Planning and Installation Guide
May 2018

AMS Device Manager

Version 14.0 Planning and Installation Guide

EMERSON

Disclaimer

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. We reserve the right to modify or improve the designs or specifications of such products at any time without notice. This document is not to be redistributed without permission from Emerson.

Copyright and trademark information

The Emerson logo is a trademark and service mark of Emerson Electric Co.

AMS, Plantweb™ Plantweb Optics™, SNAP-ON™, DeltaV™, RS3™, PROVOX™, Ovation™, FIELDVUE™, and ValveLink™ are marks of one of the Emerson group of companies.

FOUNDATION™, HART® and *Wireless*HART® are marks of the FieldComm Group of Austin, Texas, USA.

Intel® and Intel® Core™ are registered trademarks, or trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the United States and/or other countries.

All other marks are property of their respective owners.

Document history

Part number	Date	Description
	November 2013	Update, software version 12.5
10P5824D001	April 2015	Update, software version 13.0
10P5824D002	August 2015	Update, software version 13.0 Service Pack 1
10P5824D003	November 2016	Update, software version 13.1.1
	May 2017	Update, software version 13.5
	May 2018	Update, software version 14.0

License Agreement

Definitions: The term "You" includes, but is not limited to, users of the Fisher-Rosemount Systems, Inc. (FRSI) product embodied in the computer program herein, the user's employer, the employer's wholly owned subsidiaries, parent company, agents, employees, contractors, and subcontractors. The term "License Agreement" refers to one of FRSI's License Agreements, including but not limited to, all Software License Agreements, accompanying FRSI products, all Beta Test Agreements, and all Master License Agreements.

Any and all use of this product is subject to the terms and conditions of the applicable License Agreement. The terms and conditions of the applicable License Agreement by and between You and FRSI shall remain effective to govern the use of this product.

The existence of a License Agreement by and between You and FRSI must be confirmed prior to using this product. If the site at which this Program is used is a Licensed Facility under a Master License Agreement with FRSI, the applicable License Certificate that was sent to You applies. If the site at which this Program is used is NOT a Licensed Facility under a Master License Agreement with FRSI and the use of the program is NOT governed by a Beta Test Agreement, the use of this Program shall be governed by the Software License Agreement that is printed in the sales literature, on the package in which the program was delivered, and in this manual.

License Certificate for AMS Device Manager

If the site at which this Program is used is a Licensed Facility under a Master License Agreement between You and Fisher-Rosemount Systems, Inc., this Licensed Copy is provided for Licensee's use pursuant to its Master License Agreement with FRSI ("Agreement") as modified herein. If this is an original Licensed Copy, it may be used only on the equipment with which it has been provided except as otherwise provided in the Agreement. If this is a Licensed Copy of a Revision or Upgrade, it may only be used in lieu of and under the same terms as the Licensed Copy previously provided to Licensee.

Notwithstanding provisions of the Agreement, the term of the Limited Warranty for this Licensed Copy is 90 days from the date of shipment from FRSI. Licensee's other rights and obligations with respect to its use of this Licensed Copy are set forth in the Agreement. Questions concerning Licensee's rights and obligations should be directed to Contract Management, Fisher-Rosemount Systems, Inc., 1100 W Louis Henna Blvd, Round Rock, Texas 78681.

Software License Agreement for AMS Device Manager

BY OPENING THIS PACKAGE YOU AGREE TO ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE WITH THESE TERMS, YOU SHOULD PROMPTLY RETURN THE PACKAGE UNOPENED AND YOUR MONEY WILL BE REFUNDED. FRSI provides this computer program and related materials for your use. You assume responsibility for the acquisition of a machine and associated equipment compatible with the program, and for installation, use, and results obtained from the program.

LICENSE: FRSI grants to you a non-transferable, non-exclusive license to: (a) use all fully paid up licensed programs provided to you to run a single machine; (b) copy the program for backup or modification purposes in support of the program on the single machine. You must reproduce and include the copyright notice on any copy or modification. YOU MAY NOT REVERSE ENGINEER, USE, COPY, OR MODIFY ANY PROGRAM OR RELATED MATERIALS OR ANY COPY, MODIFICATION, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE. IF YOU TRANSFER POSSESSION OF ANY COPY OR MODIFICATION OF THE PROGRAM OR RELATED MATERIALS TO ANOTHER PARTY, YOUR LICENSE IS AUTOMATICALLY TERMINATED. No license, express or implied, is granted under any intellectual property directly or indirectly owned by FRSI which does not specifically read on the program as provided hereunder, nor shall any license, except the license specifically granted herein, be implied in law, implied in equity, or exist under the doctrine of patent exhaustion.

TITLE: Title to and ownership of the program and related materials shall at all times remain with FRSI or its licensors. Your right to use the same is at all times subject to the terms and condition of this Agreement. FRSI may, from time to time, revise or update the program and/or related materials and, in so doing, incurs no obligation to furnish such revisions or updates to you.

TERM: This license is effective upon opening this package. You may terminate it at any time by destroying the program and the related materials together with all copies and modifications in any form. It will also terminate upon conditions set forth elsewhere in this Agreement or if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the program and the related materials together with all copies and modification in any form.

LIMITED WARRANTY: FRSI warrants the media on which the program is furnished to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to you as evidenced by a copy of your invoice. However, FRSI does not warrant that the functions contained in the program will meet your requirements or that the operation of the program will be uninterrupted or error free. THE PROGRAM AND RELATED MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU; SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

LIMITATIONS OF REMEDIES: FRSI's entire liability and your exclusive remedy shall be: (1) the replacement of any media not meeting FRSI's "Limited Warranty" and which is returned with a copy of your invoice to Fisher-Rosemount Systems, Inc., 1100 W Louis Henna Blvd, Round Rock, Texas 78681, USA, or (2) if FRSI is unable to deliver replacement media which is free of defects in materials or workmanship, you may terminate this Agreement by returning the program and your money will be refunded. IN NO EVENT WILL FRSI BE LIABLE TO YOU FOR ANY DAMAGES ARISING OUT OF ANY CAUSES WHATSOEVER (WHETHER SUCH CAUSES BE BASED IN CONTRACT, NEGLIGENCE, STRICT LIABILITY, OTHER TORT, PATENT INFRINGEMENT, OR OTHERWISE), INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PROGRAM EVEN IF FRSI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR OF ANY CLAIM BY ANY OTHER PARTY.

GOVERNING LAW: This Agreement, and all matters concerning its construction, interpretation, performance, or validity, shall be governed by the laws of the State of Texas.

EXPORT RESTRICTIONS: Licensee shall comply fully with all laws, regulations, decrees, and orders of the United States of America that restrict or prohibit the exportation (or reexportation) of technical data and/or the direct product of it to other countries, including, without limitation, the U.S. Export Administration Regulations.

U.S. GOVERNMENT RIGHTS: The programs and related materials are provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in the Federal Acquisition Regulations and its Supplements.

THE PROGRAM IS NOT FOR USE IN ANY NUCLEAR AND RELATED APPLICATIONS. You accept the program with the foregoing understanding and agree to indemnify and hold harmless FRSI from any claims, losses, suits, judgements and damages, including incidental and consequential damages, arising from such use, whether the cause of action be based in tort, contract or otherwise, including allegations that FRSI's liability is based on negligence or strict liability.

To the extent that a third party owns and has licensed to FRSI any portion of the program, such third party owner shall be a beneficiary of this Agreement, and shall have the right to enforce its rights under this Agreement independently of FRSI.

GENERAL: You may not sublicense, assign, or transfer the license or the program and related materials without the prior written consent of FRSI. Any attempt otherwise to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder without such consent is void.

Should you have any question concerning this Agreement, please contact your FRSI representative or sales office.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN US WHICH SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, EXCEPT THE MASTER LICENSE AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS BETWEEN US RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT. YOU AGREE THAT FRSI MAY AUDIT YOUR FACILITY TO CONFIRM COMPLIANCE OF THE FOREGOING PROVISIONS.

Contents

Appendices and reference

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 or Ovation 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*, Ovation system interface deployment concepts – Provides architecture diagrams for implementing AMS Device Manager with Ovation.
- *Appendix C*, Other deployment concepts – Provides architecture diagrams for implementing AMS Device Manager with supported system interfaces.
- *Appendix D*, Version compatibility – Provides matrices on AMS Device Manager compatibility with SNAP-ON applications, DeltaV, and Ovation.

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.

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 9*)
- Database backup procedures (see *page 3*)
- Database restore procedures (see *page 4*)

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.

Installation overviews

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

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.

1. Read *Before you begin* on page 1.
2. Confirm that your system meets AMS Device Manager requirements on *page 9*.
3. Do one of the following:
   - For a new installation, follow the Server Plus Station installation steps on *page 56*.
   - For upgrading from AMS Device Manager 12.5 or later, see *page 51*.

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.

1. Read *Before you begin* on page 1.
2. Confirm that your system meets AMS Device Manager requirements on *page 9*.
3. Do one of the following:
   - For a new installation, follow the Server Plus Station and Client SC Station installation steps on *page 49*.
   - For upgrading from AMS Device Manager 12.5 or later, see *page 51*.

Install AMS Device Manager on a DeltaV system

1. Read *Before you begin* on page 1.

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 71*.

Install AMS Device Manager on an Ovation system

1. Read *Before you begin* on page 1.
2. Confirm that your system meets minimum requirements for a co-deployment (refer to the documentation provided with your Ovation system).
3. Follow the installation steps on *page 72*.

Database operations

The following database procedures are essential to successfully install or upgrade to AMS Device Manager 14.0:

- *Back up a database* on page 3 – Do this procedure before upgrading to AMS Device Manager 14.0.
- *Restore a database* on page 4 – Do this procedure after upgrading AMS Device Manager to 14.0 from version 9.0 to 11.5.

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.

1. Enter Database Backup on the Start screen and click Database Backup.
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.

   Notes

   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 Database Verify Repair until there are no more errors and repeat steps 1 to 3.

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.

1. Close AMS Device Manager and any related applications (for example, Alert Monitor, 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.

Uninstall AMS Device Manager

You must uninstall AMS Device Manager if you are upgrading to the current version from versions 9.0 to 11.5. You do not need to uninstall the current AMS Device Manager software if you are upgrading from version 12.0 or higher. AMS Device Manager must always be uninstalled when co-deployed with a DeltaV system being upgraded.

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).

1. Back up the database (see *page 3*).
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.

Reference documents

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

- *AMS Device Manager Books Online*
- *AMS Device Manager Planning and Installation Guide*
- *Release Notes*
- *Supported Device List*

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.

What's This? Help

You can get help for device parameters on most AMS Device Manager supported devices by clicking  and then clicking on a field. The help is displayed in a window that you can dismiss by simply clicking anywhere on the screen. This help is provided by the device manufacturer and can also be viewed by clicking in a field and pressing the F1 key.

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.

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 DVD1

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

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 DVD 2.

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.

Product data sheets and white papers

AMS Device Manager product data sheets provide product descriptions, features, and benefits. White papers help you understand AMS Device Manager systems and items important to system planning. Please have the sheets 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 product data sheets or white papers. The data sheets and white papers are available on the *Emerson* website.

Knowledge Base Articles

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

- KBA NA-0400-0046 *Firewall Whitepaper to be Used for AMS Device Manager Installations*
- KBA NA-0400-0084 *AMS Device Manager Multiplexer System Interface Setup & Troubleshooting Guide*
- KBA NA-0500-0085 *Configuring Windows Firewalls for AMS Device Manager functionality*
- 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 NA-0700-0071 *Interoperability Requirements Between AMS Device Manager and Ovation*
- KBA NK-1300-0136 *Device Description Update Manager Architectures and Information*
- KBA NK-1300-0138 *Softing FG-110 HSE Linking Device is Now Supported With AMS Device Manager*
- KBA NK-1300-0268 *AMS Device Manager Support in Virtual Environments*
- KBA NK-1500-0051 *Suggested Memory Configuration for SQL Server When Used With AMS Device Manager*
- KBA NK-1800-0002 *Guidelines For Installing A Standard Version Of SQL Server 2014 To Be Used With AMS Device Manager V14.x*

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.

