device Manager supports a variety of multiplexers, each with different capabilities and requirements. Supported multiplexer types can have between 32 and 256 device connections.

A HART multiplexer network requires:

- One serial communication port for each HART multiplexer network.
- An RS-232 to RS-485 converter or a supported Ethernet serial hub

### Table 2-1: Supported HART Multiplexers

| Manufacturer | Model | Max Channels | Hardware supports Enhanced Polling | Default in AMS Device Manager | Notes |
|---|---|---|---|---|---|
| Arcom | H-Port | 32 | Yes | Off | Contact the Emerson Global Service Center or your local support office for details on enabling Enhanced Polling for ARCOM H-PORT multiplexers. |
| Elcon | 1700 | 32 | No | Off | - HART 6 and 7 devices may experience communication errors. |
| | 2700A | 32 | No | Off | - HART 6 and 7 devices may experience communication errors. |
| Pepperl + Fuchs | HiDMux2700 | 32 | Yes | On | The HiDMux2700 must be upgraded with firmware version 7 or later to work correctly with AMS Device Manager version 7.0 or higher. |
| | KFD2-HMM-16 | 256 | Yes | On | See [1] below. |
| | KSD2-GW-xxx | Service Bus | Yes | On | Appears as HART Multiplexer 255-way. HART 6 and 7 devices may experience communication errors. |

**Table 2-1: Supported HART Multiplexers *(continued)***

| Manufacturer | Model | Max Channels | Hardware supports Enhanced Polling | Default in AMS Device Manager | Notes |
|---|---|---|---|---|---|
| MTL/Novatech | 4841/4842 (Device Type 15) | 256 | No | Off | Novatech recommends customers with MTL 4841-AMS multiplexers, who want to use enhanced polling, contact them about upgrading to an MTL 4841-AMSv7 multiplexer. You will either have to return the MTL 4841-AMS multiplexer for reprogramming or replace your existing multiplexer with a new MTL 4841-AMSv7. HART 6 and 7 devices may experience communication errors |
| | 4841/4842 (Device Type 16) | 256 | Yes | On | Changing the damping of a DVC6000 connected to a MTL 4841 multiplexer (4841 rev 1, hardware rev 1, software rev 5) may cause the device to lose communication with the ValveLink SNAP-ON application. |
| | 4850 | 32 | Yes | On | |
| | 4850-TR | 32 | Yes | Off | |
| | 4851-4852 | 16 | Yes | Off | |
| | 4854 | 32 | Yes | Off | |
| | 8000/8512 | 256 | No | Off | |

**Table 2-1: Supported HART Multiplexers *(continued)***

| Manufacturer | Model | Max Channels | Hardware supports Enhanced Polling | Default in AMS Device Manager | Notes |
|---|---|---|---|---|---|
| Spectrum | Connects (v6.0, 6.1) | 256 | No | Off | If you have a Spectrum CONNECTS multiplexer, you will need to have additional software installed on your PC. Contact Spectrum for details (www.spectrumcontrols.com). |
| Phoenix Contact | GW PL ETH/ BASIC-BUS with GW PL ETH/UNI-BUS and GW PL HART4-BUS | | | | Burst mode is not supported. Also, problems seen when P&F USB modem installed on the same station. (part numbers 2702321, 2702233, 2702234) |
| Emerson Machine Automation Solutions | PACSystems HART Multiplexer | 16,384 | No | Off | Virtual Mux (v 1.2) |
| GM International | 5700-110 | 256 | No | No | Software Rev 0, Hardware Rev 1 |

1 *P+F KFD2-HMM-16 multiplexers behave differently than the other multiplexers in duplicate device ID situations. When duplicate devices are attached to these multiplexers, the duplicate device ID icons are not displayed and only one of the duplicate devices will show up in the multiplexer hierarchy. AMS Device Manager cannot determine that multiple devices have the same device ID. However, AMS Device Manager does recognize that the multiplexer thinks it has more devices than what it is telling AMS Device Manager in its device list, and AMS Device Manager logs this information in the Windows Event Log. Revisions 5 - 9 of the P+F KFD2-HMM-16 multiplexer are not supported. Appears as HART Multiplexer 255-way.*

For specific information about a supported multiplexer, see the manufacturer's documentation. For more information about multiplexer networks, see *KBA NA-0400-0084*.

## 2.6.6 Wireless

The Wireless System Interface allows you to view and configure *Wireless*HART devices in a Wireless Network. A Wireless Network is made up of one or more wireless gateways and *Wireless*HART devices.

The Wireless System Interface requires:

- An Ethernet adapter to connect to the gateway.
- One or more wireless gateways that allow communication between the AMS Device Manager station and a collection of wireless devices.
- *Wireless*HART devices. See the *AMS Device Manager Supported Device List* for a list of supported *Wireless*HART devices.
- A valid SSL certificate (if using the recommended Security Setup utility) allowing the AMS Device Manager station to securely communicate with the gateway. See *AMS Device Manager Books Online* and the *Smart Wireless Gateway* manual for more information about the Security Setup utility and certificate.

AMS Device Manager supports the following wireless gateways:

- 2.4 GHz Rosemount Rev 2 1420 versions 3.9.5 and later
- 2.4 GHz Rosemount Rev 3 1420 versions 4.2.9 and later
- 2.4 GHz Rosemount Rev 4 1420 versions 4.3.17 and later
- 2.4 GHz Rosemount Rev 4 1410/1420 and Cisco 1552WU version 4.4.30 and later
- 2.4 GHz Rosemount Rev 5 1410/1420 and Cisco 1552WU version 4.5.27 and later

**Note**
The 2.4 GHz Rosemount Rev 2 1420 version 3.9.5 gateway does not support HART 6 devices.

## 2.7 AMS Device View

Once you have installed the AMS Device View web server. you can use a supported browser to launch AMS Device View screens. Desktop/laptop browsing of AMS Device View data and opening device details screens can only be launched from a Windows PC.

### 2.7.1 AMS Device Manager compatibility with AMS Device View

AMS Device View requires AMS Device Manager 14.5 FP1. You can install AMS Device View on a standalone PC without AMS Device Manager or co-deployed with AMS Device Manager. If you install AMS Device View on a standalone PC or on a Client SC Station, the installation will prompt you to enter the Server Plus Station name or IP address and the AMSDBUser password. If AMS Device View is installed on a non-AMS Device Manager station, you will need to manually install certificates to ensure secure communications. See the videos for AMS Device View on the AMS Device Manager media at \Certificate_Videos.

**Note**
You do not need to enter the AMSDBUser password if it has not been changed.

## 2.7.2 DeltaV compatibility with AMS Device View

To deploy AMS Device View on the control network, install the AMS Device View web server on a DeltaV Application Station. Alternatively, it can be installed on the DeltaV ProfessionalPlus station, but this is NOT recommended. If you want to access AMS Device View on the plant network, we recommend that you install the AMS Device View web server on a standalone PC in a demilitarized zone above the control network.

DeltaV security settings prevent correct installation of AMS Device View. You will need to temporarily change group policy settings on the PC when installing AMS Device View on a DeltaV station. See KBA NK-2200-0080 for details.

**Note**
AMS Device View is not supported on any other DeltaV stations. AMS Device View is not supported on a PC with Plant Messenger installed.

# 3 Install AMS Device Manager

AMS Device Manager can be installed as a single-station system or as a multi-station, distributed system. The single-station system is a Server Plus Station that maintains the AMS Device Manager database, with no associated Client SC Stations. A distributed AMS Device Manager system is a client/server deployment of AMS Device Manager Stations. It allows multiple AMS Device Manager Stations access to a common database and all connected devices in the distributed system.

A distributed system contains a Server Plus Station and one or more Client SC Stations. Each station has access to a common database located on the Server Plus Station.

The procedures in this chapter are for installing and configuring AMS Device Manager on the following types of stations:

- Server Plus Station
- Client SC Station

For a distributed system to function as intended, all Client SC Stations must have network access to the Server Plus Station. The Server Plus Station must be able to successfully ping each Client SC Station by computer name. You can install a Client SC Station first if that is required for your network configuration (for example, if installing on domain controllers and non-domain controllers). Otherwise, it is recommended that AMS Device Manager software be installed first on the PC to be the Server Plus Station (see page 41), and then on each PC to be used as a Client SC Station (see page 42). All stations must use the same revision of AMS Device Manager software.

If you are installing an AMS Device Manager distributed system on domain controller PCs or a mix of domain controllers and non-domain controller PCs, do all the domain controller installations first (see page 54).

If you are installing an AMS Device Manager distributed system on a workgroup, a common username and password is required and should be added to the AMSDeviceManager Windows user group on every AMS Device Manager station on the workgroup.

If you are installing AMS Device Manager on a DeltaV station, see page 57.

If you are installing an AMS Device Manager distributed system and the Server Plus Station is separated from the Client SC Station(s) by a firewall, refer to AMS Device Manager Product Security Guide.

If you are installing AMS Device Manager on a PC that has AMS Wireless Configurator installed, see page 40.

**Note**
It is recommended that you install AMS Device Manager before installing antivirus software. Check the Knowledge Base Articles if there are known issues with your antivirus software.

**Important**
Do NOT install AMS Device Manager and Plantweb Optics™ on the same PC.

# 3.1 Upgrade an AMS Device Manager system

When you upgrade to a new version of AMS Device Manager, the installation process overwrites all existing files located in the AMS folder (except the database files and license files).

**⚠ CAUTION**

Before you upgrade, you should back up your database as a precaution against loss of data (see page 7). Make sure you have installed the latest Hotfix bundle for the version you are using before upgrading.

The backup files are not changed during installation. In the unlikely event that database files are damaged or altered in some way, you can use the backup files to restore the database.

Upgrading to AMS Device Manager 14.5 FP1 from version 13.1.1 and higher does not require you to uninstall previous versions and restore the database after installation. See Upgrade an AMS Device Manager Server Plus Station or Upgrade an AMS Device Manager Client SC Station.

Upgrading to AMS Device Manager 14.5 FP1 from version 13.0 or lower requires you to back up the database and uninstall the previous version.