Sizing considerations

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

System Sizing	Quantity	Supported Maximum	Comments
Number of wired HART Devices?			If the system will support more than 3,000 devices, see the requirements on *page 19*.
Number of FF Devices?			
Number of *Wireless*HART Devices?			
Wireless Gateway?		16 Wireless Gateways for each Wireless Interface	Each Wireless Gateway requires an AMS Tag
*Wireless*HART Adapters?			Each *Wireless*HART Adapter requires an AMS Tag
Number of PROFIBUS DP and PROFIBUS PA Devices?			
Conventional Devices?			
Multiplexers?		3,000 tags per station	Each multiplexer requires an AMS Tag
Calibrators?			Some calibrator modules require an AMS Tag
Number of devices connected using Det-Tronics EQP system (including EQP Controller)?			How many fire and gas detectors are on the Det-Tronics EQP system?
Total Tag Count?		30,000 (Per System)	Supported Maximum: 30,000 (Per System)
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	Required System Interfaces	Total Number of Devices Connected per Interface	Comments
DeltaV			When installing AMS Device Manager on a DeltaV system, a licensed AMS Device Manager station (ServerPlus or ClientSC) must be installed on the ProfessionalPLUS.
Ovation			AMS Device Manager Server Plus software is NOT supported on an Ovation Database Server. ClientSC only.
HART Modem			
FOUNDATION fieldbus modem			
Wireless Network			Emerson recommends a maximum of 16 wireless gateways for each Wireless Interface.
FF HSE Network			
Multiplexer Interface			You should not exceed 10 of the 32 Channel Multiplexers or 2 of the 255 Device Multiplexers per Multiplexer Network. Emerson recommends a maximum of 3000 devices per station. A system should have no more than 14 interfaces per station.
Stahl Network			Requires Multiplexer Interface licensing.
8000 BIM Network			Requires Multiplexer Interface licensing.
RS3 Network			The AMS ValveLink SNAP-ON application is not supported with this interface.
PROVOX Network			
Kongsberg			
HART Over PROFIBUS			
ABB			
PROFIBUS			

Supported System Interfaces	Required System Interfaces	Total Number of Devices Connected per Interface	Comments
Field Communicator		• You can only connect one 375/475 Field Communicator at a time to an AMS Device Manager station. • You can only connect one AMS Trex unit at a time to an AMS Device Manager station using USB. • You can connect multiple AMS Trex units to an AMS Device Manager station using WiFi.	
Calibrator			
USB Fieldbus Interface			
Det-tronics			

Networking Considerations	Quantity	Supported Maximum	Comments
Number of Network Domains?			If you will be installing AMS Device Manager on a Domain Controller, it must be installed on the Domain Controller before installing on the Non-Domain Controller computers. See *KBA NA-0800-0113* for more information about domains and installing on Domain Controllers. AMS Device Manager supports deployment within a single domain or workgroup or across multiple domains or workgroups. Moving from a workgroup to a domain requires you to uninstall AMS Device Manager, add the PC to the domain, and reinstall.
Number of Network Workgroups?			The Hosts file on each AMS Device Manager station must be modified to include the computer names and IP addresses for all AMS Device Manager computers in the network. AMS Device Manager supports deployment within a single domain or workgroup or across multiple domains or workgroups.
Number of Networks that will have an AMS Device Manager station?			

Networking Considerations	Quantity	Supported Maximum	Comments
Number of Ethernet Serial Hubs?			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.
Network Firewalls		N/A	Complement firewalls with antivirus software. If AMS Device Manager is installed on a DeltaV workstation, an Ovation Station, etc., be sure to install an antivirus software according to the specifications of those systems. See KBAs *NA-0400-0046* and *NA-0500-0085* for more information.

Networking Considerations	Quantity	Supported Maximum	Comments
Will Remote Desktop Services or Remote Desktop Session Host be used? (Yes or No)		5 Concurrent Sessions	Use of Remote Desktop Services or Remote Desktop Session Host is limited to 5 concurrent sessions when AMS Device Manager is installed. If you are using Remote Desktop Session Host, it must be installed before AMS Device Manager installation. The level of support of Remote Desktop Services with AMS Device Manager SNAP-ON applications varies. For more detailed information, contact the SNAP-ON application manufacturer. When implementing Remote Desktop Services or Remote Desktop Session Host, a Client SC Station license should be purchased for each session. Questions regarding station licensing requirements should be directed to your local Emerson sales office. See *page 17* for information about supported operating systems.

Hardware Considerations	Quantity	Comments
HART Modems?		
Field Communicators?		
Calibrators?		
HART Multiplexers?		
RS232 to RS485 Converters?		
Ethernet Serial Hubs?		
USB Fieldbus Interface?		
PROFIBUS Gateways		
PROFIBUS Couplers		

Hardware requirements

PC processing speed, memory, and disk space

Station Type	Minimum requirements
Server Plus Station	Intel® Core™ i5 quad processor, 2.4 GHz or greater 8 GB or more of memory[1] 10 GB or more of free hard disk space[2, 3, 4, 5]
Client SC Station	Intel® Core™ i5 dual processor, 2.4 GHz or greater 8 GB or more of memory[1] 10 GB or more of free hard disk space[2, 3, 4, 5]
Notes	
[1] Set virtual memory to 2-3 times the size of the physical memory.	

Serial interfaces

- 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 VMWare and Hyper-V virtual PCs is NOT supported.

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 and USB Fieldbus Interface drivers are required to use the USB Fieldbus Interface.
- 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.
- A USB port is required to connect a 375 or 475 Field Communicator using a USB Infrared Data Association (IrDA) adapter. In some cases, IrDA drivers may be necessary. See the *Release Notes* for a list of supported adapters.
- A USB port is required to connect a 475 Field Communicator or Bluetooth modem using a USB Bluetooth adapter. Only Microsoft Bluetooth components are supported (see the *Release Notes* for more information).
- 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.

Network requirements

- 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 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 62*).
- 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 77*.

Note

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

Software requirements

Operating systems

AMS Device Manager supports the following Windows operating systems:

Operating System	Version	Service Pack
Windows 7	Professional or greater editions	1
Windows 10	Professional or greater editions	
Windows Server 2008 R2	Standard or greater editions	1
Windows Server 2012 R2	Standard or greater editions	
Windows Server 2016	Standard or greater editions	
Notes		
• Only 64-bit versions of the operating systems are supported. • Desktops, laptops, and tablets with touchscreens are supported on Windows 10. • 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 operating system families is supported only in the following combinations: Windows 7 and Windows Server 2012 R2 PCs; Windows 10 and Windows Server 2012 R2 PCs. • 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 19*); 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* on page 77 for additional operating system configuration considerations. • AMS Device Manager also supports localized versions of the listed operating systems.		

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 *http://www2.emersonprocess.com/en-US/brands/sureservice/availabilityservices/guardiansupportservice/Pages/GuardianSupportService.aspx*.

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 14.0 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 AMS Device Manager is co-deployed with DeltaV, Remote Desktop Services is disabled except on virtual PCs.
- 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.

Web browsers

AMS Device Manager supports the following web browsers:

- Microsoft Internet Explorer version 11
- Microsoft Edge

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 14.0 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.

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.

.NET Framework

AMS Device Manager requires

- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 3.5 Service Pack 1.

Database

AMS Device Manager 14.0 uses a named instance, Emerson2014, of SQL Server 2014 Service Pack 2 for its database. The size of your database determines which edition of SQL Server 2014 Service Pack 2 you must use:

- *If your database is less than 10 GB*, you can use SQL Server 2014 Express Service Pack 2. The AMS Device Manager 14.0 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 2014 Service Pack 2 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 (including AMS Suite APM), a full version of SQL Server 2014 Service Pack 2 is recommended regardless of database size.

A full version of SQL Server 2014 Service Pack 2 must be purchased separately (if you do not already have it). We recommend that the full version of SQL Server 2014 Service Pack 2 is installed on a server operating system.

Notes

- Contact Microsoft for more information about appropriate licensing for a full installation of SQL Server 2014.
- 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.
- If you are installing other applications on the computer where AMS Device Manager and a full version of SQL Server 2014 Service Pack 2 is installed, do NOT use the default Maximum server memory setting in SQL Server Management Studio. See *KBA NK-1500-0051* for more information.

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

- If SQL Server 2014 Service Pack 2 is not installed, the AMS Device Manager 14.0 installation program will install SQL Server 2014 Express Service Pack 2 with Advanced Services, and create an Emerson2014 named instance.
- If an instance of SQL Server 2014 Service Pack 2 is installed, but not the Emerson2014 named instance, the AMS Device Manager 14.0 installation program will create the Emerson2014 named instance.
- If the SQL Server 2014 Service Pack 2 Emerson2014 named instance is already installed, the AMS Device Manager 14.0 installation program will continue with the next part of the installation.
- If you have previously installed a full version of SQL Server 2014 Service Pack 2, you should create the Emerson2014 named instance before installing AMS Device Manager 14.0 (refer to your SQL Server documentation). Otherwise, the AMS Device Manager installation will install SQL Server 2014 Express Service Pack 2.

Microsoft Office

The following Microsoft Office applications are supported:

- Microsoft Word 2010, 2013, 2016 (for Drawings and Notes)
- Microsoft Excel 2010, 2013, 2016 (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.

Windows security requirements

AMS Device Manager installation

You need Windows system administrator rights to install and configure AMS Device Manager. Other network security requirements may also apply to the installation. 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.

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.

AmsServiceUser

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.

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 68*).

This user account runs the AMS Device Manager Servers. 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 74*) 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.

Requirements for system interfaces

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

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.

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 2008, Windows Server 2012, or Windows Server 2016.
- Installing a HART Modem in Network Configuration requires Windows Administrators group permissions.

Field Communicators

The Trex, 475 and 375 Field Communicators are portable, handheld communicators from Emerson used in the field or in the shop to configure, test, and diagnose HART and FOUNDATION fieldbus devices. For information on using the Field Communicators, see their respective manuals.

The Field Communicator Interface is a licensable option that lets you use a Field Communicator and AMS Device Manager together to transfer HART and FOUNDATION fieldbus data. Trex communicates with an AMS Device Manager station automatically, after an initial pairing in AMS Device Manager. The 475 communicates with an AMS Device Manager station using a USB IrDA adapter (ordered separately) or the Microsoft Windows Bluetooth interface on a Bluetooth-enabled PC. The 375 communicates with an AMS Device Manager station using a USB IrDA adapter (ordered separately). You can communicate with only one Field Communicator at a time on a PC. Communication between AMS Device Manager and a connected Field Communicator is initiated by the AMS Device Manager software.

The AMS Trex Device Communicator uses the Field Communicator license, and communicates with AMS Device Manager on USB and 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.