### Table 3-1: Upgrade an AMS Device Manager Server Plus Station 13.1.1 or higher

| Server Plus Station to Server Plus Station | Server Plus Station to Client SC Station |
|---|---|
| 1. Check in all calibration routes.<br>2. Clear all existing alerts from Alert Monitor.<br>3. Back up the database (see page 7).<br>4. Consolidate existing databases, if necessary (see page 47).<br>5. Uninstall SNAP-ON applications, (except ValveLink SNAP-ON), Device Description Update Manager, AMS Device Manager Asset Source Interface (ASI), and Web Services, if installed. See the Knowledge Base Article on AMS Device Manager ASI for details on uninstalling that product.<br>6. Uninstall AMS Device Manager Calibration Connector application, if installed.<br>7. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing).<br>8. Remove any configured HART Over PROFIBUS System Interfaces.<br>9. Stop any programs or processes that access AMS Device Manager Server .<br>10. Stop AMS Device Manager Server in system tray if running.<br>11. Install Server Plus Station software (see page 41).<br>12. Get new license codes (see page 45).<br>13. Add or edit users (see *AMS Device Manager Books Online*).<br>14. Reapply the DeltaV System Interface[1], if applicable.<br>15. Install required SNAP-ON applications (see page 55).<br>16. Install AMS Device Manager Calibration Connector application, if applicable.<br>17. Install new Softing smartLink components, if applicable.<br>18. Configure HART-IP System Interfaces, if applicable.<br>19. If the Server Plus will have system interfaces, copy the .cer file found in AMS folder to the AMS folder on all Client SC stations.<br>20. Install the latest version of AMS Device Manager Asset Source Interface, and Web Services, if required (see page 55). See the Knowledge Base Article on AMS Device Manager ASI for details on installing that product.<br>21. Copy device manuals (see page 10). | 1. Check in all calibration routes.<br>2. Clear all existing alerts from Alert Monitor.<br>3. Uninstall SNAP-ON applications, (except ValveLink SNAP-ON) Device Description Update Manager, AMS Device Manager Asset Source Interface, and Web Services, if installed. See the Knowledge Base Article on AMS Device Manager ASI for details on uninstalling that product.<br>4. Uninstall AMS Device Manager Calibration Connector application, if installed.<br>5. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing).<br>6. Remove any configured HART Over PROFIBUS System Interfaces.<br>7. Stop any programs or processes that access AMS Device Manager Server.<br>8. Stop AMS Device Manager Server in system tray if running.<br>9. Uninstall previous AMS Device Manager Server software (see page 8).<br>10. Install Client SC Station software (see page 42).<br>11. Get new license codes.<br>12. Install required SNAP-ON applications (see page 55).<br>13. Add or edit users (see *AMS Device Manager Books Online*).<br>14. Configure required communication interfaces.[1]<br>15. Install new Softing smartLink components, if applicable.<br>16. Configure HART-IP System Interfaces, if applicable.<br>17. If the Client SC will have system interfaces, copy the .cer file found in AMS folder to the AMS folder on the Server Plus station and any other Client SC stations.<br>18. Copy device manuals (see page 10). |

### Table 3-2: Upgrade an AMS Device Manager Client SC Station 13.1.1 or higher

| Client SC Station to Server Plus Station | Client SC Station to Client SC Station |
|---|---|
| 1. Check in all calibration routes.<br>2. Clear all existing alerts from Alert Monitor.<br>3. Back up the database (see page 7).<br>4. Uninstall SNAP-ON applications (except ValveLink SNAP-ON) and Web Services, if installed.<br>5. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing).<br>6. Remove any configured HART Over PROFIBUS System Interfaces.<br>7. Stop any programs or processes that access AMS Device Manager Server.<br>8. Stop AMS Device Manager Server in system tray if running.<br>9. Uninstall previous AMS Device Manager Server software (see page 8).<br>10. Install Server Plus Station software (see page 41).<br>11. Get new license codes (see page 45).<br>12. Add or edit users (see *AMS Device Manager Books Online*).<br>13. Configure required communication interfaces[1].<br>14. Install required SNAP-ON applications (see page 55).<br>15. Install AMS Device Manager Calibration Connector application, if applicable (see page 59).<br>16. Install new Softing smartLink components, if applicable.<br>17. Configure HART-IP System Interfaces, if applicable.<br>18. If the Server Plus will have system interfaces, copy the .cer file found in AMS folder to the AMS folder on the Client SC stations.<br>19. Install latest version of Device Description Update Manager, AMS Device Manager Asset Source Interface, and Web Services, if required (see page 55). See the Knowledge Base Article on AMS Device Manager ASI for details on installing that product.<br>20. Copy device manuals (see page 10). | 1. Uninstall SNAP-ON applications (except ValveLink SNAP-ON) if installed.<br>2. Clear all existing alerts from Alert Monitor.<br>3. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing).<br>4. Remove any configured HART Over PROFIBUS System Interfaces.<br>5. Stop any programs or processes that access AMS Device Manager Server .<br>6. Stop AMS Device Manager Server in system tray if running.<br>7. Install Client SC software (see page 42).<br>8. Add or edit users (see *AMS Device Manager Books Online*).<br>9. Reapply the **DeltaV** System Interface, if applicable[1].<br>10. Install required SNAP-ON applications (see page 55).<br>11. Install new Softing smartLink components, if applicable.<br>12. Configure HART-IP System Interfaces, if applicable.<br>13. If the Client SC will have system interfaces, copy the .cer file found in AMS folder to the AMS folder on the Server Plus station, and other Client SC stations.<br>14. Copy device manuals (see page 10). |

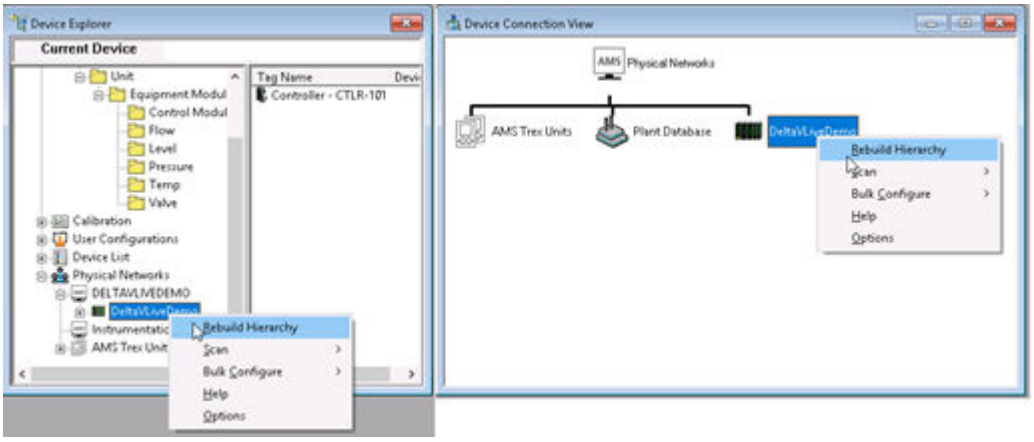
| Upgrade notes |
| --- |
| [1]The **DeltaV** System Interface requires that you re-apply the interface after upgrading AMS Device Manager. To do this, in the Network Configuration utility, display the properties of the **DeltaV** System Interface, click **OK**, and then click **Close**.<br>Manually installed Device Descriptions that are still not included in the AMS Device Manager 14.5 FP1 installation must be reinstalled after the upgrade. |

### Table 3-3: Upgrade from AMS Device Manager 12 to 13.0

| Upgrade from version 12.0-13.0 |
| --- |
| 1. Back up the database (see page 7).<br>2. Uninstall SNAP-ON applications (except ValveLink SNAP-ON) and Web Services, if installed.<br>3. Uninstall AMS Device Manager (see page 8).<br>4. Ensure the PC meets system requirements (see page 13).<br>5. Install AMS Device Manager 14.5 FP1 (see page 41 or page 42, depending on the type of installation needed).<br>6. Install required SNAP-ON applications (see page 55).<br>7. Restore your database (see page 8). |
| **Notes** |
| If you are upgrading from a version lower than 12.x, contact your Emerson Sales/Service Office for assistance. |

After you have completed the upgrade,

- Configure any required system interface networks and then open AMS Device Manager 14.5 FP1. Right-click each of the network icons and select **Rebuild Hierarchy** followed by **Scan → New Devices**.




If you are using the Alert Monitor feature, click **Alert Monitor** on the AMS Device Manager toolbar to open the Alert List. Click **Station Monitoring** on the Alert Monitor toolbar and ensure that the station you are monitoring is checked.

- From the Windows Start menu on each station, select **AMS Device Manager → Certificate Manager** and Import certificates from any other stations to ensure secure communications between components.

### 3.1.1 Upgrade from AMS Wireless Configurator

To install an AMS Device Manager Server Plus Station or **Client SC Station** on a PC that has **AMS Wireless Configurator** installed:

#### Procedure

1. Contact your Emerson Sales/Service Office to get new license codes for AMS Device Manager.
2. Back up the database (see page 7).
3. Right-click the AMS Device Manager Server icon in the Microsoft Windows system tray and select **Stop AMS Device Manager Server** from the context menu.
4. Open the Windows Control Panel and use Programs and Features to remove **AMS Wireless Configurator**.
5. Install AMS Device Manager (see Install Server Plus Station software or Install Client SC Station software).
6. Do one of the following:
   - If you installed a Server Plus Station in the previous step, license AMS Device Manager (see page 45) and restore your backed-up database (see page 8).
   - If you installed a **Client SC Station** in the previous step, you may need to consolidate your backed-up **AMS Wireless Configurator** database with an existing database (see page 47).

### 3.1.2 Upgrade from AMS Device Configurator for DeltaV

AMS Device Configurator for DeltaV is a limited-feature version of AMS Device Manager provided to DeltaV users, and does not require a license. To upgrade to the full version of AMS Device Manager:

#### Procedure

1. Contact your Emerson Sales/Service Office to get new license codes for AMS Device Manager.
2. Right-click the AMS Device Manager Server icon in the Microsoft Windows system tray and select **Stop AMS Device Manager Server** from the context menu.
3. License AMS Device Manager (see page 45).
4. Restart your PC.
5. Start AMS Device Manager.

# 3.2 Install Server Plus Station software

**Notes**

- If you are upgrading your software and changing the station type, you must uninstall the earlier version of AMS Device Manager before upgrading to AMS Device Manager 14.5 FP1. (See Table 3-1). If changing domains or moving a PC from a workgroup to a domain, you must uninstall and reinstall AMS Device Manager.
- If you are installing an AMS Device Manager distributed system using a domain controller, see page 54 for other requirements.

**Procedure**

1. Exit/close all Windows programs, including any running in the background (including virus scan software).
2. Browse to the AMS Device Manager .ISO image.
3. Double-click AMSDeviceManager_Setup.exe.
4. Click **Next**.
5. Accept the License Agreement and click **Next**.
6. Read the *Release Notes* and click **Yes**.
7. Optional: If you are upgrading AMS Device Manager from a previous version, click **Yes**. If you want to install AMS Device Manager on a different location or install a different AMS Device Manager station type, click **No**. See Upgrade an AMS Device Manager system for more information on AMS Device Manager upgrade options.
8. Click **Server Plus Station**.
9. Select the AMS Device Manager components you want to install:
   - HART Modem Driver
   - DTM Launcher Application
10. Follow the prompts.

**NOTICE**

Do not interrupt the installation process, or the software will not be fully installed and will malfunction. The installation process includes some system restarts. Do not remove the media until the installation is complete.

**Note**

If you are installing on a PC with User Account Control enabled, the User Account Control dialog displays after rebooting the PC. Select **Yes** to continue with the AMS Device Manager installation.

If you do not click **Yes** within 2 minutes, the dialog closes and to complete the installation you must select **Start** → **All Programs** → **AMS Device Manager** → **Continue the AMS Device Manager installation**.

11. If the **Remove old Emerson Instance Name** dialog appears, it is recommended to remove old versions to prevent performance issues. Select the instance you want to remove and click **Remove**. Otherwise, click **Skip**.
12. Enter a new AMS Device Manager system password. This password must meet OS complexity requirements, and must be identical for all AMS Device Manager stations.
13. License AMS Device Manager (see page 45).
14. If you are installing a distributed system, configure the Server Plus Station to recognize each station connected in the system (see page 46). This step is essential for the other stations to access the Server Plus Station.
15. If your Server Plus station will host system interfaces, copy the .cer file found in the AMS folder to the AMS folder on the Client SC stations.
16. Set up and configure the system interfaces needed on this station (see page 61).
17. Optional: Install the latest versions of any licensed SNAP-ON applications (see page 55).
18. Open AMS Device Manager, right-click each of the network icons and select **Rebuild Hierarchy** followed by **Scan → New Devices**.
19. If you are using the Alert Monitor feature, click the **Alert Monitor** button on the AMS Device Manager toolbar to open the Alert List. Click the **Station Monitoring** button in the toolbar and ensure that the station you are monitoring is checked. Only stations with system interfaces configured need to be checked.