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

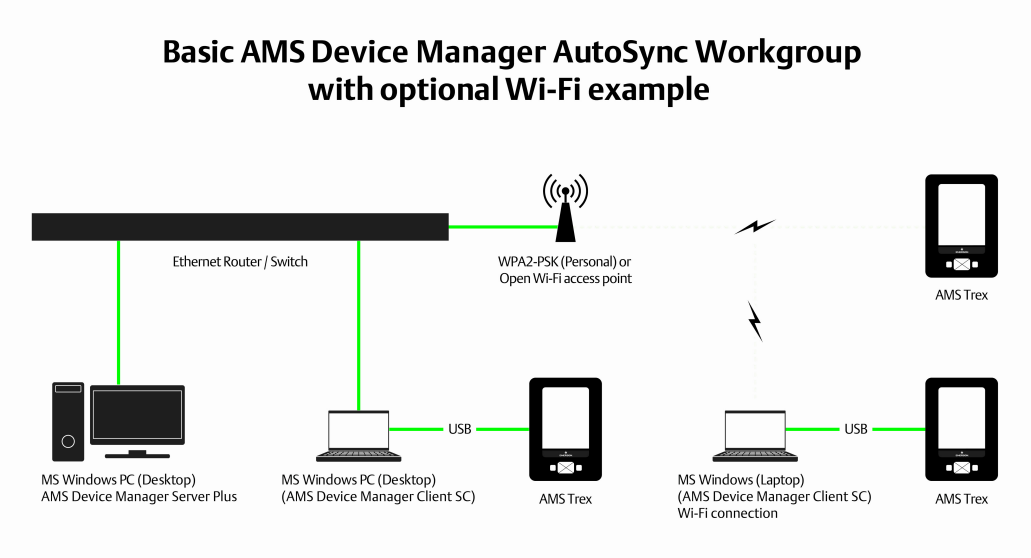
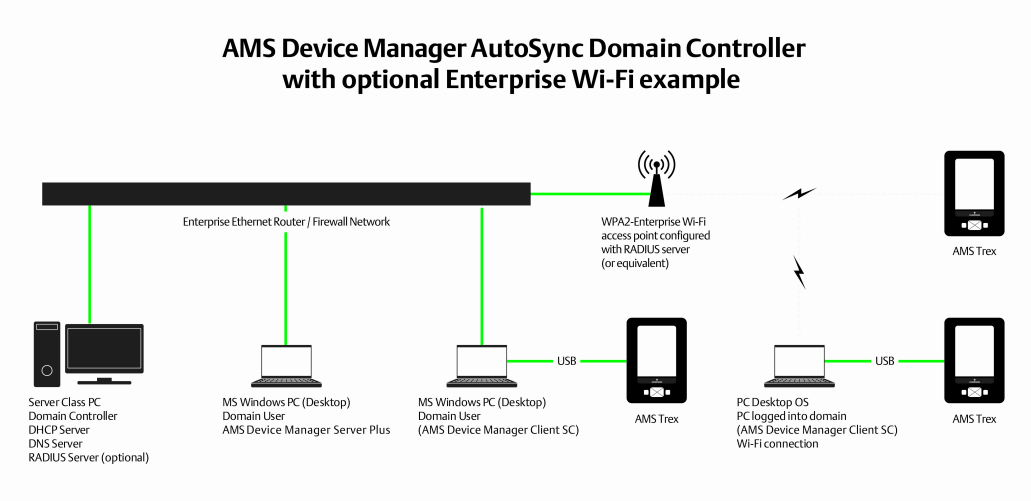


Figure 2-2: AMS Trex connection points in a domain



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 702, 743*, 744*, 754*
- Druck DPI605, DPI615, DPI620 CE/IS/Genii+, MCX 2, Unomat TRX-II
- Rosemount P330, P370, T460, T490
- Beamex MC5*, MC5-IS*, MC5P*, MC3, MC5FF, MC6
- 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 following calibrators support downloading of test definitions for fieldbus devices:

Beamex MC5, MC5-IS, MC5P, MC3, MC5FF, MC6

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

8000 BIM

The 8000 BIM System Interface displays HART field devices connected to an 8000 BIM system.

The physical connection between your AMS Device Manager PC and the 8000 BIM system requires one of the following:

- A serial connection using an RS-485 converter (BIM)
- An Ethernet connection using TCP/IP addressing (eBIM)

Supported analog input modules:

- 8101-HI-TX — 4-20mA, 8 channel, Div. 2/2
- 8201-HI-IS — 4-20mA, 8 channel, Div. 2/1
- 8301-HI-IS — 4-20mA, 8 channel, Div. 1/1

Supported analog output modules:

- 8102-HO-IP — 4-20mA, 8 channel, Div. 2/2
- 8202-HO-IS — 4-20mA, 8 channel, Div. 2/1
- 8302-HO-IS — 4-20mA, 8 channel, Div. 1/1

ABB

The ABB System Interface lets you use AMS Device Manager to view and configure HART devices connected to I/O modules supported by the ABB System 800xA control system.

AMS Device Manager Client SC Station or Server Plus Station software can be installed on an ABB Station if PC hardware and software requirements are met, or on a separate PC. The ABB Station must have the 800xA station software installed and configured for AMS Device Manager to communicate with HART instruments connected using the ABB Controller. The ABB System Interface requires:

- That the ABB Network is licensed in AMS Device Manager.
- That the ABB Station software version is 5.1 along with the “Performance Pack” enhancement release from ABB.

- That the ABB communications certificate be manually installed. See ABBSystemInterface-Readme.pdf inside the SNAP-ONS And Tools\ABB HPT Certificate folder on the AMS Device Manager DVD 2 for installation instructions.
- The AMS Device Manager user must be the same as the ABB user on the station that runs the "ABB HART Pass Through Service".
- Use of the AC 800M series controllers.
- Use of supported multiplexers, including:
  - Pepperl+Fuchs KFD2-HMM-16
  - MTL4840
  - Elcon Series 2700-G

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 14.0 can only be installed on the following DeltaV 12.3, 12.3.1, 13.3, 13.3.1, and 14.3 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 - Professional - Operator - Base - Maintenance	Server Plus Station or Client SC Station
Operator Station as Remote Client Server	Client SC Station only
Remote "Operate" Station - Professional - Operator - 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 12.3 and later in co-deployed installations only.

Table 2-1: Supported DeltaV Controllers

Item Type	Item	Versions*
Controller	MD	v12.3.0 or higher
	MD+	v12.3.0 or higher
	MX	v12.3.0 or higher
	SD+	v12.3.0 or higher
	SX	v12.3.0 or higher
	MQ	v12.3.0 or higher
	SQ	v12.3.0 or higher
	PK	v14.3.0 or higher

Table 2-1: Supported DeltaV Controllers *(continued)*

Item Type	Item	Versions*
HART I/O	HART AI 8 channel Card, Series 1	Rev. 2.21 or higher
	HART AI 8 channel Card, Series 2	Rev. 1.26 or higher
	HART AI 16 channel Card	Rev. 1.17 or higher
	HART AO Card, Series 1	Rev. 2.25 or higher
	HART AO Card, Series 2	Rev. 1.26 or higher
	HART AI 8 channel card S-Series	Rev 1.26 or higher
	HART AI 16 channel card S-Series	Rev 1.17 or higher
	HART AO Card, S-Series	Rev. 1.26 or higher
	HART AI Redundant High Density S-Series	Rev. 1.0 or higher
	HART AO Redundant High Density S-Series	Rev. 1.0 or higher
IS I/O HART	IS AI HART 8 channel Card	Rev. 2.39 or higher
	IS AO Hart 8 channel Card	Rev. 2.00 or higher
Zone 1 I/O	AI/AO	Rev 1.14 or higher
Fieldbus I/O	Fieldbus H1 Series 1	Rev 1.8 or higher
	Fieldbus H1 Series 2	Rev 2.2 or higher
	Fieldbus H1 S-Series Integrated Power	Rev 4.87 or higher
	Fieldbus H1 S-Series	Rev 2.2 or higher
	Fieldbus H1 S-Series 4 port	Rev 1.0 or higher
PROFIBUS I/O	PROFIBUS Series 2+	Rev 1.36 or higher
Wireless I/O	WIOC	v12.3.1 or higher
	Smart Wireless Gateway	v3.95 or higher
CHARM I/O	CIOC	v12.3.1 or higher
	CIOC2	v14.3.0 or higher
	AI 4-20 mA HART CHARM	v1.18 or higher
	AO 4-20 mA HART CHARM	v1.18 or higher
	AI 4-20 mA HART (Intrinsically Safe) IS	v1.74
	AO 4-20 mA HART (Intrinsically Safe) IS	v1.76
PROVOX Migration I/O		
Controller	M-Series	Version V12.3 or higher
	S-Series	V12.3.1 or higher

Table 2-1: Supported DeltaV Controllers *(continued)*

Item Type	Item	Versions*
RS3 Migration I/O		
Controller	M-Series	Version 7.2 or higher
SIS Logic Solver I/O		
Logic Solver	SLS	Version 1.1 or higher
SIS CHARM I/O		
Controller	SZ	V12.3 or higher
Logic Solver	CSLS	V1.1 or higher
CHARM	LS AI 4-20 mA HART	V1.15 or higher
	LS AI 4-20 mA HART (Intrinsically Safe)	V1.15 or higher
	LS DVC HART DTA	V1.16 or higher
	LS DVC HART (Redundant DTA)	V1.16 or higher

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 12.3 or higher with an S-Series 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 12.3 or later (SIS) CHARMs logic solvers

DeltaV versions 12.3 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 79*).

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 AMS ValveLink SNAP-ON application is supported for DeltaV and PROVOX I/O cards, but not for RS3 cards. See *page 46* for I/O requirements.

The DeltaV System Interface supports AMS 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.

DeltaV Simulate support

This targeted DeltaV System provides an offline development environment that can be used to test new process configurations, provide training for system personnel, and is not designated for use in a production environment. A DeltaV Simulate Standalone station has a single DeltaV simulation station that functions like a ProfessionalPLUS station with no licensing limits on size and functionality.

A DeltaV Simulate Multi-node system has two or more simulation stations that communicate over a DeltaV Control Network. It consists of one networked ProfessionalPLUS Station and quantities of networked Professional Stations, Operator Stations, and Application Stations. Actual controllers can be used in a DeltaV Simulate Multi-node system by connecting them to the DeltaV Control Network.

A Simulate ID key (VX Dongle) is required to identify a DeltaV Simulate Multi-node system.

For AMS Device Manager system requirements for use with DeltaV Simulate, contact you local Emerson sales office.

Det-Tronics

The Det-Tronics System Interface is used to monitor fire and gas detectors on the Det-Tronics Eagle Quantum Premier (EQP) fire and gas safety system.

Before configuring the system interface, you must:

- Install the Det-Tronics Safety System Software (S3) application version 8.7.x.x or higher
- Install the Det-Tronics EQP application
- Program the S3 dongle/key to include the AMS Driver

The Det-Tronics System Interface supports alerts for devices if the following are true:

- AMS Device Manager Server is running on the station where the Det-Tronics network is connected.
- The device has been previously identified.
- The device is in the Device Monitor List.

FF HSE

The FF HSE System Interface lets you use AMS Device Manager to configure and view alerts for FOUNDATION fieldbus devices connected to FOUNDATION fieldbus linking devices.

The FF HSE System interface requires:

- One or more (up to 64) commissioned FF HSE Linking Devices that conform to the FOUNDATION fieldbus HSE and H1 specifications. The Remote Operations Controller for FOUNDATION fieldbus (ROC FF) and the ControlWave linking devices are displayed in AMS Device Manager in the FF HSE hierarchy. For setup and configuration of ROC FF and ControlWave linking devices, see the documentation supplied with them.

Note

All linking devices on the same network must have unique tag names. If duplicate tag names are used, the hierarchy will not build properly.

- The device manufacturer's commissioning/decommissioning utility.
- FF HSE Linking Devices with unique TCP/IP addresses.
- An AMS Device Manager station with 1 or 2 Ethernet network interface cards (NIC). A NIC dedicated to the FF HSE segment is recommended to reduce the amount of competing network communications.