During installation, the **AMSDeviceManager** Windows user group is given access to the AMS folder, subfolders, and files. When an administrator adds specific Windows users in the AMS Device Manager User Manager utility, these users are automatically added to the AMSDeviceManager Windows user group. However, they have no ability to use AMS Device Manager features until permissions are assigned to them in User Manager.

The installation creates a share of the AMS folder. This allows connected Client SC Stations to access the Server Plus Station. It also allows connected Client SC Stations to use the Drawings/Notes feature of AMS Device Manager. If your situation makes this security configuration undesirable, consult your operating system documentation or your system administrator.

From the Windows Start menu on each station, select **AMS Device Manager → Certificate Manager** and Import certificates from any other stations to ensure secure communications between components.

**Note**
The AMS Device Manager installation program turns off Windows Automatic Updates. After AMS Device Manager is installed, check to see that the Windows Automatic Updates function is set as desired.

# 3.3 Install Client SC Station software

### Procedure

1. Verify Client SC Station connectivity.

Use the ping command to verify that the designated Client SC Station PC responds to communications sent to it by the Server Plus Station.

a) At the AMS Device Manager Server Plus Station, enter CMD on the **Start** screen.

b) At the command prompt, enter `PING <Client SC Station Computer Name>`.

c) Press ENTER.

d) Verify that the Client SC Station PC responds to the ping command.

The ping command should return a reply message. If the ping command fails, verify that you entered the correct PC name in the command line. Also verify that your network is functioning properly. Contact your IT department if you cannot establish connectivity.

2. Exit/close all Windows programs, including any running in the background (including virus scan software).
3. Browse to the AMS Device Manager .ISO image.
4. Double-click AMSDeviceManager_Setup.exe.
5. Click **Next**.
6. Accept the License Agreement and click **Next**.
7. Read the *Release Notes* and click **Yes**.
8. Click **Client SC Station**.
9. Select the AMS Device Manager components you want to install:
   - HART Modem Driver
   - DTM Launcher Application
10. Follow the prompts.

**NOTICE**

Do not interrupt the installation process, or the software will not be fully installed and will malfunction. The installation process includes some system restarts. Do not remove the media until the installation is complete.

**Note**

If you are installing on a PC with User Account Control enabled, the User Account Control dialog displays after rebooting the PC. Select **Yes** to continue with the AMS Device Manager installation.

If you do not click **Yes** within 2 minutes, the dialog closes and to complete the installation you must select **Start** → **All Programs** → **AMS Device Manager** → **Continue the AMS Device Manager installation**.

11. Enter a new AMS Device Manager system password. This password must meet OS complexity requirements, and must be identical for all AMS Device Manager stations.
12. License AMS Device Manager (see page 45).

13. Add the user to the AMSDeviceManager group (from Windows Control Panel launch User Accounts. Select Manage User Accounts. From the Advanced tab, select Advanced, and select Groups. Right-click AMSDeviceManager, and select Add to Group...).
14. If the Client SC station will host system interfaces, copy the .cer file found in AMS folder to the AMS folder on the Server Plus and any Client SC stations.
15. Set up and configure the system interfaces needed on this station (see page 61).
16. Optional: Install the latest versions of any licensed SNAP-ON applications (see page 55).
17. Open AMS Device Manager, right-click each locally configured network icon and select **Rebuild Hierarchy** and then **Scan → New Devices**.
18. If you are using the Alert Monitor feature, click the **Alert Monitor** button on the AMS Device Manager toolbar to open the Alert List. Click the **Station Monitoring** button in the toolbar and ensure that the station you are monitoring is checked. Only stations with system interfaces configured need to be checked.

**Notes**

- The AMS Device Manager installation program turns off Windows Automatic Updates. After AMS Device Manager is installed, check to see that the Windows Automatic Updates function is set as desired.
- You must add the Windows user as a user in AMS Device Manager User Manager (see *AMS Device Manager Books Online*) or the AMS Device Manager Server icon will not display in the Windows system tray.
- From the Windows Start menu on each station, select **AMS Device Manager → Certificate Manager** and Import certificates from any other stations to ensure secure communications between components.

## 3.4 Install the AMS Device View web server

If your Server Plus PC is on a different domain, follow the cross-domain rules specified in KBA NA-0800-0113 before installing AMS Device View.

**Procedure**

1. Install IIS.
2. Exit/close all Windows programs, including any running in the background (including virus scan software).
3. Browse to the AMS Device Manager .ISO image.
4. In the AMS Device View folder, double-click AMSDeviceView_Setup.exe.
5. If a message about third-party components is displayed, click OK.
6. Restart your PC, if prompted.
7. Click **Next**.
8. Choose the deployment type.
9. Enter the activation code and click **Next**.

**Note**
For information on how to get your activation code, follow the installation prompts.

10. Accept the License Agreement and click **Next**.
11. Do one of the following:
    - Click **Next** to install AMS Device View in the default location.
    - Click **Browse** to select a different location, and click OK.
12. Click **Next**.
13. The AMS Device View Server Config dialog is displayed if you are installing on a PC without the Server Plus Station installed. Enter the Server Plus Station PC name or IP address and the AMSDbUser Password and click **Configure**.

**Note**
If the AMSDbUser Password has not been changed, leave the default entry and click **Configure**.

14. Click **Finish**.
15. If co-deployed on an AMS Device Manager station, run Terminate Servers from the AMS menu. If the AMS Device View web server is not on an AMS station, skip to step 18.
16. Run Certificate Manager, and in the Local Certificate Status pane, select the vertical bar menu for the AMSSuite.Client certificate, and choose **Export**. Copy the .cer file to the /AMS folder on the Server Plus station.
17. On the Server Plus station, run Terminate Servers from the AMS menu. Run Certificate Manager, and from the Install tab, choose the AMSSuite.Client certificate, and select **Install**. Skip to step 20.
18. Install AMS Device View certificates on the appropriate PCs. Emerson requires secure communications. See the videos for AMS Device View on the AMS Device Manager media at \Certificate_Videos.
19. To associate the installed certificates with AMS Device Manager Database, run AMSDeviceViewCertificateRegistration.exe utility in the\AMS\bin folder.
20. In AMS Device Manager User Manager, add the PC name of the AMS Device View web server, and any usernames on that PC.

## 3.5 License AMS Device Manager

All licensing for an AMS Device Manager system is done on the Server Plus Station. After installation, start the Licensing Wizard and follow the prompts to gather registration information. Have the Machine Fingerprint generated from the Licensing Wizard, as well as your System ID available to register the software. You will enter them on the registration web page.

https://guardian.emerson.com/Guardian/Pages/AmsRegistration/

When you receive your license, run the Licensing Wizard on the Server Plus Station to enter your license, which enables your system.

**Note**
During the licensing process, you must have read access to the PC disk drive you installed on (C: drive by default) so that the Licensing Wizard can uniquely identify the PC.

### Procedure

1. Enter `Licensing Wizard` on the **Start** screen and click **Licensing Wizard**.
2. Follow the instructions in the Licensing Wizard. Take note of the Machine Fingerprint for the next step.
3. To register your system and generate a license file, click **Register**. This will take you to the registration web page. Enter required information.
4. You will receive a license file. Save it to a location accessible from the Server Plus station.
5. In the Licensing Wizard, click **Browse** and select the file.
6. If you are installing new license information on an existing station, start AMS Device Manager to see the changes.

## 3.6 License AMS Device View

You need an activation code to install AMS Device View. To get the activation code, email Emerson Worldwide Customer Service or call Toll-Free 888.367.3774 (U.S. and Canada) or +63.2.702.1111 (Rest of World) and provide your AMS Device Manager system ID. Your system ID can be found by opening **Help** → **About AMS Device Manager** on your AMS Device Manager system.

## 3.7 Register your product with SureService

### Prerequisites

Install and license your AMS Device Manager stations.

### Procedure

1. Run the **SureService Registration** application from the AMS Device Manager Windows Start menu of the Server Plus station.
2. Retrieve the latest-generated registration file that ends with “SysRegData.epm” in the `\AMS\Db\xml\EPM` folder.
3. Upload the file on the Guardian website under **System Info** → **Registration**.

## 3.8 Configure and secure a Distributed System

Before you can use your distributed system, you must configure the Server Plus Station so the Client SC Stations can access the Server Plus Station. In addition, any Server Plus station, and stations with a configured System Interface after copying their certificate to all other stations, must run Certificate Manager on those stations.

### Procedure

1. On the Server Plus Station, enter `Station Configuration` on the **Start** screen and click **Station Configuration**.
2. In the Station Configuration dialog, click **Add**.
3. Enter the computer name of the Client SC Station PC (see page 48), and click **OK**.

**Note**
The station name is not case-sensitive. Do not include a domain name or any other characters that are not part of the computer name. Use station names of 15 ISO Latin-1 characters or less.

4. Repeat steps 2 and 3 for each licensed Client SC Station, and click **Close** when done.
5. Restart AMS Device Manager on the Server Plus station.
6. From the Server Plus station, and each station with a configured System Interface, copy the .cer file found in the /AMS folder to the /AMS folder on all other stations. If you are using corporate certificates, copy the .PFX or .P12 certificate provided by your organization to the /AMS folder.
7. Run Terminate Servers from the AMS folder of the Windows start menu on each station.
8. Run Certificate Manager in the AMS folder of the Windows start menu on each station. Follow the prompts on the **Install** tab.

## 3.8.1 Consolidate databases

If you have multiple Server Plus Stations, you can consolidate their databases for use in a distributed system.

### Procedure

1. Back up the current database on all stations containing a database you want to consolidate (see page 7).
2. Select one of the Server Plus Stations to hold the consolidated database. Import the database information from the other Server Plus Stations one at a time. This may be done using one of the following methods.

   **Method 1**

   Use this method when all the stations are connected to the same network and domain and at the same AMS Device Manager revision level.

   - Right-click the **Plant Database** icon on the designated consolidation Server Plus Station, select **Import** → **From Remote** to import the database from the other stations one at a time. Click **Help** on the **Import From Remote System** dialog for instructions.

**Note**
To Import > From Remote, you must have AMS Device Manager System Administration permissions.

**Method 2**

Use this method when the stations are not connected to a common network.

- From the **Plant Database** icon on all the non-consolidation Server Plus Stations, select **Export → To <type> Export File** to prepare a database merge file. Click **Help** on the **AMS Device Manager Export** dialog for instructions.

3. When the databases have been consolidated, perform a database backup of the consolidated database.
4. The AMS Device Manager 14.5 FP1 Server Plus Station can be installed using one of the following methods:
   - Install AMS Device Manager 14.5 FP1 as a station upgrade, if upgrading from version 13 or later which automatically migrates the consolidated database (see page 36).
   - Uninstall the 10.0-12.5 station software and install AMS Device Manager 14.5 FP1 as a new Server Plus Station (see page 41). Restore the consolidated database (see page 8).

## 3.8.2 Consolidate Service Notes

The database backup operation also creates a backup file of service notes. If you would like to consolidate the service notes from multiple AMS Device Manager stations, follow the relevant instructions in the readme file for the Drawings and Notes Management Utility. This information is included in the `Tech_Support_Utilities \DrawingsAndNotesUtility` folder on the AMS Device Manager media.