The following linking devices are supported:

Manufacturer	Device ID	Device Type	Web Interface	Version	Notes
Rosemount	0x001151	0x0770	No	NA	see 1) below.
Smar	0x00302	0x0026	Yes	V 1_0_0-RC10	FF HSE Linking Device is registered with the Fieldbus Foundation. FF Devices are always powered by separate power source.
Softing	0x1E6D11	0x4000	Yes	NA	FG-100 does not support alerts. FG-110 does support alerts. FG-200 replaces both FG-100 and FG-110

Manufacturer	Device ID	Device Type	Web Interface	Version	Notes
Remote Automation Solutions	0x524153	0x0001 (ROC)	Yes	3.1.15 or greater	Requires a Fieldbus Interface Module (FIM) that supports HSE. The H1 links provide power to the FF devices.
	0x524153	0x0002 (ControlWave)	Yes	3.1.15 or greater	Requires a Fieldbus Interface Module (FIM) that supports HSE. The H1 links provide power to the FF devices.
1) The Emerson USB Fieldbus Interface implements a single FF H1 Link. A separate driver and configuration utility installation is required, which is included with the interface. A single USB Fieldbus Interface can optionally power approximately 2-3 FF devices. Up to 16 devices can be accessed by a single USB Fieldbus Interface if the devices are powered from an external source or if accessed as a visitor.					

NOTICE

If you have an Ovation System Interface installed, use the network interface card IP address of the FF HSE Server for the FF HSE System Interface.

USB Fieldbus Interface

The USB Fieldbus Interface enables two-way communication between an AMS Device Manager station and fieldbus devices through USB connection. While other linking devices are connected using a dedicated Ethernet card, the USB Fieldbus Interface enables direct connection to fieldbus devices using standard USB cables.

The interface is always configured as a "visitor" and allows the setup, configuration, monitoring, and troubleshooting of fieldbus devices without interfering with existing segments controlling automation processes. The interface can detect a Link Active Scheduler (LAS) and can take over as LAS if it is not present on the segment.

AMS Device Manager supports one USB Fieldbus Interface in an FF HSE network. See the *USB Fieldbus Interface User's Manual* for more information.

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 2-2: 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.

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

Manufacturer	Model	Max Channels	Hardware supports Enhanced Polling	Default in AMS Device Manager	Notes
Pepperl + Fuchs/ Elcon	2700G	32	Yes	On	The P+F/Elcon 2700G must be upgraded with firmware version 7 or later to work correctly with AMS Device Manager version 7.0 or higher.
	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.
Pepperl + Fuchs	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 2-2: Supported HART Multiplexers *(continued)*

Manufacturer	Model	Max Channels	Hardware supports Enhanced Polling	Default in AMS Device Manager	Notes
MTL	4841/4842 (Device Type 15)	256	No	Off	MTL recommends customers with MTL 4841-AMS multiplexers, who want to use enhanced polling, contact MTL about upgrading to an MTL 4841-AMSv7 multiplexer. You will either have to return the MTL 4841-AMS multiplexer to MTL 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 AMS ValveLink SNAP-ON application.

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

Manufacturer	Model	Max Channels	Hardware supports Enhanced Polling	Default in AMS Device Manager	Notes
	4850	32	Yes	On	
	4850-TR	32	Yes	Off	
	4851-4852	16	Yes	Off	
	4854	32	Yes	Off	
	8000/8512	256	No	Off	
	Novatech 8000	256	No	Off	
Spectrum	Connects (v6.0)	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).
Stahl	ICS Modul 9161/ 9148				Uses the Stahl HSI interface
	VOS 200 9503/9548				
	I.S. 1 9440/9461/ 9466				
	I.S. 1 9440/9468				
	IS PAC				
Phoenix Contact	MACX MCR-S-Mux				
	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)

(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*.

HART Over PROFIBUS

The HART Over PROFIBUS System Interface lets you use AMS Device Manager to view and configure HART devices that are connected to PROFIBUS remote I/O subsystems via the Softing Ethernet PROFIBUS Interface (xEPI) PROFIBUS Gateway. The interface addresses the gateway by either its DNS or IP address.

Note

Before upgrading to AMS Device Manager 14.0 from previous versions supporting HART Over PROFIBUS, contact your Emerson Sales/Service Office to ensure your system is fully supported. Additional testing may be required.

The HART Over PROFIBUS System Interface requires that:

- AMS Device Manager is installed on a PC running a supported operating system.
- A control system that supports PROFIBUS DPV1 is configured and operational.
- At least one Softing PROFIBUS Gateway (xEPI-2 HW2.0 or FW 5.2.2.6) for communications is configured and the T+H AMS Device Manager Communications Components (TACC) software version 3.20 is installed.
- At least one PROFIBUS DP remote I/O subsystem that supports HART communications is connected to the control system.
- At least one HART I/O module is installed in the remote I/O subsystem.
- At least one HART instrument is present on a module channel.

Table 2-3: Supported Controllers for HART over PROFIBUS

Controller	Hardware	Software Version
ABB AC 800M with CI854	0205	FW 5.54
ABB CMC 70	CMC70-0/AC 870P/PM875	FW 2.04
Siemens Simatic S7	S7 315-2DP (6ES7 315-2AF01-0AB0)	E-Stand 2
	S7 400-H CPU 417-4 H (6ES7 417-4HT14-0AB0)	E-Stand 1; FW 4.5.6
Altus Ponto 4053 Redundant	CPU PO3247	Rev AK 130 Beta4

Table 2-3: Supported Controllers for HART over PROFIBUS *(continued)*

Controller	Hardware	Software Version
	Master PROFIBUS Interface PO4053	Rev BG and BF

Table 2-4: Supported Remote I/O for HART over PROFIBUS

Remote I/O Type	Hardware	Software Version
ABB S800	CI840	FW 3.2/1
	AI845	
	AO845	
	AI895	
	AO895	
	CI801	FW 1.2/3
	AI815	
	AO815	
ABB S900	CI920S AI930N AI4H AO930N AO4H	FW 1.42 FW 1.79 FW 1.79
Altus Ponto 5064	PO5064 PO1114 8AI PO2134 4AO	FW1.01 FW1.00 and FPGA FW1.00 and FPGA
Altus Ponto 5065 Redundant	PO5065 PO1114 8AI PO2134 4AO	FW1.01 FW1.00 and FPGA FW1.00 and FPGA
MTL 8000	850-BI-DP 802-HO-04 818-DX-08 801-HI-04 815-DO-04	FW. 1.63 FW 1.79 FW 1.41 FW 1.43

Table 2-4: Supported Remote I/O for HART over PROFIBUS *(continued)*

Remote I/O Type	Hardware	Software Version
Pepperl + Fuchs LB	LB 8106 - PROFIBUSDPV1 Comm. Interface LB 8109 - PROFIBUS DPV1 Comm. Interface LB 3002 1AI HART LB 3102 1AI HART LB 3103 1AI HART LB 3105 4AI HART LB 3106 4AI HART LB 3107 4AI HART LB 4005 4AO HART LB 4002 1AO HART LB 4102 1AO HART LB 4106 4AO HART LB 7104 4AIO HART	Rev 6.23
Pepperl + Fuchs FB	FB 8206 – PROFIBUS DPV1 Comm. Interface FB 3202 1 AI HART FB 3205 4 AI HART FB 3305 4 AI HART FB 4202 1 AO HART FB 4205 4 AO HART	Rev 6.25
Pepperl + Fuchs RPI	KSD2-GW2-PRO KSD2-CI-S-Ex.H KSD2-CO-S-Ex.H KSD2-CI-S-Ex.2H	Rev. 1.3 Rev. 3.3 Rev. 2.2 Rev. 1.1
Siemens ET 200iSP	IM 152-1 (6ES7 152-1AA00-0AB0)	E-Stand 4
	SM 134 AI 4x HART 2 Wire (6ES7 134-7TD00-0AB0)	E-Stand 4
	SM 134 AI 4x HART 4 Wire (6ES7 134-7TD50-0AB0)	E-Stand 4
	SM 135 AO 4x –HART (6ES7 135-7TD00-0AB0)	E-Stand 5
	4 F-AI I 2 Wire HART (6ES7138-7FA00-0AB0)	E-Stand
Siemens ET 200M	IM 153-2 (6ES7 153-2BA00-0XB0)	E-Stand: 4
	IM 153-2 (6ES7 153-2BA02-0XB0)	E-Stand: 1

Table 2-4: Supported Remote I/O for HART over PROFIBUS *(continued)*

Remote I/O Type	Hardware	Software Version
	SM 336 AI 6x HART (6ES7 336-4GE00-0AB0)	E-Stand: 3; FW 1.02
	SM 331 AI 8x HART	
	(6ES7 331-7TF00-0AB0)	E-Stand: 4
	(6ES7 331-7TF01-0AB0)	E-Stand: 1
	SM 332 AO 8x HART	
	(6ES7 332-8TF00-0AB0)	E-Stand: 1
	(6ES7 332-8TF01-0AB0)	E-Stand: 2
STAHL I.S.1	CPM 9440/15-01-11	FW 02-30
	AIM HART 08 9461/12-08-11	C 00-34
	AIM HART 08 9461/12-08-21	
	AOM HART 08 9466/12-08-11	C 02-02
	AUM HART 08 9468/32-08-11	
Turck BL20	GW-DPV1 2AOH-I 2AIH-I E-GW-EN 2AOH 2AIH-I	FW 1.22 VN 01-02 VN 02-01 VN 01-01 FW 1.27 VN 01-02 VN 02-01
Turck Excom	GDP 1,5 AIH40Ex AOH40Ex	FW 1.6.2 FW 1.79 FW 1.79
Wago	750-333 Fieldbus Coupler	SW 17 / HW 20
	750-833 Programmable Fieldbus Controller	SW 16 / HW 20
	750-482 2-Channel Analog Input	SW 04 / HW 05
	750-484 2-Channel Analog Input (Ex I)	SW 03 / HW 03
	753-482 2-Channel Analog Input	SW 04 / HW 05

See the *TACC Release Notes, version 3.20* from Softing for more information.

Kongsberg

The Kongsberg System Interface lets you use AMS Device Manager to communicate with HART devices using I/O modules supported by the Kongsberg Maritime System. The Kongsberg Network communicates with HART devices using the Kongsberg Automation Server which is an application with a Web Service interface.

The Kongsberg System Interface is deployed where there is access to the Kongsberg Automation Server with IIS. Install the Kongsberg Automation Server on an AMS Device Manager station for best communication performance.

If you install additional Kongsberg System Interfaces, each must be linked to unique Kongsberg Automation Server URLs. The Kongsberg System Interface supports communications with HART instruments connected to STAHL ISPac HART Multiplexers and STAHL PROFIBUS DP Remote I/O modules for HART.

The Kongsberg System Interface requires that:

- The version of the Kongsberg Control System is AIM v8.3.
- The Kongsberg System is set up and the Automation Server is accessible from the AMS Device Manager station.
- The URL for the Kongsberg Automation Server is known.
- One or more Remote Control Units (RCUs) or HART-IP Gateway nodes are available on the Kongsberg Network where PROFIBUS Masters or HART Masters may be configured.
  - PROFIBUS Masters allow the connection of HART DP Slave and I/O Modules, which connect HART instruments to the network.
  - HART Masters allow the connection of HART Multiplexers, which connect HART instruments to the network.

OpenEnterprise

The OpenEnterprise System Interface lets you use AMS Device Manager to view and configure wired HART and *Wireless*HART devices connected to an OpenEnterprise SCADA System and associated Remote Terminal Unit (RTU) controllers (that is, ROC800 series, FloBoss 107, and ControlWave).

The OpenEnterprise System Interface requires that:

- The version of OpenEnterprise Server is 3.2 or higher.
- The OpenEnterprise Server is installed on an AMS Device Manager 14.0 PC or on a network-accessible PC. If the OpenEnterprise Server is on a different PC, you must install an OpenEnterprise OPC Alarms & Events instance on the AMS Device Manager station with an OpenEnterprise System Interface to get device alerts.
- Only one OpenEnterprise System Interface is allowed for each AMS Device Manager station.

The following firmware on controllers are supported on the OpenEnterprise System Interface:

- ROC 800 Series Controller:
  - ROC 809, ROC 827 Series 2 FW v3.70
  - ROC 800L, FW v1.50
  - ROC DL8000 Series 2 FW v1.80
- FloBoss Series Controller:
  - FB107 FW v1.80
  - FB103 FW v2.15
  - FB104 FW v2.15
  - FB407 FW v1.14
  - FB503 FW v2.48
  - FB504 FW v2.48
- ControlWave Series Controller:
  - ControlWave, ControlWave Micro, FW v5.75
- Modules:
  - IEC62591 Smart Wireless Module, Rev 1.11 for ROC800, FloBoss, ControlWave series

Note

The OpenEnterprise System Interface cannot be installed on an AMS Device Manager station with a DeltaV System Interface.

Ovation

The Ovation System Interface lets AMS Device Manager communicate with HART, FOUNDATION fieldbus, PROFIBUS DPV1, and *Wireless*HART devices through an existing Ovation network. The Ovation network communicates with devices through one or more Ovation controllers. HART devices communicate with the Ovation controller through I/O modules specifically designed to communicate with HART equipment. FOUNDATION fieldbus devices communicate with the Ovation controller through I/O modules designed to communicate with FOUNDATION fieldbus devices. PROFIBUS DPV1 devices communicate using I/O modules designed for PROFIBUS. *Wireless*HART devices communicate through the Smart Wireless Gateway. Device information is passed through the Ovation controller to a Windows-based Ovation Station from which AMS Device Manager accesses device data.

FOUNDATION fieldbus device commissioning and decommissioning is accomplished through the Ovation fieldbus engineering software used by the Ovation system. AMS Device Manager is not part of this process. A FOUNDATION fieldbus device must be commissioned before AMS Device Manager can communicate with it.

AMS Device Manager 14.0 can be deployed with Ovation as a standalone or co-deployed system.

Ovation System Interface station software requirements:

- AMS Device Manager 14.0 can be installed on the following Ovation 3.5.1 and 3.6 stations:

Ovation workstations	AMS Device Manager station
Operator Station	Server Plus Station or Client SC Station
Database Server	Client SC Station

Notes

- If you install AMS Device Manager and configure an Ovation System Interface on a PC that is not an Ovation Station and try to access SIS HART devices, performance will be significantly affected if the host file on the AMS Device Manager station is missing specific entries. To improve performance, add the IP address and hostname for each configured Ovation Safety Data Server to the C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS file on the AMS Device Manager Station.
- You cannot use a single Server Plus Station for multiple Ovation systems on a network domain because Ovation systems do NOT support network trust relationships.

- If you have FOUNDATION fieldbus devices, we recommended that a licensed Client SC Station be installed on the Ovation Database Server (see *page 79*).
- The Ovation fieldbus engineering software is installed on an Ovation Station that also contains the AMS Device Manager Ovation System Interface.
- One or more Ovation controllers are configured with HART I/O modules. The HART I/O Modules may be on local or remote Ovation I/O.
- If both the Ovation System Interface and the FF HSE System Interface are installed on the same PC, configure each on a unique IP address using separate network interface cards (NIC).

For device support, you can configure AMS Device Manager with an Ovation system as follows:

- For HART devices:
  - If you want to access HART devices on your Ovation system, AMS Device Manager Server Plus Station software and the Ovation System Interface can be installed on any Ovation Station or on a standalone PC.
  - AMS Device Manager supports burst mode messages from HART devices on Ovation Stations using analog output card 5X000167 only. Each Ovation controller uses a unique TCP/IP address. AMS Device Manager communicates with HART devices through I/O modules contained in the Ovation controller chassis, or in remote nodes connected to the Ovation controller.
  - AMS Device Manager can be installed on a remote PC connected to the Ovation system through a LAN, provided the AMS Device Manager PC can communicate with the Ovation Database Server and the controllers through TCP/IP. Set the default gateway in the AMS Device Manager PC to the IP address of the primary network interface card in the Ovation station. See the Ovation documentation for information about communication settings required in the Ovation Station.
- For FOUNDATION fieldbus devices:

- For Ovation 3.5 and later, ensure the Ovation HSE Server is installed, and configure the AMS Device Manager Ovation System Interface with FOUNDATION fieldbus selected on the Ovation Database server. The AMS Device Manager Server Plus Station can be co-deployed on an Ovation Operator Station but not on the Ovation Database Server.
- To receive FOUNDATION fieldbus device alerts in AMS Device Manager, the Ovation OPC Alarm and Event Server package must be installed on your co-deployed Ovation/AMS Device Manager station. The AMS Device Manager Ovation System Interface must also be installed on this station.

Notes

- Some FOUNDATION fieldbus devices have a feature known as “reannunciation” (or “multibit”). This feature must be disabled for devices on an Ovation 3.5 or later system so that AMS Device Manager can receive alerts from these devices. This feature is typically enabled/disabled in the AMS Device Manager device Configure/Setup properties screens (the exact location varies by device).
- When AMS Device Manager is installed with Ovation, the Ovation OPC A&E Server provides access to FOUNDATION fieldbus device alarms. Access to HART device alarms is available by polling the Ovation controller. Ovation OPC A&E Server access is controlled by Ovation user security.

- For *Wireless*HART devices:
  - If you want to access information for *Wireless*HART devices on an Ovation system, configure an Ovation System Interface in AMS Device Manager with *Wireless*HART support enabled and a connection to a Smart Wireless Gateway configured.
- For PROFIBUS DPV1 devices:
  - If you want to access information for PROFIBUS DPV1 devices on an Ovation 3.4 or later system, configure an Ovation System Interface in AMS Device Manager with PROFIBUS DP support enabled.
  - PROFIBUS DPV1 devices will only be supported on Ovation 3.4 or later networks. A PROFIBUS DP module can contain up to 2 ports. Each port can be connected to up to 124 PROFIBUS DPV1 devices.
- For SIS HART devices:
  - If you want to access SIS HART device information on your Ovation system through AMS Device Manager, AMS Device Manager can be configured on an Ovation Station or on a non-Ovation Station. Use the AMS Device Manager Network Configuration utility to set up an Ovation System Interface.
- For non-AMS Device Manager and third-party components - Install the components on an AMS Device Manager station that is not co-deployed with Ovation.

Each Ovation controller uses a unique TCP/IP address. AMS Device Manager communicates with HART devices, *Wireless*HART devices, FOUNDATION fieldbus devices, and devices connected to Ovation Safety Instrumented System (SIS) logic solvers through I/O modules contained in the Ovation controller chassis, or in remote nodes connected to the Ovation controller.

- Supported HART I/O hardware:

  - Analog Input, 5X00058/5X00059, Version 9 or higher
  - Analog Input High Performance, 5X00106/5X00109, Version 6 or higher
  - Analog Output, 5X00062/5X00063, Version 8 or higher
  - Analog Output High Performance, 5X00167, Version 1 or higher
- Supported FOUNDATION fieldbus I/O:
  - Gateway 5X00151G01 and H1 Series 2 Module 5X00152G01, Version 1 or higher
  - Module 5X00301 with cavity insert 1X00458H01 or Module 5X00301 with Personality Module 5X00327, Version 1 or higher (two each of 5X00301 and 5X00327 may also be configured to provide redundancy)
- Supported Intrinsically Safe controller:
  - Ovation SIS Logic Solver, KJ2201X1-PW1, Version 1 or higher
- SIS CHARM I/O
  - CHARMs Safety Logic Solver Version 1.1.2.15
- Supported PROFIBUS DP I/O (Ovation 3.4 and later, with the correct Ovation patch):
  - PROFIBUS module 5X00300/5X00321, Version 1 or higher (two each of 5X00300 and 5X00321 may also be configured to provide redundancy)
- Supported Wireless Gateway (Ovation 3.4 and later) with Smart *Wireless*HART adapter (Ovation 3.4 and later):
  - 1X00693H01 through 1X00693H04

PROFIBUS

The PROFIBUS System Interface lets you use AMS Device Manager to view and configure PROFIBUS DPV1 or PROFIBUS PA devices connected to a Softing PROFIBUS Ethernet Gateway or a Softing PROFIusb Modem.

The PROFIBUS System Interface requires:

- For Ethernet connections, a Softing PBPro ETH, single, dual, or triple channel. The FG-100 and FG-300 are supported as well.
- For modem connections, a Softing PBPro USB, single channel modem. The PROFIusb is supported as well.
- Softing PROFIBUS drivers must be installed on the PC that will use Softing PROFIBUS interface hardware.
- To allow application programs to use the Softing PBPro USB Modem, it must first be configured using Softing's Driver Configuration utility.
- To allow application programs to use the PBPro Gateways, each bus channel must first be configured and scanned using Softing's Driver Configuration utility.
- Ensure that you have installed and configured the Softing device drivers before configuring the PROFIBUS System Interface.
- For connections using the PROFIBUS Ethernet Gateway, only one DNS name or IP address can be configured for each PROFIBUS Network.

PROVOX

A PROVOX system controls field devices linked together by a communication network called a highway. All communicating PROVOX field devices, including the SRx Controller Family products, are connected to this network.

Field devices are grouped into communication highways in the PROVOX Data Highway or PROVOX Highway II. Both systems are multi-drop, half-duplex type. A traffic controller supervises the communication on a PROVOX Data Highway; a token-passing technique controls communication on a PROVOX Highway II.

The PROVOX System Interface requires:

- I/O type (inputs)–CL6822, CL6825, or CL6827
- I/O type (outputs)–CL6826 (will only support standard HART messaging, it will not support AMS ValveLink Diagnostics); CL6828, P3.1 or greater (will support standard HART messaging and AMS ValveLink Diagnostics)
- Controller options–SR90 P5.4 with I/O Driver P5.5 or higher or SRx P5.5 or higher
- System software options–OWP with P1.2 or higher, PROVUE P5.5 or higher, and ENVOX 3.4 or higher; I/O must be configured as “digital” or “hybrid”
- Dedicated HDL with Ethernet connection (TCP/IP) to AMS Device Manager PC

RS3

A Rosemount System 3 (RS3) system controls field devices linked together through Controller cards connected to a PeerWay through ControlFiles. You can have a maximum of 31 PeerWays. A PeerWay can accommodate up to 32 system devices, called nodes, to allow each control system device to communicate through the PeerWay and the RS3 Network Interface (RNI).

The RS3 System Interface requires:

- I/O hardware–FIC 4.8 or higher I/O cards with smart daughterboard and boot revision supplied with P1R1.4 or MAIO FIM with 2.6 or higher
- Controller hardware–MPC II Controller Processor or higher, CP-IV Coordinator Processor or higher
- System software–P1R3.4 or higher with controller image P1.10 or higher
- Dedicated RNI–The RNI needs to be either version 4.1 (NT) or version 5.0 (XP or Server 2003/2008). A single RNI will support multiple AMS Device Manager connections.

Note

AMS Device Manager and RS3 Operator Station (ROS), or DeltaV Operate for RS3 (DOR) cannot be installed on the same PC.

STAHL

A STAHL HART System Interface supports STAHL systems that communicate with HART field devices. AMS Device Manager can read and write device information through existing plant wiring by communicating with multiple devices through the STAHL network. Various STAHL systems can coexist on a single STAHL network.

The STAHL HART System Interface requires:

- RS-232/RS-485 converter for each network (see the *Release Notes* for supported models)
- STAHL ICS Modul–9148 Multiplexer Module installed on a 9161 Module Board with up to 16 HART Transmitter Supply Units (module 9103)
- VOS 200 System, – Central Unit Module 9503, Multiplexer Module 9548
- I.S.1 System–Central Unit Module 9440, Multiplexer Module 9461 (HART analog input) or 9466 (HART analog output)
- IS PAC 9192 HART multiplexer
- Phoenix Contact MACX MXR-S-MUX

Note

You may not be able to use AMS Device Manager to communicate with HART devices through a STAHL IS PAC multiplexer at the same time a handheld communicator is communicating with the device loop. Consult your STAHL representative for details.

The ICS Module is a single HART multiplexer that supports HART transmitter supply units connected to field devices. The I.S.1 System routes messages to their multiplexers with attached HART field devices. For additional information on supported STAHL equipment, see the *Release Notes* and the manufacturer's documentation.