## 3.8.3 Determine computer names

Computer names are needed to identify the Server Plus Station and the connected Client SC Stations during distributed system installation and configuration (see page 46). Due to a Windows networking requirement, station names must be 15 bytes or less. Please note that some languages have characters that use more than 1 byte.

To find and record a computer name (do not use IP addresses):

1. Right-click the Windows desktop **This PC** icon and select **Properties**.
2. Record the name of each computer that will be part of your distributed system (see the Computer name log example below).

**Note**
Computer names and DNS names must be the same. “Localhost” cannot be used for AMS Device View. Do not include “\\” in any computer names.

**Figure 3-1: Computer name log example**

| | A | B |
|---|---|---|
| 1 | **Station** | **Computer Name** |
| 2 | Server Plus Station | AMS-ServerPlus |
| 3 | Client SC Station 1 | AMS-ClientSC1 |
| 4 | Client SC Station 2 | AMS-ClientSC2 |
| 5 | Client SC Station 3 | AMS-ClientSC3 |
| 6 | Client SC Station ... | AMS-ClientSC... |
| 7 | | |

# 3.9 Modify a Distributed System

Once your distributed system is installed, any changes to its physical configuration may require special procedures in AMS Device Manager. If you are moving the PC where AMS Device Manager is currently installed from a Domain to a Workgroup, or vice-versa, you will need to uninstall and reinstall AMS Device Manager.

To change station types in an existing system, see page 49. For other types of changes, see the following:

- Change a Client SC Station to access a different Server Plus Station.
- Add Client SC Stations.
- Replace a Server Plus Station PC.
- Replace a Client SC Station PC.
- Rename a Server Plus Station PC.
- Rename a Client SC Station PC.
- Add a new communication interface.
- Add more tags than currently licensed.

## 3.9.1 Change station types

If you are changing station types, perform the following appropriate procedures. You may also need to reset your users' permissions (see page 61).

### Change a Server Plus Station to a Client SC Station

#### Procedure

1. Back up the database (see page 7).
2. Uninstall the previous Server Plus Station software (see page 8).
3. Ensure that a connection can be made to an available Server Plus Station.
4. Install the Client SC Station software (see page 42).
5. Restore or combine the database on another Server Plus Station (see page 8).

### Change a Client SC Station to a Server Plus Station

#### Procedure

1. Contact your Emerson Sales/Service Office to get new license codes for AMS Device Manager.
2. Uninstall the previous Client SC Station software (see page 8).
3. Install the Server Plus Station software (see page 41).
4. License AMS Device Manager (see page 45).

## 3.9.2 Change a Client SC Station to access a different Server Plus Station

#### Procedure

1. In Network Configuration on the Client SC Station, remove any configured system interfaces (other than HART Modem and Calibrator).
2. Enter `Server Plus Connect` on the **Start** screen and click the **Server Plus Connect**.
3. In the Server Plus Connect dialog, select a **Server Plus Station PC** from the drop-down list or enter the name of the PC where the desired Server Plus Station is installed.
4. Click **Connect**.

**Note**
For more information about the Server Plus Connect utility, refer to *AMS Device Manager Books Online*.

The Server Plus Connect utility cannot be used on Client SC Stations installed on DeltaV workstations. In these configurations, use the procedure below.

1. Uninstall AMS Device Manager on the Client SC Station (see page 8).
2. Reinstall AMS Device Manager on the Client SC Station and indicate the new Server Plus Station (see page 42).

## 3.9.3 Add Client SC Stations

To expand an existing distributed system:

#### Procedure

1. Determine the number of stations covered by your current license (select **Help** → **About** from the AMS Device Manager toolbar).
   - To add stations that will be covered by your current license, continue with step 2.
   - To add more stations than currently licensed, contact your Emerson Sales/Service office to get new license codes. After you receive your new license

codes, run the Licensing Wizard on the Server Plus Station (see page 45) and then continue with step 2.

2. To install AMS Device Manager on the added Client SC Stations, see page 42.
3. Update the Client SC Station configuration on the Server Plus Station (see page 46).
4. To enable the stations in the distributed system to recognize the added Client SC Station, shut down and restart AMS Device Manager on the Server Plus station.

## 3.9.4 Replace a Server Plus Station PC

### Procedure

1. Contact your Emerson Sales/Service Office to get new license codes for AMS Device Manager.
2. Back up the database (see page 7).
3. Uninstall AMS Device Manager from the old PC (see page 8). Rename or disconnect the PC from the network.
4. Connect the new PC to the network and give it the same computer name as the old PC.

**Note**
If the new Server Plus Station PC has a different computer name, all active alerts that were in the Alert List on the old PC will be lost. In addition, you will be required to run the Server Plus Connect utility on all Client SC Stations to connect to the new Server Plus Station (see page 50).

5. Install Server Plus Station software on the new PC (see page 41).
6. License AMS Device Manager (see page 45).
7. Set up the server configuration to recognize each Client SC Station connected in the system (see Configure and secure a Distributed System).
8. Restore the database (see page 8).

## 3.9.5 Replace a Client SC Station PC

### Procedure

1. Uninstall AMS Device Manager from the old PC (see page 8). Disconnect the PC from the network, if appropriate.
2. Connect the new PC to the network.
3. On the Server Plus Station, enter `Station Configuration` on the **Start** screen and click **Station Configuration**.
4. In the Station Configuration dialog, select the name of the old PC and click **Remove**.
5. In the Station Configuration dialog, click **Add**.
6. Enter the computer name of the new Client SC Station PC (see page 48 ), and click **OK**. The station name is not case-sensitive. Do not include a domain name or any other characters that are not part of the computer name.

7. On the new Client SC Station PC, install the Client SC Station software (see page 42).

## 3.9.6 Rename a Server Plus Station PC

**Note**
If you have a system interface configured on the Server Plus Station, the Device Monitor List and Alert Monitor alerts will be lost when the PC is renamed.

**Procedure**

1. Back up the database (see page 7).
2. Record all devices contained in the Device Monitor List.
3. Uninstall AMS Device Manager on the Server Plus Station (see page 8).
4. Rename the Server Plus Station PC:
   a) Right-click the Windows desktop My Computer icon.
   b) Select **Properties**.
   c) On the Computer Name tab, click **Change**.
   d) Enter a new computer name and click **OK**.
   e) Click **OK**.
5. Install AMS Device Manager on the Server Plus Station (see page 41).
6. Restore the database backed up in step 1 (see page 8).
7. Reinstall the required system interfaces (see page 61) and SNAP-ON applications (see page 55).
8. Open AMS Device Manager, right-click each network icon, and select **Rebuild Hierarchy** and then **Scan → New Devices**.
9. Add the devices recorded in step 2 to the Device Monitor List (refer to *AMS Device Manager Books Online*).

## 3.9.7 Rename a Client SC Station PC

**Note**
If you have a system interface configured on the Client SC Station, the Device Monitor List and Alert Monitor alerts will be lost when the PC is renamed.

**Procedure**

1. Record all devices contained in the Device Monitor List.
2. Uninstall AMS Device Manager on the Client SC Station PC (see page 8).
3. Rename the Client SC Station PC:
   a) Right-click the Windows desktop My Computer icon.
   b) Select **Properties**.
   c) On the Computer Name tab, click **Change**.

d) Enter a new computer name and click **OK**.

e) Click **OK**.

4. On the Server Plus Station, open Station Configuration and remove the old name of the Client SC Station PC and add the new name (see page 46).
5. Install AMS Device Manager on the Client SC Station PC (see page 42).
6. Reinstall the required system interfaces (see page 61) and SNAP-ON applications (see page 55).
7. Open AMS Device Manager, right-click each network icon, and select **Rebuild Hierarchy** and then **Scan → New Devices**.
8. Add the devices recorded in step 1 to the Device Monitor List on the Client SC Station (refer to *AMS Device Manager Books Online*).

## 3.9.8 Add a new communication interface

### Procedure

1. Contact your Emerson Sales/Service Office to get a new license code for the desired communication interface.
2. Run the Licensing Wizard on the Server Plus Station (see page 45).
3. Configure the new communication interface (see *AMS Device Manager Books Online*).

## 3.9.9 Add more tags than currently licensed

### Procedure

1. Contact your Emerson Sales/Service Office to get new license codes to cover the number of tags needed.
2. Run the Licensing Wizard on the Server Plus Station (see page 45).
3. Start AMS Device Manager.
4. Install and configure the additional devices.

# 3.10 Installing AMS Device Manager on domain controllers

AMS Device Manager creates Windows user accounts on each station in a distributed system. When AMS Device Manager is installed on a domain controller, these accounts are created as domain users. Communication failures will result if installation is not done correctly as follows:

- If Windows domain controllers are used in a distributed network, the AMS Device Manager station on the domain controller must be installed first before any other station on the common network domain. If AMS Device Manager is installed on a domain controller, all other stations that are part of that domain use the domain account, not a local account. Microsoft SQL Server 2019 Reporting Services is not allowed on a Windows domain controller due to Microsoft Windows restrictions, so Bulk Transfer reports will not work.
- If installing AMS Device Manager in a domain deployment, and access to an AMSServiceUser Windows account on the domain controller is required, the Windows user must be a domain administrator for the AMSServiceUser to be installed correctly.
- If AMS Device Manager will be used in a cross-domain configuration, either install an AMS Device Manager station on the domain controller or if AMS Device Manager will not be installed on a domain controller, create the AmsServiceUser account on the domain controller before installing AMS Device Manager on them. Refer to *KBA NA-0800-0113*.

**Notes**

- After installing a Client SC Station on a domain controller together with a DeltaV ProfessionalPLUS workstation, the AMS Device Manager Server system tray icon may not appear. Log out of the domain controller and log back in to make the AMS Device Manager Server system tray icon appear.

## 3.10.1 Domain controller security requirements

To launch and run AMS Device Manager, you must be a member of the AMSDeviceManager Windows user group.

## 3.10.2 Add a user to the AMSDeviceManager group on a domain controller

**Note**
The following procedure requires network administrator permissions.

**Procedure**

1. Select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Select **<Domain Name>** → **Users**.
3. Double-click the **AMSDeviceManager** group.

4. Click **Add**.
5. Enter the Windows User ID you want to add to the group and click **OK**.
6. Click **OK**.

## 3.11 Install SNAP-ON applications

After you have installed and licensed your AMS Device Manager software, you can install SNAP-ON applications. Each SNAP-ON application is licensed separately and will not run if your station is not licensed for it. Most SNAP-ONs are installed from the AMS Device Manager media; if it is not present, contact the manufacturer to acquire it.

Additional installation requirements may apply to a SNAP-ON application. Before you install a SNAP-ON application, check its documentation to confirm that all installation requirements are satisfied.

### Procedure

1. Browse to the AMS Device Manager .ISO image.
2. Browse to \SNAP-ONS And Tools\SNAP-ONS\Installs\<*Folder Name*> (where <*Folder Name*> is the name of the folder for the SNAP-ON application to be installed).
3. Double-click the appropriate setup file.
4. Follow the prompts.

### Notes

- Most SNAP-ON applications need to be installed on each station in a distributed system. See the documentation provided with the SNAP-ON application.
- Calibration Assistant is enabled through licensing–no separate installation is required.
- For all SNAP-ON applications except ValveLink and AMS Wireless, users must also have Device Write permission (see *AMS Device Manager Books Online*).
- ValveLink SNAP-ON application user privileges must be enabled in AMS Device Manager User Manager.
- If a SNAP-ON application is not installed in the C:\Program Files folder, the AMSDeviceManager Windows user group must be given access to the location.

## 3.12 Install AMS Device Manager Web Services on a station

### Procedure

1. Review the AMS Device Manager Web Services software requirements (see page 21).
2. Ensure that appropriate Windows Firewall security settings have been selected (see page 61).
3. Exit/close all Windows programs, including any running in the background (including antivirus software).

4. Browse to the AMS Device Manager .ISO image.
5. Browse to `D:\SNAP-ONS And Tools\AMSWebServices` (where D is the drive letter).
6. Double-click SETUP.EXE.
7. Follow the prompts.

## 3.13 Mobile workstation

A mobile workstation is an AMS Device Manager Client SC Station connected wirelessly to a LAN. As long as the PC meets the AMS Device Manager requirements (see page 19), it functions like a station connected to a wired Ethernet LAN. However, do not configure system interfaces on a mobile workstation, as this can cause database issues regarding the path of the connected device. If at any time the mobile workstation wireless network connection is lost, you may have to restart AMS Device Manager to reestablish network connectivity.

## 3.14 Licensing AMS Device Manager 14.5 FP1 on DeltaV stations

If you have licensed your AMS Device Manager 14.5 FP1 software, you see a full-function application when you launch the product. Otherwise, you can use a limited AMS Device Manager feature set provided with each DeltaV installation. If this is your situation, refer to the *DeltaV Books Online* for information.

There are several licensing considerations when you install AMS Device Manager on a DeltaV station. To ensure that your installation functions as you expect, please contact your Emerson Sales/Service Office. After you have received the appropriate licensing information and AMS Device Manager setup instructions for your situation, install AMS Device Manager as described beginning on page 57.

# 3.15 Installing AMS Device Manager 14.5 FP1 on DeltaV stations

AMS Device Manager 14.5 FP1 can be co-deployed only on DeltaV 13.3.2 -15.LTS stations. To ensure a proper installation, DeltaV must be installed before AMS Device Manager.

**Notes**

- Any AMS Device Manager station (either Server Plus Station or Client SC Station) installed on a DeltaV 13.3.2-15.LTS ProfessionalPLUS workstation must be licensed to ensure proper licensing functionality, security, user synchronization between DeltaV and AMS Device Manager, and Device Description (DD) installation.
- Installing a new version of AMS Device Manager does not install new AMS Device Manager DDs on DeltaV.
- If you are installing AMS Device Manager on any domain controller stations, refer to page 54.
- If you are installing on a system with a DeltaV Independent Domain Controller (IDDC), see Network requirements first.

Before you install AMS Device Manager on your DeltaV stations, ensure that you have all the proper AMS Device Manager and DeltaV licensing and installation instructions (see page 56).

To install Server Plus Station software on a supported DeltaV station, see page 41. To install Client SC Station software on a supported DeltaV station, see page 42.

## 3.15.1 DeltaV actions

**⚠ CAUTION**

Do not configure a DeltaV System Interface for the same DeltaV system on more than one AMS Device Manager station.

After installing AMS Device Manager on a DeltaV Station, you must perform a download of the DeltaV workstation (refer to *DeltaV Books Online*).

**Important**
Ensure that the AMS Device Manager Server Plus Station is already installed before you download the DeltaV workstation.

Downloading a DeltaV workstation adds DeltaV database account users to the AMS Device Manager database. Creating a new Windows user in DeltaV User Manager also adds that user to the AMSDeviceManager Windows user group. add all desired DeltaV users into the AMS Device Manager Windows group on all stations. Add all desired DeltaV users into the AMS Device Manager Windows group on all stations.

**Note**
Each time a ProfessionalPLUS Station is downloaded, some DeltaV user permissions overwrite AMS Device Manager user permissions if the **User Download** checkbox in the **DeltaV** tab of **Tools** → **Options** is selected.

### 3.15.2 DeltaV Upgrade Wizard

The DeltaV Upgrade Wizard automates the process of upgrading a DeltaV Station from an earlier version and ensures that crucial steps are performed. Do not run the DeltaV Upgrade Wizard before uninstalling AMS Device Manager. If you run the DeltaV Upgrade Wizard first, AMS Device Manager will not function as expected and a PC restart may be needed before AMS Device Manager can be uninstalled.

### 3.15.3 Uninstall DeltaV software

To uninstall DeltaV on a station that has AMS Device Manager co-deployed, you must uninstall AMS Device Manager first and then DeltaV. You can then reinstall AMS Device Manager. If you uninstall DeltaV first, AMS Device Manager will not function as expected.

If you have co-deployed AMS Device Manager on domain controllers and non-domain controllers, you must remove AMS Device Manager from all non-domain controllers first, then from all backup/secondary domain controllers, and then from the primary domain controller. Uninstall DeltaV only after AMS Device Manager has been uninstalled on all PCs.

## 3.16 Other Applications

### 3.16.1 DTM Launcher

The DTM Launcher application enables users to install and use certain HART, *Wireless*HART, and FOUNDATION fieldbus Device Type Manager (DTM) drivers with AMS Device Manager. DTMs are an alternative to the traditional Device Descriptions (DDs) supported in AMS Device Manager. DTMs are provided by various device manufacturers and are configured using the DTM Catalog Manager. For more information, refer to *AMS Device Manager Books Online*.

AMS Device Manager supports Launcher and Catalog Manager 4.0.0.xxx, with M&M Library version 4.7.22098.42904 . You can choose to install the DTM Launcher application during AMS Device Manager installation or install it separately by running `setup.exe` from the `Install_Files\DTMLauncher` folder of the AMS Device Manager .ISO image.

**Notes**

- Do not install other DTM frames as these may cause conflicts with the DTM Launcher application.
- If you are upgrading to AMS Device Manager 14.5 FP1, the DTM Launcher application and DTM Catalog is removed during installation. You need to reinstall the DTM Launcher application and reconfigure the DTM Catalog Manager.

### 3.16.2 AMS Device Manager Calibration Connector

AMS Device Manager Calibration Connector is a separately licensed and installed application that integrates with Beamex CMX to provide full-featured calibration management capabilities beyond the basic features available in AMS Device Manager calibration management. AMS Device Manager Calibration Connector provides a solution for users to take advantage of the functionality of other calibration management

applications while maintaining the benefits of device configuration and calibration management data synchronization. For more information about AMS Device Manager Calibration Connector, contact your local Emerson Sales/Service Office.

AMS Device Manager Calibration Connector supports:

- Beamex CMX version 2.11.5 with 2.11.7 patch

AMS Device Manager Calibration Connector can only be installed on a Server Plus Station. You must have Windows Administrator permissions to install AMS Device Manager Calibration Connector.

### Install AMS Device Manager Calibration Connector

#### Procedure

1. Browse to the AMS Device Manager Calibration Connector .ISO image.
2. Double-click AMSDeviceManagerCalibrationConnector_Setup.exe.
3. Follow the prompts on the installation window.
4. Click **Finish** when done.

For additional information about using AMS Device Manager Calibration Connector, refer to *AMS Device Manager Books Online* or *AMS Suite Calibration Connector and Beamex CMX Installation and Setup* document. Also, refer to your Beamex CMX documentation for more information.

**Note**
Refer to the *AMS Device Manager Supported Device List* to determine if a device supports calibration.

## 3.16.3 User Configuration Reports

The User Configuration Reports tool works with the Bulk Transfer Utility on the AMS Device Manager Server Plus Station. It allows you to verify that multiple devices are configured according to a specified user configuration. The User Configuration Reports tool allows you to check the device configurations of multiple devices and quickly identify any incorrect settings. For more information about user configurations and the Bulk Transfer Utility, see *AMS Device Manager Books Online*.

The User Configuration Reports tool (and its SQL add-on) is installed automatically with an AMS Device Manager Server Plus Station.

**Note**
Microsoft does not allow the SQL (2019) add-on to be installed on a domain controller, so reports will not function in Bulk Transfer.

The User Configuration Reports tool uses AMS Device Manager Generic Export to get device parameter data. If you have a large AMS Device Manager system, or many devices or device parameters, the Generic Export process can take several hours.

# 4 Prepare to use AMS Device Manager

There are several configuration steps you must take before using AMS Device Manager. If you do not configure your PC and network as described, AMS Device Manager will not function as expected.

## 4.1 Change Windows Firewall settings

When operating AMS Device Manager on a Windows PC, some changes to Windows Firewall settings may be required. If your PC is adequately protected by a corporate firewall, you may be able to turn off the Windows Firewall protection on your AMS Device Manager PC.

If your AMS Device Manager PC is not protected by a corporate firewall and you have enabled the Windows Firewall, you must change the firewall settings on your PC to allow program and port exceptions that enable AMS Device Manager operation. For assistance configuring your Windows Firewall, contact your IT department.

**Note**
For more information on security considerations, or for deployment scenarios that require AMS Device Manager Client SC Stations to cross External Firewalls, refer to the AMS Device Manager Security Guide.

## 4.2 Usernames and passwords

**Note**
When AMS Device Manager is co-deployed with DeltaV, your DeltaV username and password can also provide AMS Device Manager access.

AMS Device Manager security is based on Windows user authentication.

All Windows users using AMS Device Manager must be added in User Manager; if you install AMS Device Manager, your Windows username is added automatically and given User Manager administrator permissions. The AMS User Manager administrator determines the plant locations and/or functions allowed on a user account. To launch User Manager, enter `User Manager` on the **Start** screen and click **User Manager**.

See *AMS Device Manager Books Online* for more information on User Manager functionality.

## 4.3 Configure system interfaces

AMS Device Manager communicates with HART, *Wireless*HART, FOUNDATION fieldbus, PROFIBUS DPV1 and PROFIBUS PA devices through various system interfaces. If this is a new installation or you are adding interfaces to an existing system, you need to configure the network after you have installed the software. Ensure certificates from the PC hosting the system interface are copied to the AMS folder on other stations in the distributed system, and run Certificate Manager on those stations.

You need to configure the system interfaces that are relevant to each station. You should only configure a particular physical network on one station within the distributed network to avoid the potential for simultaneous device configuration.

To configure a system interface, check the system requirements (see page 25) and refer to the *Network configuration overview* topic in *AMS Device Manager Books Online*. Some system interfaces that require additional configuration are discussed in this section.

## 4.3.1 DeltaV

A DeltaV control network is an isolated Ethernet local area network (LAN) that provides communication between the controllers and the stations. It uses one or more Ethernet hubs for communication.

**Note**
Do not configure an AMS Device Manager Wireless System Interface if a DeltaV System Interface will be using the same wireless gateway.

For information about AMS Device Manager compatibility with DeltaV, refer to page 28.

DeltaV can access devices in RS3 and PROVOX I/O systems through the DeltaV Interface for RS3 I/O and DeltaV Interface for PROVOX I/O, respectively. The devices are displayed in the DeltaV network hierarchy in AMS Device Manager. For more information, refer to the *DeltaV Books Online*.

The ValveLink SNAP-ON application is supported for DeltaV and PROVOX I/O cards, but not for RS3 I/O cards.