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, 3.9.7, 3.9.8, 3.9.9
- 2.4 GHz Rosemount Rev 3 1420 versions 4.2.9
- 2.4 GHz Rosemount Rev 4 1420 versions 4.3.17, 4.3.19, 4.4.15
- 2.4 GHz Rosemount Rev 4 1410/1420 and Cisco 1552WU version 4.4.30, 4.4.45, 4.4.47-4.4.51
- 2.4 GHz Rosemount Rev 5 1410/1420 and Cisco 1552WU version 4.5.27, 4.5.32, 4.6.59, 4.6.64, 4.7.53

Note

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

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 56*), and then on each PC to be used as a Client SC Station (see *page 58*). 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 68*).

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 71*.

If you are installing AMS Device Manager on an Ovation station, see *page 72*.

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 *KBA NA-0400-0046*.

If you are installing AMS Device Manager on a PC that has AMS Wireless Configurator installed, see *page 54*.

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.

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 3*).

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 14.0 from version 12.0 and higher does not require you to uninstall previous versions and restore the database after installation. See *Table 3-1* on page 52 to upgrade a Server Plus Station or *Table 3-2* on page 53 to upgrade a Client SC Station.

Upgrading to AMS Device Manager 14.0 from version 11.5.7 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 12.0 or higher

Server Plus Station to Server Plus Station	Server Plus Station to Client SC Station
1. Check in all calibration routes. 2. Clear all existing alerts from Alert Monitor. 3. Back up the database (see *page 3*). 4. Consolidate existing databases, if necessary (see *page 61*). 5. Uninstall SNAP-ON applications, 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. 6. Uninstall AMS Device Manager Calibration Connector application, if installed. 7. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing). 8. Remove any configured HART Over PROFIBUS System Interfaces. 9. Stop any programs or processes that access AMS Device Manager Server [1]. 10. Stop AMS Device Manager Server in system tray if running. 11. Install Server Plus Station software (see *page 56*). 12. Get new license codes, if required (see *page 60*). 13. Add or edit users (see *AMS Device Manager Books Online*). 14. Reapply the DeltaV System Interface[3], if applicable. 15. Install required SNAP-ON applications (see *page 69*). 16. Install AMS Device Manager Calibration Connector application, if applicable. 17. Install new Softing TACC components, if applicable[2]. 18. Configure HART Over PROFIBUS System Interfaces, if applicable[2, 4]. 19. Install the latest version of AMS Device Manager Asset Source Interface, and Web Services, if required (see *page 69*). See the Knowledge Base Article on AMS Device Manager ASI for details on installing that product. 20. Copy device manuals (see *page 6*).	1. Check in all calibration routes. 2. Clear all existing alerts from Alert Monitor. 3. Uninstall SNAP-ON applications, 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. 4. Uninstall AMS Device Manager Calibration Connector application, if installed. 5. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing). 6. Remove any configured HART Over PROFIBUS System Interfaces. 7. Stop any programs or processes that access AMS Device Manager Server[1]. 8. Stop AMS Device Manager Server in system tray if running. 9. Uninstall previous AMS Device Manager Server software (see *page 4*). 10. Install Client SC Station software (see *page 58*). 11. Install required SNAP-ON applications (see *page 69*). 12. Add or edit users (see *AMS Device Manager Books Online*). 13. Configure required communication interfaces[4]. 14. Install new Softing TACC components, if applicable[2]. 15. Configure HART Over PROFIBUS System Interfaces, if applicable[2, 4]. 16. Copy device manuals (see *page 6*).

Table 3-2: Upgrade an AMS Device Manager Client SC Station 12.0 or higher

Client SC Station to Server Plus Station	Client SC Station to Client SC Station
1. Check in all calibration routes. 2. Clear all existing alerts from Alert Monitor. 3. Back up the database (see *page 3*). 4. Uninstall SNAP-ON applications and Web Services, if installed. 5. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing). 6. Remove any configured HART Over PROFIBUS System Interfaces. 7. Stop any programs or processes that access AMS Device Manager Server[1]. 8. Stop AMS Device Manager Server in system tray if running. 9. Uninstall previous AMS Device Manager Server software (see *page 4*). 10. Install Server Plus Station software (see *page 56*). 11. Get new license codes, if required (see *page 60*). 12. Add or edit users (see *AMS Device Manager Books Online*). 13. Configure required communication interfaces[3]. 14. Install required SNAP-ON applications (see *page 69*). 15. Install AMS Device Manager Calibration Connector application, if applicable (see *page 74*). 16. Install new Softing TACC components, if applicable[2]. 17. Configure HART Over PROFIBUS System Interfaces, if applicable[2, 4]. 18. Install latest version of Device Description Update Manager, AMS Device Manager Asset Source Interface, and Web Services, if required (see *page 69*). See the Knowledge Base Article on AMS Device Manager ASI for details on installing that product. 19. Copy device manuals (see *page 6*).	1. Uninstall SNAP-ON applications if installed. 2. Clear all existing alerts from Alert Monitor. 3. Uninstall Softing TACC components, if installed (refer to TACC guides downloaded from Softing). 4. Remove any configured HART Over PROFIBUS System Interfaces. 5. Stop any programs or processes that access AMS Device Manager Server [1]. 6. Stop AMS Device Manager Server in system tray if running. 7. Install Client SC Station software (see *page 58*). 8. Add or edit users (see *AMS Device Manager Books Online*). 9. Reapply the DeltaV System Interface, if applicable[3]. 10. Install required SNAP-ON applications (see *page 69*). 11. Install new Softing TACC components, if applicable[2]. 12. Configure HART Over PROFIBUS System Interfaces, if applicable[2, 4]. 13. Copy device manuals (see *page 6*).

Upgrade notes
[1] Processes that must be stopped in Windows Task Manager before upgrading include: • AMSPlantServer • AMSFileServer • AMSConnectionServer • AMSOPC • AMSGenericExports • AMSFFServer • AmsFFAtDeviceBroker • AMSLicenseServer • AmsDeviceAlertServer • AmsHseServer • AMSDevTypeRemote • AMSPBServer [2] If you intend to use the HART Over PROFIBUS System Interface, after upgrading AMS Device Manager Server you must reinstall the Softing TACC components whether or not you install new components. [3]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. [4] Refer to the procedure in *AMS Device Manager Books Online*. Manually installed Device Descriptions that are still not included in the AMS Device Manager 14.0 installation must be reinstalled after the upgrade.

Table 3-3: Upgrade from AMS Device Manager 9.0 to 11.5

Upgrade from version 9.x, 10.x, 11.0, or 11.5
1. Back up the database (see *page 3*). 2. Uninstall SNAP-ON applications and Web Services, if installed. 3. Uninstall AMS Device Manager (see *page 4*). 4. Ensure the PC meets system requirements (see *page 9*). 5. Install AMS Device Manager 14.0 (see *page 56* or *page 58*, depending on the type of installation needed). 6. Install required SNAP-ON applications (see *page 69*). 7. Restore your database (see *page 4*).
Notes
If you are upgrading from a version lower than 9.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 14.0. 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 toolbar and ensure that the station you are monitoring is checked.

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:

1. Contact your Emerson Sales/Service Office to get new license codes for AMS Device Manager.
2. Back up the database (see *page 3*).
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* on page 56 or *Install Client SC Station software* on page 58).
6. Do one of the following:
   - If you installed a Server Plus Station in *Step 5*, license AMS Device Manager (see *page 60*) and restore your backed-up database (see *page 4*).
   - If you installed a Client SC Station in *Step 5*, you may need to consolidate your backed-up AMS Wireless Configurator database with an existing database (see *page 61*).

Upgrade from AMS Device Configurator

AMS Device Configurator 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:

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 60*).
4. Restart your PC.
5. Start AMS Device Manager.

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 14.0. (See *Table 3-1* on page 52). 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 68* for other requirements.

1. Exit/close all Windows programs, including any running in the background (including virus scan software).
2. Insert the AMS Device Manager program DVD 1 in the DVD drive of the PC to be used as the Server Plus Station.
3. When the AMS Device Manager setup starts, click Install AMS Device Manager.

Notes

- If the autorun function is disabled on your PC, double-click D:\AMSDEVICEMANAGER_SETUP.EXE (where D is the DVD drive letter) and click OK.
- Stopping services may take some time to complete.

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* on page 51 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 program DVD 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 you are installing on a Windows 10 or Windows Server 2016 PC without .NET Framework 3.5 Service Pack 1 installed, do the following when the Install .NET Framework 3.5 dialog appears:
    a. Click Yes.
    b. Insert the Windows installation DVD in the DVD drive.
    c. Browse to the root directory of the Windows installation DVD and click Next.
    d. Once .NET Framework 3.5 SP1 installation is complete, replace the Windows installation DVD with the AMS Device Manager program DVD 1 and click OK.
12. 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.
13. License AMS Device Manager (see *page 60*).
14. If you are installing a distributed system, configure the Server Plus Station to recognize each station connected in the system (see *page 60*). This step is essential for the other stations to access the Server Plus Station.
15. Set up and configure the system interfaces needed on this station (see *page 78*).
16. (Optional) Install the latest versions of any licensed SNAP-ON applications (see *page 69*).
17. Open AMS Device Manager, right-click each of the network icons and select Rebuild Hierarchy followed by 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.

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.

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.

Install Client SC Station software

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. Insert the AMS Device Manager program DVD 1 in the DVD drive of the PC to be used as a Client SC Station.
4. When the AMS Device Manager setup starts, click Install AMS Device Manager.

   Notes

   - If the autorun function is disabled on your PC, double-click D:\AMSDEVICEMANAGER_SETUP.EXE (where D is the DVD drive letter) and click OK.
   - Stopping services may take some time to complete.

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 program DVD 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 you are installing on a Windows 10 or Windows Server 2016 PC without .NET Framework 3.5 Service Pack 1 installed, do the following when the Install .NET Framework 3.5 dialog appears:
    a. Click Yes.
    b. Insert the Windows installation DVD in the DVD drive.
    c. Browse to the root directory of the Windows installation DVD and click Next.
    d. Once .NET Framework 3.5 SP1 installation is complete, replace the Windows installation DVD with the AMS Device Manager program DVD 1 and click OK.
12. License AMS Device Manager (see *page 60*).
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. Set up and configure the system interfaces needed on this station (see *page 78*).
15. (Optional) Install the latest versions of any licensed SNAP-ON applications (see *page 69*).
16. Open AMS Device Manager, right-click each locally configured network icon and select Rebuild Hierarchy and then Scan > New Devices.
17. 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.

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.

Note

To gather the registration information, you need to know your Customer Access Code (supplied with your AMS Device Manager software).

After you register your software, the Registration Center returns your license codes and checksums by downloading from the AMS Device Manager registration website at:

http://www.emersonprocess.com/systems/support/ams_register/10.c.survey.login.asp

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

Notes

- 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 verify the hard disk serial number.
- License codes are assigned to the hard disk serial number of the C:\ boot partition.

1. Enter Licensing Wizard on the Start screen and click Licensing Wizard.
2. Follow the instructions in the Licensing Wizard.
3. If you are installing new license information on an existing station, start AMS Device Manager to see the changes.

Configure 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.

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 62*), 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 each Client SC station for all stations to recognize each other.

Consolidate databases

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

1. Back up the current database on all stations containing a database you want to consolidate (see *page 3*).
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 14.0 Server Plus Station can be installed using one of the following methods:

   - Install AMS Device Manager 14.0 as a station upgrade, if upgrading from version 12.5 or later which automatically migrates the consolidated database (see *page 51*).
   - Uninstall the 9.0-11.5 station software and install AMS Device Manager 14.0 as a new Server Plus Station (see *page 56*). Restore the consolidated database (see *page 4*).

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 DVD 2.