### Prepare the DeltaV system

To prepare a DeltaV control system to communicate with an AMS Device Manager station, you need to:

- Know the node name of the DeltaV ProfessionalPLUS Station you are connecting to. If you do not know this name, see your system administrator.
- Know the password associated with the DeltaVAdmin account on the ProfessionalPLUS Station, if it has been changed from the default password.
- Configure a HART-Enabled Channel so that AMS Device Manager knows where to look for a HART field device. If an I/O channel is enabled for HART but it does not have an associated DeltaV device signal tag, it will not appear in AMS Device Manager.
- Commission any FOUNDATION fieldbus devices you want to be displayed in AMS Device Manager.

### Set DeltaV alert capability

To receive alerts from devices connected to PROVOX and RS3 Migration Controllers in your DeltaV network hierarchy, you must run a utility to properly set the DeltaV alert capability.

#### Procedure

1. Enter `C:\AMS\BIN\DELTAVFASTSCANUTILITY.EXE` (where C is the drive containing the AMS folder) on the **Start** screen.

2. Uncheck the box for the appropriate DeltaV network.
3. Click **Save Changes**.

# 4.4 Add devices to AMS Device Manager

All available information for supported field devices (other than device manuals) is included and installed with the AMS Device Manager application. If it is necessary to install additional devices after the initial installation, refer to Device Type Installation in *AMS Device Manager Books Online*. Additional device descriptions can be downloaded using this link: https://www.emerson.com/en-us/catalog/ams-guardiansupportdevicemanager.

# 4.5 Attach a Roving Station to a Server Plus Station

A Roving Station is a portable PC (laptop or notebook computer) with AMS Device Manager Server Plus Station software installed. A Roving Station is configured as such in the Options for AMS Device Manager dialog (**Tools → Options**). A Roving Station can be temporarily connected to a stationary Server Plus Station to enable uploading of AMS Device Manager information from the Roving Station. For more information about Roving Stations, refer to *AMS Device Manager Books Online*.

# 4.6 AMS Device View

Once you have installed the AMS Device View web server. you can use a supported browser to launch AMS Device View screens. Desktop/laptop browsing of AMS Device View data and opening device details screens can only be launched from a Windows PC.

## 4.6.1 Configure AMS Device View client devices

**Note**
There is a limit of 20 concurrent clients accessing the AMS Device View server.

There are several configuration tasks you must do before using AMS Device View. If you do not configure your client devices as described, AMS Device View will not function as expected.

## 4.6.2 Install the latest version of a supported operating system

To allow a browser to access AMS Device View data, you must install the latest version of a supported operating system. This ensures certificates can be installed that enable secure communications. This includes:

- Android and iOS (for mobile browsing of AMS Device View data)
- Windows (for desktop/laptop browsing of AMS Device View data)

See Web Browsers for the list of supported browsers.

## 4.6.3 Verify browser security settings

Ensure your Windows PC has sufficient security settings to allow AMS Device View to communicate with AMS Device Manager.

**Note**
Some settings may be controlled by your Windows system administrator.

### Procedure

1. Type **Internet Options** in the Windows search bar, and open its control panel.
2. Select the **Security** tab.
3. Select Trusted Sites.
4. Set the Security Level for this zone as Medium-High.
5. Select the **Sites** button.
6. Enter the AMS Device View site (ex: https://<computername>. Select **Add** then **Close**.
7. Select **Custom Level**.
8. In the Security Settings - Trusted Sites Zone dialog box, ensure Reset custom settings is set to **Medium-high**.
9. Select **Reset...**, and choose **Yes.**
10. Scroll to Downloads, and select **Enable** under File Download.
11. Select **OK**, then **OK** again.

## 4.6.4 Export the AMS Device View certificate

If you are using the Emerson self-signed certificate, and your AMS Device View web server is installed on an AMS station, use Certificate Manager to export the certificate. Otherwise, use this procedure to save the AMS Device View certificate to install on any computer that will be communicating securely with the AMS Device View web server. There are additional procedures. You can access videos about how to do that from the AMS Device Manager media at \Install_Files\Certificate_Videos.

### Procedure

1. On the AMS Device View web server, enter **certlm.msc** on the Start screen and press **Enter**.
2. Expand **Trusted Root Certification Authorities** and select **Certificates**.
3. Right-click the AmsDeviceView.<servername> certificate and select **All Tasks** → **Export**.
4. Click **Next**.
5. Select **DER encoded binary X.509 (.CER)**. Next.
6. Browse to a location where you want to save the certificate and enter a file name. You will be installing this certificate on another PC, or sending it to a mobile device, so make sure the location is accessible.
7. Click **Save**.

8. Click **Next**.
9. Click **Finish.**

## 4.6.5 Install the AMS Device View certificate on Windows PCs

For AMS Device View to communicate securely with AMS Device Manager, you must export and install Emerson self-signed security certificates from AMS Device Manager Server Plus and AMS Device View PC, and vice-versa. If your AMS Device Manager web server is deployed on an AMS station, you can use Certificate Manager to deploy the certificates. If not, you can access videos about how to do that from the AMS Device Manager media at \Install_Files\Certificate_Videos.

### Procedure

1. Copy the certificate file you exported in the AMS Device View web server to your AMS Device View client PC.
2. Right-click and choose **Install Certificate**.
3. Select **Local Machine** and click **Next**.
4. Click **Next**.
5. Select **Place all certificates in the following store**.
6. Click **Browse** and select **Trusted Root Certification Authorities**.
7. Click **OK**.
8. Click **Next**.
9. Click **Finish**.
10. If you see a **Security warning dialog**, click **Next**.
11. Click **OK**.

## 4.6.6 Install the AMS Device View certificate on iOS

### Procedure

1. Send the certificate file you exported on the AMS Device View server to an account accessible on your iOS device.
2. Open the message or email, and tap the attached certificate file.
3. Tap **Save to Files**.
4. Choose a location and press **Save**.
5. In the Files app, Tap the .cer file to download its profile.
6. Tap **Close**.
7. Open the **Settings** app.
8. Tap **Profile Downloaded** then **Install** and enter your passcode. Read the warning, and tap **Install** again.
9. Tap **Done**.
10. Open **Settings** → **General** → **About** → **Certificate Trust Settings**

11. Enable the AMS Device View certificate under the section **Enable Full Trust for Root Certificates**. Tap **Continue**.

**Note**
When you open AMS Device View, ensure that you use the fully qualified domain name, for example:

```
https://myserver.mydomain.com/AmsDeviceView
```

of the AMS Device View web server.

You can now access AMS Device View from the mobile device's browser.

## 4.6.7 Install the AMS Device View certificate on Android

### Procedure

1. Email the certificate file you exported on the AMS Device View server to an account accessible on your Android device.
2. Tap the certificate. An underlined checkmark displays in the menubar.
3. Go to **Settings** → **Security** → **Encryption & Credentials** → **Install a Certificate** → **CA certificate**.
4. Tap **Install anyway**.
5. Tap the certificate file from the list of files in **Download**.
   Verify the CA certificate installed popup displays at the bottom of the screen, and in **Trusted credentials** → **User**. You can now access AMS Device View from the mobile device's browser.

**Note**
When you open AMS Device View, ensure that you use the fully qualified domain name, for example:

```
https://myserver.mydomain.com/AmsDeviceView
```

of the AMS Device View web server.

## 4.6.8 View the fully qualified domain name of the AMS Device View web server

This name defines the AMS Device View web server, and is needed in the URL field of the browser when accessing it.

### Procedure

1. On the AMS Device View server PC, click **Start**.
2. Right-click on **This PC**.
3. Select **Properties**.
   The fully qualified domain name is listed in the Full computer name field.

# 5 Troubleshoot installation errors

If you get error messages during the installation or startup of AMS Device Manager, you may be able to resolve these errors using the troubleshooting procedures in this section.

If you are unable to resolve installation problems after carefully following the installation steps outlined in this guide and using these troubleshooting suggestions, contact your local Emerson Sales/Service Office. Additional Support Center Contact Information can be found here.

To troubleshoot non-installation issues, refer to *KBA NK-1400-0417*.

## 5.1 Error messages

| Error message / Indication | Possible Cause | Possible solution |
|---|---|---|
| | | |
| AMS Device Manager has detected an incorrect version of the database.<br>The version detected is x.x, the correct version should be y.y. | Database Verify/Repair was not run before upgrading AMS Device Manager to the current release or AMS Device Manager has detected a fault that occurred during the Verify/ Repair operation. | Run the database conversion utility (AmsConvertDb.exe) from the `AMS\Bin` folder:<br>1. Open the AMS\Bin folder.<br>2. Double-click AmsConvertDb.exe.<br>If the database conversion utility does not complete successfully, contact your local Emerson Sales/Service Office. |
| Cannot find server or DNS Error. | | Open port 80 on the Server Plus Station where AMS Device Manager Web Services is configured. See Change Windows Firewall settings. |
| Unable to launch the AMS Device Manager application from the Client SC Station. | | Open port 135. See Change Windows Firewall settings. |
| “Connecting to OPC Server Failed” when attempting to launch the OPC Client application. | | Add AMSOPC.exe to the exception list. See Change Windows Firewall settings. |
| Unable to launch the AMS Device Manager application from the Client SC Station. | | Add sqlserver.exe and sqlbrowser.exe to the exception list. See Change Windows Firewall settings. |

| Error message / Indication | Possible Cause | Possible solution |
|---|---|---|
| AMS Device Manager may be slow to start when launched from the Windows Start menu. The following messages are displayed in the Application event log:<br>Unable to retrieve the current configuration information for server, <PC name>.<br>Error calling GetServersAsXml. | | Add AMSServicesHoster.exe to the exception list. See Change Windows Firewall settings. |

# A DeltaV system interface deployment concepts

## A.1 Architecture Constraints

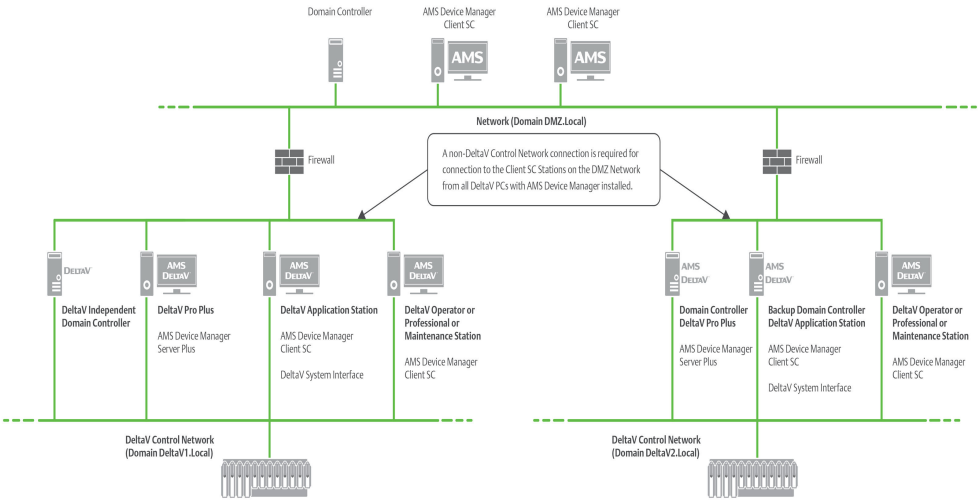
In addition to meeting the other installation requirements detailed in this document, the connectivity requirements for AMS Device Manager and DeltaV result in the following architecture constraints:

AMS Device Manager is designed and supported for two installation scenarios when used with DeltaV.

1. For ACN resident machines: The machine must have a supported DeltaV workstation if AMS Device Manager is to be installed. This is due to enhanced domain security features employed in later versions of DeltaV. The scenario of a standalone AMS Device Manager, Server Plus or Client SC resident on the DeltaV ACNs has not been designed or tested for. Settings on a DeltaV node are configured as part of the installation process. When Device Manager is installed on a PC where DeltaV has been installed, all domain security parameters will be properly configured.
2. For non-ACN resident machines: The AMS Device Manager Server Plus or Client SC must be installed in a separate Windows security domain and must have two way trusts established with the applicable DeltaV systems.

Other combinations may be possible, but require site specific security settings that are not covered under standard Guardian Support. Contact your local Emerson business partner for paid for service options for site-specific custom installations.

# A.2 AMS Device Manager on Multiple Domain Networks with a Server Plus on each of the DeltaV Control Networks




## Notes

- The DeltaV System Interface must be configured on an AMS Device Manager station installed on each DeltaV Network and cannot be configured on the same Client SC Station used with Server Plus Connect.
- All AMS Device Manager installations must be at the same version. See DeltaV topic for supported DeltaV versions.
- The AMS Device Manager Station installed on the ProfessionalPLUS must be licensed. If the Server Plus is not installed on the ProfessionalPLUS, an additional license is needed for the Client SC that is installed on the ProfessionalPLUS.
- Each DeltaV network is treated as a separate network and therefore the Cross Domain requirements in *KBA NA-0800-0113* might apply.
- If you are installing on a Domain Controller, see Network requirements.
- Accessing devices between DeltaV systems or across zones is not supported. Accessing devices from multiple DeltaV systems or from multiple zones is only supported from the Server Plus station or the Client SC stations on the Plant Network.

### Primary Use

This architecture is for a larger user installation (with multiple DeltaV systems, Domains, or Zones) in which the AMS Device Manager Client SC Stations (Non-DeltaV workstations) located on the Plant Network allow users to access devices located on the DeltaV system.

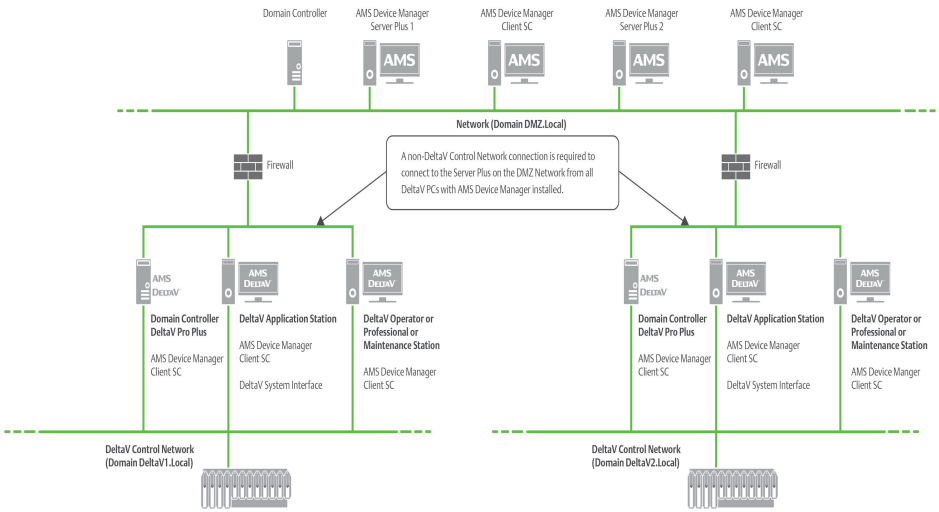
### General Deployment Information

In a deployment with multiple control networks, AMS Device Manager Client SC Stations may use the Server Plus Connect functionality. These AMS Device Manager Client SC Stations can connect to either control network as long as all versions of software are the same across the networks. There can be one AMS Device View server and one Read-Only server per distributed system.

### Adding Device Files

- The user can add device files at any station in *each* distributed system. The system then automatically makes these updates to the other stations in the system, without manual intervention.
- To install properly, the GSD and DD files are needed for PROFIBUS DPV1 and PROFIBUS PA devices.
- PROFIBUS DP/PA couplers are also needed (see the DeltaV documentation for supported couplers).

# A.3 Single AMS Device Manager distributed network that supports multiple DeltaV control networks with or without Zones




## Notes

- The AMS Device Manager Station installed on the ProfessionalPLUS must be licensed. If the Server Plus is not installed on the ProfessionalPLUS, an additional license is needed for the Client SC that is installed on the ProfessionalPLUS.
- The DeltaV System Interface must be configured on an AMS Device Manager station installed on each DeltaV Network/Zone.
- All AMS Device Manager installations must be at the same version. See DeltaV topic for supported DeltaV versions.
- Each DeltaV network is treated as a separate network and therefore the Cross Domain requirements in *KBA NA-0800-0113* might apply.
- If you are installing on a Domain Controller, see Network requirements.
- If the Server Plus Station fails, all Client SC Stations from different DeltaV Zones will lose communication back to the Server Plus Station. Redundant networking is recommended.
- This architecture includes multiple DeltaV Networks with many devices, therefore a full version of SQL Server is recommended for improved performance.

- Accessing devices between DeltaV systems or across Zones is not supported. Accessing devices from multiple DeltaV systems or from multiple zones is only supported from the Server Plus station or the Client SC stations on the Plant Network.

---

AMS Device Manager supports multiple DeltaV networks or multiple DeltaV Zones/ Network Domain systems with a single AMS Device Manager system connecting to multiple Zones within a DeltaV Zones system, or with an AMS Device Manager system on each Zone in a DeltaV Zones system.

In the case of a single AMS Device Manager system deployed across a single DeltaV Zones system, there is only one AMS Device Manager Server Plus Station, which is connected to the Plant Network. Each DeltaV station can have an AMS Device Manager Client SC Station and must be connected back to the Plant Network.

### Primary Use

- To have one main station that consolidates all information but still allows the user write privileges to any station/system below.
- This architecture is for a user installation in which the AMS Device Manager Server Plus Station is located on the Plant Network and allows users to access devices located on multiple DeltaV systems or Zones.
- This architecture is valuable for a user who wants to have a single AMS Device Manager database and perform AMS Device Manager functions from a centralized location. There can be one AMS Device View server and one Read-Only server per distributed system.

### Network Domain Deployment

- If the network connection to the AMS Device Manager Server Plus Station is lost, NO device commissioning or device configuration can be done on the DeltaV network until the network connection has been restored.

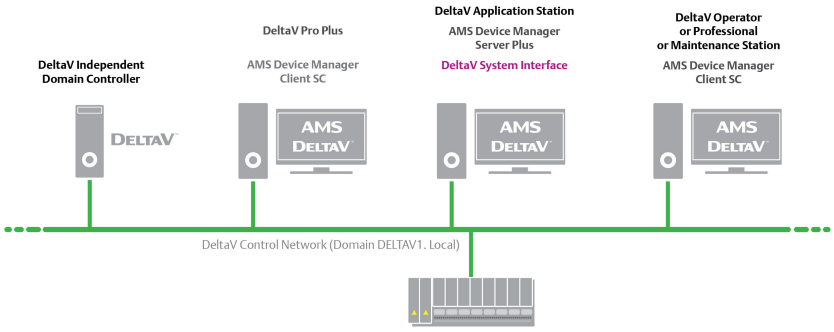
### Security

- Any user account setup/changes need to be made on all stations. Information relating to the setup or changes to user account security can be found in *AMS Device Manager Books Online*.

### Adding Device Files

- The user can add device files at any station. The system then automatically makes these updates to the other stations in the system, without manual intervention.
- To install properly, the GSD and DD files are needed for PROFIBUS DPV1 and PROFIBUS PA devices.
- PROFIBUS DP/PA couplers are also needed (see DeltaV documentation for supported couplers).

# A.4 AMS Device Manager with DeltaV Control Networks-Independent Domain Controller




## Note

### Primary Use

- This architecture is for a customer installation when the DeltaV system is set up with an Independent Domain Controller.
- The version of AMS Device Manager must be compatible with the DeltaV version. See DeltaV topic for supported versions.

### Network Domain Deployment

- The IDDC is also supported with the Multiple Domain Networks and Single distributed system DeltaV deployments.
- When installing AMS Device Manager on DeltaV systems with IDDC, the logged in Windows user needs to be a Domain Administrator. This is to ensure the proper accounts get created on the IDDC. No other software is required to be installed on the IDDC.
- If you are installing on a Domain Controller, see Network requirements.

- If the network connection to the Server Plus computer is lost, NO device commissioning or device configuration can be done on the DeltaV network until the network connection has been restored.

### Security

- Security modifications such as adding, removing, or modifying users / privileges must be made by the user at the DeltaV Pro Plus stations, the AMS Device Manager Server Plus stations, and the other stations on the Network.
- For ACN resident PCs: The PC must have DeltaV and AMS Device Manager installed. This is due to enhanced security features employed in later versions of DeltaV. The scenario of a standalone AMS Device Manager, Server Plus or Client SC resident on the DeltaV ACNs has not been designed or tested.
- For non-ACN resident PCs: The AMS Device Manager Server Plus or Client SC must be installed in a separate Windows security domain and must have two-way trusts established with the applicable DeltaV systems.

### Adding Device Files

- The user can add devices files an any station except for the Domain Controller. The system then automatically makes these updates to the other stations in the system, without manual intervention.
- To install properly, the GSD and DD files are needed for PROFIBUS DPV1 and PROFIBUS PA devices.
- PROFIBUS DP/PA couplers are also needed (see the DeltaV documentation for supported couplers).

# B Other deployment concepts

## B.1 AMS Device View

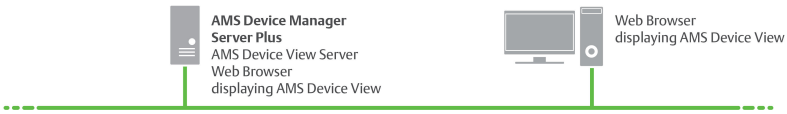
AMS Device View can be deployed read-only, or with the ability to edit some parameters on an AMS Device Manager system following these requirements:

- IIS must be installed on the PC before installing AMS Device View, and must be in the same time zone as the AMS Device Manager Server Plus Station.
- AMS Device View server must be installed on a supported Windows Server-class machine.
- Only one AMS Device Manager database is allowed; the AMS Device View Server can only connect to one (1) Server Plus station.
- Upgrades to AMS Device View require upgrades to AMS Device Manager. Versions cannot be intermixed.
- AMS Device Manager should be installed or upgraded before installing AMS Device View, whether deploying on workgroups or a Windows domain.
- You must export and install certificates between AMS Device Manager stations and AMS Device View server. See the AMS Device View videos for how to do this on your install media \Install_Files\Certificate_Videos.

**Note**
If you are deploying a Read/Write AMS Device View server, ensure your organization employs a firewall or other control to limit access and prevent device configuration changes by unauthorized personnel.

### Deployed on AMS Device Manager Server Plus Station

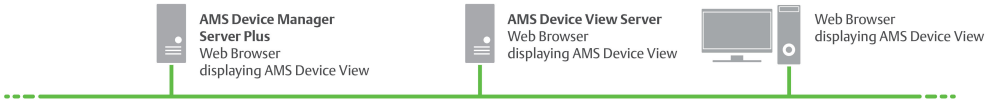
**Figure B-1: AMS Device View server on the AMS Device Manager Server Plus Station**




### Deployed on a non-AMS Device Manager PC

**Note**
Emerson does not recommend installing AMS Device View on a domain controller unless DeltaV is also on the same server.