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 60*). 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 My Computer 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 in a distributed system. 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		

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 63*. For other types of changes, see the following:

Change station types

If you are changing station types, perform the following appropriate procedures. You may also need to reset your users' permissions (*page 77*).

Change a Server Plus Station to a Client SC Station

1. Back up the database (see *page 3*).
2. Uninstall the previous Server Plus Station software (see *page 4*).
3. Ensure that a connection can be made to an available Server Plus Station.
4. Install the Client SC Station software (see *page 58*).
5. Restore or combine the database on another Server Plus Station (see *page 4*).

Change a Client SC Station to a Server Plus Station

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 4*).
3. Install the Server Plus Station software (see *page 56*).
4. License AMS Device Manager (see *page 60*).

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

1. In Network Configuration on the Client SC Station, remove any configured system interfaces (other than HART Modem).
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 or Ovation workstations. In these configurations, use the procedure below.

1. Uninstall AMS Device Manager on the Client SC Station (see *page 4*).
2. Reinstall AMS Device Manager on the Client SC Station and indicate the new Server Plus Station (see *page 58*).

Add Client SC Stations

To expand an existing distributed system:

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 60*) and then continue with step 2.
2. To install AMS Device Manager on the added Client SC Stations, see *page 58*.
3. Update the Client SC Station configuration on the Server Plus Station (see *page 60*).
4. To enable the stations in the distributed system to recognize the added Client SC Station, shut down and restart AMS Device Manager on all the stations.

Replace a Server Plus Station PC

1. Contact your Emerson Sales/Service Office to get new license codes for AMS Device Manager.
2. Back up the database (see *page 3*).
3. Uninstall AMS Device Manager from the old PC (see *page 4*). 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 Viewer 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 63*).

5. Install Server Plus Station software on the new PC (see *page 56*).
6. License AMS Device Manager (see *page 60*).

7. Set up the server configuration to recognize each Client SC Station connected in the system (see *Configure a Distributed System* on page 60).
8. Restore the database (see *page 4*).

Replace a Client SC Station PC

1. Uninstall AMS Device Manager from the old PC (see *page 4*). 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 62*), 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 58*).

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.

1. Back up the database (see *page 3*).
2. Record all devices contained in the Device Monitor List.
3. Uninstall AMS Device Manager on the Server Plus Station (see *page 4*).
4. Rename the Server Plus Station PC:
   a. Right-click the Windows desktop My Computer icon.
   b. Select Properties.
   c. Click Change Settings (Windows 7 only).
   d. On the Computer Name tab, click Change.
   e. Enter a new computer name and click OK.
   f. Click OK.
5. Install AMS Device Manager on the Server Plus Station (see *page 56*).
6. Restore the database backed up in step 1 (see *page 4*).
7. Reinstall the required system interfaces (see *page 78*) and SNAP-ON applications (see *page 69*).
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*).

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.

1. Record all devices contained in the Device Monitor List.
2. Uninstall AMS Device Manager on the Client SC Station PC (see *page 4*).
3. Rename the Client SC Station PC:
   a. Right-click the Windows desktop My Computer icon.
   b. Select Properties.
   c. Click Change Settings (Windows 7 only).
   d. On the Computer Name tab, click Change.
   e. Enter a new computer name and click OK.
   f. 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 60*).
5. Install AMS Device Manager on the Client SC Station PC (see *page 58*).
6. Reinstall the required system interfaces (see *page 78*) and SNAP-ON applications (see *page 69*).
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*).

Add a new communication interface

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 60*).
3. Configure the new communication interface (see *AMS Device Manager Books Online*).

Add more tags than currently licensed

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 60*).
3. Start AMS Device Manager.

4. Install and configure the additional devices.

Installing AMS Device Manager on domain controllers

AMS Device Manager creates a Windows user account (AmsServiceUser) on each station in a distributed system. When AMS Device Manager is installed on a domain controller, this account is created as a domain user. 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.
- 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

- If AMS Device Manager is installed on the domain controller OR if there is an AmsServiceUser account on the Domain Controller\Active Directory, there can only be one AMS Device Manager system installed on that domain.
- If AMS Device Manager is NOT installed on the domain controller AND if there is NO AmsServiceUser account on the Domain Controller\Active Directory, multiple systems can be installed on that domain.
- 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.

Domain controller security requirements

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

Add a user to the AMSDeviceManager group on a domain controller

Note

The following procedure requires network administrator permissions.

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.

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.

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.

1. Insert the AMS Device Manager DVD 2 in the DVD drive of the PC.
2. Browse to D:\SNAP-ONS And Tools\SNAP-ONS\Installs\<*Folder Name*> (where D is the DVD drive letter and <*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. Calibration Assistant is enabled through licensing–no separate installation is required.
- For all SNAP-ON applications except AMS ValveLink and AMS Wireless, users must also have Device Write permission (see *AMS Device Manager Books Online*).
- AMS 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.

Install AMS Device Manager Web Services on a station

1. Review the AMS Device Manager Web Services software requirements (see *page 19*).
2. Ensure that appropriate Windows Firewall security settings have been selected (see *page 77*).

3. Exit/close all Windows programs, including any running in the background (including antivirus software).
4. Insert the AMS Device Manager DVD2 in the DVD drive of the PC.
5. Browse to D:\SNAP-ONS And Tools\AMSWebServices (where D is the DVD drive letter).
6. Double-click SETUP.EXE.
7. Follow the prompts.

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 17*), 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.

Licensing AMS Device Manager 14.0 on DeltaV stations

If you have licensed your AMS Device Manager 14.0 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.

When you install AMS Device Manager on a DeltaV Simulate Multi-node system, the installation program checks for the presence of a DeltaV Simulate ID key (VX dongle). If the Simulate ID key is found, AMS Device Manager licensing is enabled. Otherwise, the installation program looks for an AMS Device Manager license.dat file. If the license.dat file is found, you are granted the permissions associated with the license. If no license.dat file is found, a subset of AMS Device Manager functionality is available.

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 71*.

Installing AMS Device Manager 14.0 on DeltaV stations

AMS Device Manager 14.0 can be co-deployed only on DeltaV 12.3 or later 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 12.3 or later 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 68*.

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 70*). In addition, ensure that USB has been enabled in DeltaV Easy Security (see your DeltaV documentation for more information).

To install Server Plus Station software on a supported DeltaV station, see *page 56*. To install Client SC Station software on a supported DeltaV station, see *page 58*.

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.

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.

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.

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.

Licensing AMS Device Manager 14.0 on Ovation stations

When you install AMS Device Manager on an Ovation station, the installation program checks for the presence of an AMS Device Manager license.dat file. If the license.dat file is found, you are granted all the permissions associated with the license. If you do not have a license.dat file, see *page 60*. After you have received the appropriate licensing information, install AMS Device Manager as described on *page 72*.

Installing AMS Device Manager 14.0 on Ovation stations

AMS Device Manager 14.0 can be installed on Ovation 3.5.1 and later stations as outlined on *page 42*. AMS Device Manager stations can also be installed on separate PCs and access Ovation information through the Ovation System Interface. To ensure a properly co-deployed installation, Ovation must be installed before AMS Device Manager.

In a typical Ovation 3.5.1 deployment using FOUNDATION fieldbus devices, the AMS Device Manager Client SC Station software would be installed on the Ovation Database Server. Other AMS Device Manager Client SC Station and the Server Plus Station software would be installed on Ovation Operator stations in the network. This deployment gives all connected stations access to both AMS Device Manager and Ovation databases.

Before you install AMS Device Manager on your Ovation stations, ensure that you have all the proper AMS Device Manager and Ovation licensing and installation instructions (see *page 72*).

To install Server Plus Station software on a supported Ovation station, see *page 56*. To install Client SC Station software on a supported Ovation station, see *page 58*.

Configure the Ovation System Interface (see *AMS Device Manager Books Online*) so that AMS Device Manager can detect and work with devices on the Ovation network.

Configure any other required communication interfaces (see *page 78*).

Notes

- If you are installing AMS Device Manager on any domain controller stations, see *page 68*.
- Do not configure an Ovation System Interface for the same Ovation system on more than one AMS Device Manager station.
- If you install a Client SC Station on an Ovation station running on a Windows Server PC, add the Client SC Station PC name to the DNS forward lookup zones list. Contact your IT department for assistance.

Uninstalling Ovation software

To uninstall Ovation on a station that has AMS Device Manager co-deployed, you must uninstall AMS Device Manager first and then Ovation. You can then reinstall AMS Device Manager. If you uninstall Ovation 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 Ovation only after AMS Device Manager has been uninstalled on all PCs.

Miscellaneous applications

AMS Device View

AMS Device View extends your AMS Device Manager system by delivering device health, calibration, and project status information through a browser. With AMS Device View, you can quickly see which devices need maintenance and you can view recommended actions - from any place with a browser connection.

To install AMS Device View, the following requirements must be met:

- The PC must be running a supported operating system (see *page 17*).
- IIS must be installed on the PC before installing AMS Device View.
- You must have Windows system administrator rights to install AMS Device View.

The *AMS Device View Installation Guide* is available in the AMS Device View\Install_Files\PDF Documentation folder on AMS Device Manager DVD 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*.

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 AMS Device Manager DVD 1.

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 14.0, 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.

AMS Device Manager Calibration Connector

AMS Device Manager Calibration Connector is a separately licensed and installed application that integrates with Beamex CMX or Meridium APM Framework software 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:

- AMS Suite APM version 3.5.1 or later
- Beamex CMX version 2.74 and 2.81

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

1. Insert the AMS Device Manager Calibration Connector DVD in the DVD drive of your PC.
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*, *AMS Suite Calibration Connector and AMS Suite APM Installation and Setup* document, and *AMS Suite Calibration Connector and Beamex CMX Installation and Setup* document. Also, refer to your AMS Suite APM or Beamex CMX documentation for more information on these products.

Note

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

Device Description Update Manager

The Device Description Update Manager automates the installation of device descriptions from Guardian Support into AMS Device Manager, DeltaV, and Ovation through the Add Device Type utility. These device descriptions can be new or updates to previously installed devices. The Device Description Update Manager provides 2 ways to install device descriptions:

- Scheduled/fully automated
- User-initiated/interactive

There are 3 ways that this feature can be installed:

- Server Station
- Client Station
- Server/Client Station

The Server Station can be installed with or without an AMS Device Manager station already installed but it must be installed on the same PC as the Guardian Software Update Delivery Service download folder.

The Client Station must be installed on an AMS Device Manager 14.0 Server Plus Station that can access the Server Station to initiate installation of device descriptions. The Client Station will be supported on an AMS Device Manager Server Plus Station co-deployed on either a DeltaV workstation or an Ovation workstation.

In a Server/Client Station installation, both the Server Station and Client Station are installed on the same Server Plus Station.

See *KBA NK-1300-0136 Device Description Update Manager Architectures and Information* for more information.

Install Device Description Update Manager

1. Insert the AMS Device Manager DVD 2 in the DVD drive of your PC.
2. In the Device Description Update Manager folder, double-click DDUMInstall_Setup.exe.
3. Follow the prompts on the installation window.
4. Click Finish when done.

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 is installed automatically with an AMS Device Manager Server Plus Station. It requires Advanced Services SQL add-on (which is included in the AMS Device Manager SQL 2014 Express edition on the media).

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.

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 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 as described, AMS Device Manager will not function as expected.

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 more information, refer to *KBA NA-0500-0085*. For assistance configuring your Windows Firewall, contact your IT department.

Notes

- On a Windows 7 PC, all entered firewall exceptions display as "AMS Suite: Intelligent Device Manager" in the firewall exceptions list. You must view the properties of each entry to see what was added.
- For deployment scenarios that require AMS Device Manager Client SC Stations to cross External Firewalls, refer to *KBA NA-0400-0046*.
- If AMS Device Manager is co-deployed with DeltaV 13.3, 13.3.1, or 14.3, enable Windows Firewall and open a specific port using the DeltaV Security Administration Application (refer to *DeltaV Books Online* for more information).