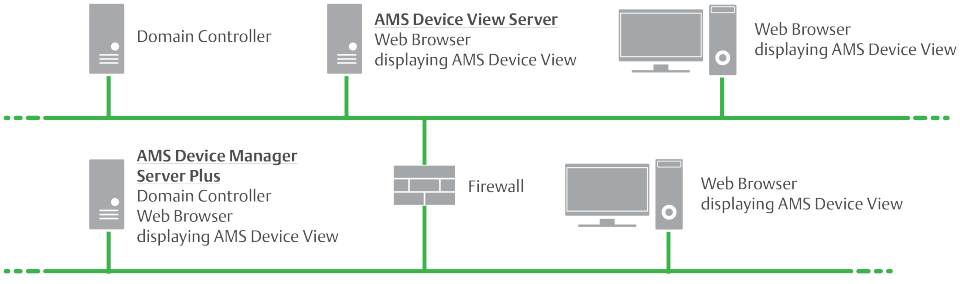
**Figure B-2: AMS Device View server not on an AMS Device Manager Station**




- A mix of domains and workgroups is not supported. The AMS Device Manager Server Plus and AMS Device View server must be both on a domain, or both on a workgroup.
- The following restrictions apply when the Windows login to AMS Device View is a local user account (and not a domain account)
  - The AMS Device Manager Server Plus and the AMS Device View server should each have their own local Windows user for the user account being used to log into AMS Device View. That local user name and password will need to be set to the same values across both servers.
  - In AMS Device Manager User Manager, add the AMS Device View server as a Windows machine.
  - In AMS Device Manager User Manager, the user accounts logging into AMS Device View must be added under the AMS Device Manager Server Plus and the AMS Device View PCs
  - In AMS Device Manager User Manager, the Assigned Permissions for the account under both PCs must be identical

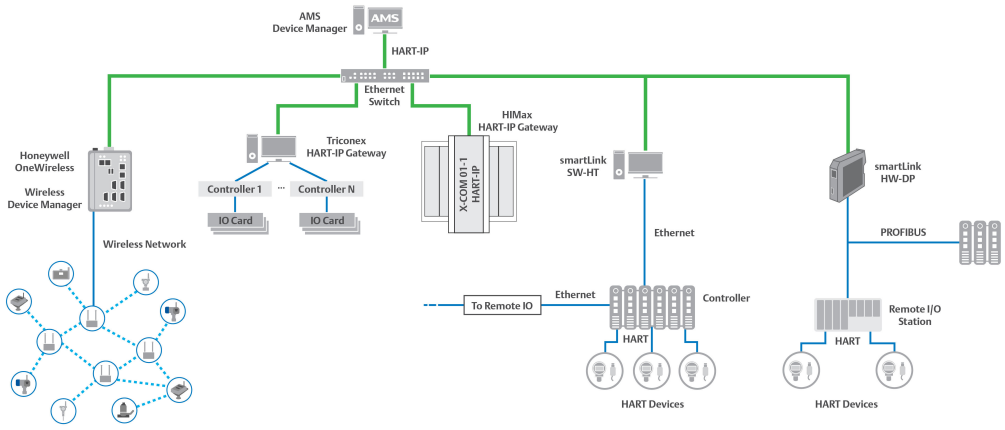
**Note**
When installing AMS Device View on a different domain than AMS Device Manager Server Plus, refer to KBA NA-0800-0113 Configuring AMS Device Manager for Cross Domain Functionality

**Figure B-3: AMS Device View server installed on a different domain than AMS Device Manager Server Plus**



# B.2 HART-IP Interface

**Figure B-4: HART-IP supported Interfaces**




Honeywell OneWireless Wireless Device Manager, WDMX, WDMY; OneWireless R240, R300, R310 and R320

Triconex Tricon CX version 11.5

HIMA HIMax major version 5, configured with SilWorx v 5.30

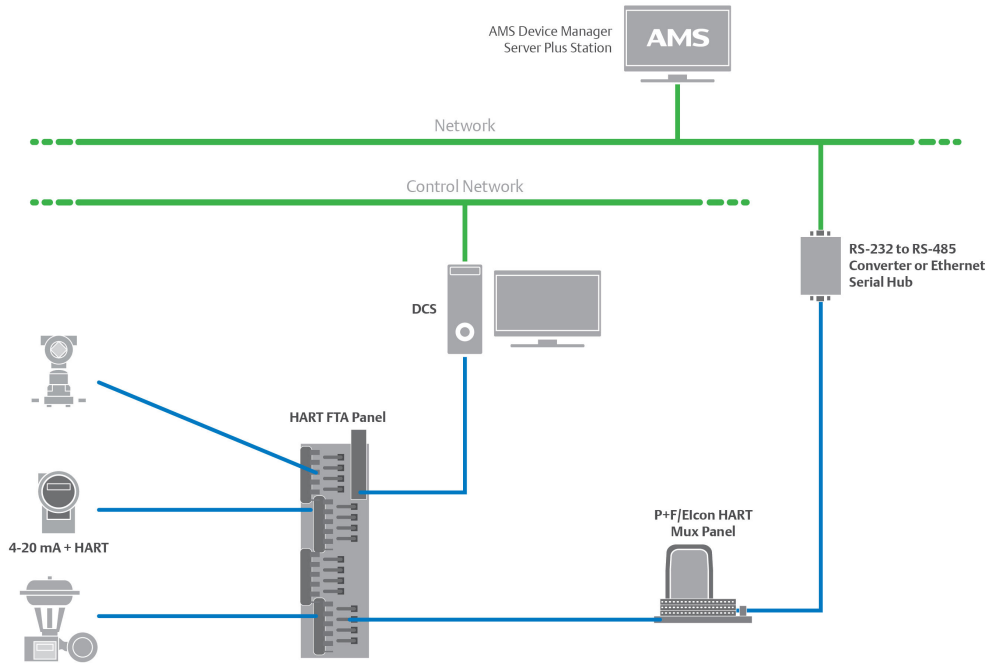
Phoenix Contact Ethernet HART multiplexer GW PL ETH/BASIC-BUS (2702321) and GWPL ETH/UNI-BUS (2702233)

Softing smartLink HW-DP v 2.0, SW-HT v 1.20 and higher

**Notes**

- The diagram shows individual networks and is not intended to imply all networks being connected simultaneously.
- For additional connection details and Windows ports, see AMS Device Manager Security Guide, and for details on HART-IP systems, contact the manufacturer or your local Emerson impact partner or system integrator.

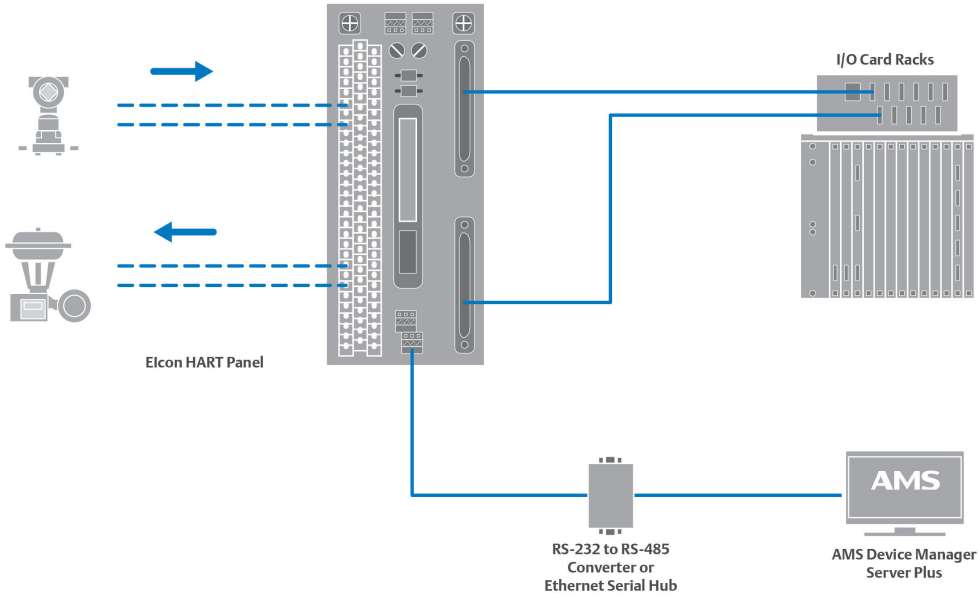
# B.3 HART Interface Solution – External Interfaces




**Notes**

- This deployment provides AMS Device Manager access to all HART devices connected to multiplexers.
- The Server Plus Station must be licensed to cover all HART devices.
- For applications where P+F/Elcon customized replacement panels cannot be used, P+F/Elcon also provide a family of external interface panels. The P+F/Elcon external interface panels are used in conjunction with the DCS or PLC existing termination panels. External interfaced panels are daisy-chained to create the multiplexer network used by AMS Device Manager to gain access to the HART information from the field instruments.
- RS-485 signal from the multiplexer can be connected to an Ethernet serial hub or to an RS-485/RS-232 converter, for the HART signal to be accepted into the AMS Device Manager PC.

# B.4 HART Custom Solution – Integrated HART Panel Incorporating Multiplexer and Field Termination Panel (FTP)




**Notes**

- This deployment is typically used on new installations or upgrades where the digital control system is purchased with a P+F/Elcon panel.
- This deployment can be used to replace existing term panels to add multiplexers to an existing system.
- This deployment provides AMS Device Manager access to all HART devices connected to multiplexers.
- The Server Plus Station must be licensed to cover all HART devices.
- The RS-485 signal from the Multiplexer can be connected to an Ethernet serial hub or to an RS-485/RS-232 converter, for the HART signal to be accepted into the AMS Device Manager PC.

# C Version compatibility

As of the initial release of AMS Device Manager 14.5 FP1, the following SNAP-ON applications are supported:

**Table C-1: SNAP-ON applications/AMS Device Manager compatibility matrix**

| SNAP-ON application | SNAP-ON application version | AMS Device Manager 14.5 FP1 |
|---|---|---|
| AlertTrack | 6.8.1.3 | x |
| AMS Wireless | 14.5 | x |
| Flowserve ValveSight | 1.0.0.2 (Logix MD HART, Logix420); 1.0.0.11 (Logix MD +); 1.1.1.8 (Logix 3400MD) | x |
| Masoneilan ValVue HART | 2.81.1 | x |
| Masoneilan ValVue FF | 2.32.1 | x |
| Meter Verification | 3.5.b11.r0 | x |
| ProofCheck | See NK-2200-0374 | x |
| QuickCheck | 9.4.0.3 | x |
| Rosemount MV Engineering Assistant | 5.5.1 | x |
| Rosemount MV Engineering Assistant | 6.5.1 | x |
| ValveLink | 13.7 | x |

**Table C-2: DeltaV/AMS Device Manager compatibility matrix**

| DeltaV Versions | AMS Device Manager version 14.5 FP1 |
|---|---|
| 13.3.2 | x |
| 14.LTS | x |
| 14.FP1, 14.FP2, 14.FP3 | x |
| 15.LTS | x |

**Note**
AMS Device Manager supports DeltaV version 13.3.2, 14.LTS, 14.FP1, 14.FP2, 14.FP3, and 15.LTS in co-deployed installations only.

# Index

**Emerson**
**www.Emerson.com**