Usernames and passwords

Note

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

AMS Device Manager security is based on Windows user authentication. Each user is given an AMS Device Manager username and password associated with a Windows local (workgroup) or domain account.

User permissions are set up and maintained in User Manager. 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.

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.

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 22*) 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.

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 27*.

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 AMS 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.

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.

FF HSE

Your AMS Device Manager distributed system can be configured to access FF HSE linking devices in a dedicated network environment.

This configuration is recommended and requires a dedicated network interface card (NIC) for connecting to the FF HSE linking devices. This arrangement provides best performance because the FF HSE linking devices are not required to share the network with other network traffic. In this case, you manually assign the TCP/IP address of the linking device.

The alternative is to configure your AMS Device Manager distributed system to access FF HSE linking devices from an Ethernet network that assigns TCP/IP addresses using DHCP.

Note

If you assign a static TCP/IP address to a linking device, a valid gateway address must also be provided. The gateway address is usually the TCP/IP address of the dedicated NIC. If the gateway address is invalid, you will see a delay in AMS Device Manager when rebuilding the hierarchy. In addition, no links or FOUNDATION fieldbus devices will be displayed after performing the Rebuild Hierarchy operation.

Ovation

The Ovation System Interface lets AMS Device Manager communicate with HART, FOUNDATION fieldbus, PROFIBUS DPV1, and *Wireless*HART devices through an existing Ovation network.

Prepare the Ovation system

Refer to your Ovation documentation for device connection and network setup instructions.

For Ovation 3.4, the AMS Device Manager Server Plus Station must be co-deployed on an Ovation Station with the Ovation fieldbus engineering software installed for FOUNDATION fieldbus device support. Configure the Ovation System Interface on this station.

For Ovation 3.5, the fieldbus engineering software is located on the Ovation Database Server. Therefore, it is recommended to install AMS Device Manager Client SC Station software on this station type. To install and register this software on an Ovation Operator station type, you must run an Ovation batch file on the Ovation Operator station.

Run the batch file on the Ovation Operator station

1. Enter CMD on the Start screen.
2. At the command prompt, enter CD C:\OVATION\OVATIONBASE.
3. Press ENTER.
4. At the command prompt, enter INSTALLHSESERVER -I.
5. Press ENTER.

PROVOX

A PROVOX system controls field devices linked together by a communication network called a highway. All communicating PROVOX field devices, including the SRx Controller Family products, are connected to this network.

Field devices are grouped into communication highways in the PROVOX Data Highway or PROVOX Highway II. Both systems are multi-drop, half-duplex type. A traffic controller supervises the communication on a PROVOX Data Highway; a token-passing technique controls communication on a PROVOX Highway II.

Prepare the PROVOX system

To prepare a PROVOX control system to communicate with AMS Device Manager, you need to:

- Know the TCP/IP address and DNS name of your dedicated HDL (Highway Data Link). If you do not know these, see your system administrator.
- Generate and transfer the PROVOX hierarchy information to AMS Device Manager (see *page 80*).
- Verify that the HDL responds (see *page 81*).

Generate and transfer the HLT file

The PROVOX system uses the HART Instrument Locator Tool (HILT) to create a comma-delimited value (CDV) file that defines the addresses of field devices connected to the SRx/SR90 controller. The file name can be anything that is meaningful, as long as it uses an “hlt” extension (such as Provox1.hlt). After you create the HLT file, transfer it to the AMS folder on the AMS Device Manager PC and identify the HLT file in the Connection tab of Network Configuration Properties (see *AMS Device Manager Books Online*).

AMS Device Manager reads the HLT file and attempts to communicate with devices at every defined address, which can cause unpredictable results if the file is built using “all devices” as the default setting. The HLT file should hold only the device addresses that are relevant to AMS Device Manager.

Note

For AMS Device Manager to recognize the change when you add or delete a device in PROVOX, you must regenerate the HLT file on the ENVOX PC and transfer it to the AMS folder on the AMS Device Manager PC, replacing the old HLT file.

To provide AMS Device Manager with the PROVOX HLT file information:

1. At the ENVOX PC, generate the HLT file by running the HART Instrument Locator Tool (HILT) utility.

   For information about using the HILT utility, see *Using the HART Instrument Locator Tool (HILT) Version P3.0 (Readhilt.rtf)*. This RTF file is located in the HILT folder on the AMS Device Manager DVD 2.
2. Copy the HLT file from the ENVOX PC to the AMS folder on your AMS Device Manager PC, using file transfer protocol (FTP).

Verify HDL response

Use the ping command to verify that the HDL responds to communications sent to it by AMS Device Manager:

1. Enter CMD on the Start screen.
2. At the command prompt, enter PING <HDL DNS Name>.

   If your network does not support DNS, replace the DNS name with the IP address of your HDL in the ping command.
3. Press ENTER.
4. Verify that the HDL responds to the ping command.

   The ping command should return a reply message. If the ping command fails, verify that you entered the correct address in the command line. Also verify that your network is functioning properly.

Installation is complete only after you receive a valid ping reply.

RS3

A Rosemount System 3 (RS3) system controls field devices linked together through Controller cards connected to a PeerWay through ControlFiles. A PeerWay can accommodate up to 32 system devices, called nodes, to allow each control system device to communicate through the PeerWay and the RS3 Network Interface (RNI).

Prepare the RS3 system

To prepare an RS3 control system to communicate with AMS Device Manager, you must:

- Know the TCP/IP address and DNS name of your RNI. If you do not know these, see your system administrator.

- Set up a username and password for the system interface on your RNI (see *page 82*).
- Verify that the RNI responds (see *page 82*).

Set RNI username and password

1. On your RNI, open the RNI user configuration file, \\RNIBOOT\CONFIG\USERFILE.CFG. You can open it with the Notepad utility, or any other text editor.
2. Create a user account for AMS Device Manager, ensuring that FMSPassthrough is enabled and that KeyLevel is set to Console.

   Example: The following example shows the system interface user entry in the USERFILE.CFG file. The user entry in bold is an example of an RS3 user entry. You can create the system interface user entry by copying and pasting an existing user entry in USERFILE.CFG and editing the entry for system interface.

```
<User
<Name RS3OpStation>
<Password RS3Performance>
<KeyLevel CONSOLE>
<Attributes
<ReadUsers ON>
<SendAlarms ON>
<FMSPassthrough ON>
<RemoteBoot ON>
>
<User
<Name AMS>
<Password Passthrough>
<KeyLevel CONSOLE>
<Attributes
<ReadUsers ON>
<SendAlarms ON>
<FMSPassthrough ON>
<RemoteBoot ON>
>
```

   Notes

   - The username and password are case-sensitive in the USERFILE.CFG file. When entering them in the AMS Device Manager Network Configuration utility, be sure to match the case.
   - AMS ValveLink SNAP-ON application is not supported.

3. Save and close USERFILE.CFG.

Verify communication with RNI

Use the ping command to verify that the RNI is responding:

1. Enter CMD on the Start screen.

2. At the command prompt, enter PING <RNI DNS Name>. (If your network does not support DNS, replace the DNS name with the IP address of your RNI in the ping command.)
3. Press ENTER.
4. Verify that the RNI responds to the ping command.

   The ping command should return a reply message. If the ping command fails, verify that you entered the correct address in the command line. Also verify that your network is functioning properly.

Installation is complete only after you receive a valid ping reply.

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*.

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*.

Error messages

Error message / Indication	Possible Cause	Possible solution
Bluetooth adapter stops working.		If an approved USB Bluetooth adapter is removed or disabled while AMS Device Manager is running, reinsert the adapter and reboot your workstation. After your PC restarts, try to re-establish Bluetooth communications with your Field Communicator.
The SQL Server installation fails.		Manually install SQL Server 2014 Express Service Pack 2 from the AMS Device Manager DVD. Run Install_SQL2014Express64bit.bat from the Install_Files\SQL2014SP2Exp\64 folder. If you do not have Service Pack 2 installed, run Install_SQL2014SP2Express64bit.bat.The SQL Server manual installation process requires user input that you must provide. After you install SQL Server, restart the AMS Device Manager installation process. See KBA NK-1800-0002 for details.

Error message / Indication	Possible Cause	Possible solution
AMS Device Manager Install has encountered an error trying to login to the SQL Server database. Please refer to the Installation Guide for SQL Server database configuration. Setup will now abort.	This occurs on a domain-based AMS Device Manager system where a different administrator installed SQL Server and another administrator is installing the Server Plus Station.	Open SQL Server Management Studio and add the user who is installing the Server Plus Station. See KBA NK-1800-0002 for details.
AMS Device Manager has detected an incorrect version of the database. 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: 1. Open the AMS\Bin folder. 2. Double-click AmsConvertDb.exe. 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* on page 77.
Unable to connect to live device.		Add AmsFFServer.exe to the exception list. See *Change Windows Firewall settings* on page 77.
Unable to launch the AMS Device Manager application from the Client SC Station.		Open port 135. See *Change Windows Firewall settings* on page 77.
“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* on page 77.
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* on page 77.

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: Unable to retrieve the current configuration information for server, <PC name>. Error calling GetServersAsXml.		Add AMSServicesHoster.exe to the exception list. See *Change Windows Firewall settings* on page 77.

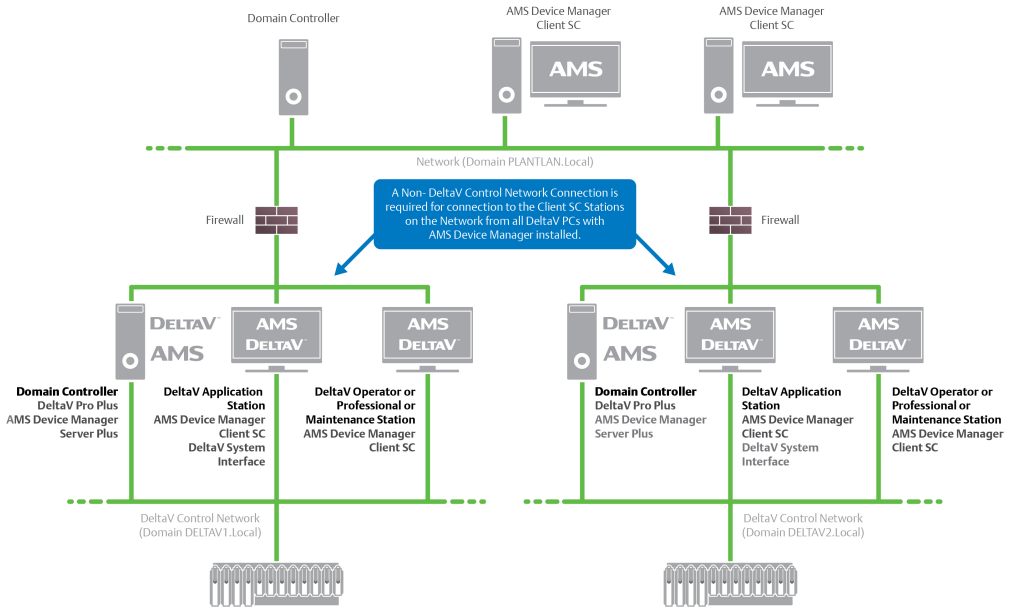
Appendix A
DeltaV system interface deployment concepts

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:

- Each Client SC Station must have a network connection to the Server Plus Station. The Client SC Station must have access to the database.
- Each AMS Device Manager station must have a network connection to the AMS Device Manager station where the DeltaV System Interface is configured in order to have online access to the devices.
- For any architecture where an AMS Device Manager station in one domain must communicate with an AMS Device Manager station in a different domain, the Cross Domain requirements in *KBA NA-0800-0113* apply.

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. DeltaV can be versions 12.3, 12.3.1, 13.3, 13.3.1, or 14.3.*
- *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.*

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.

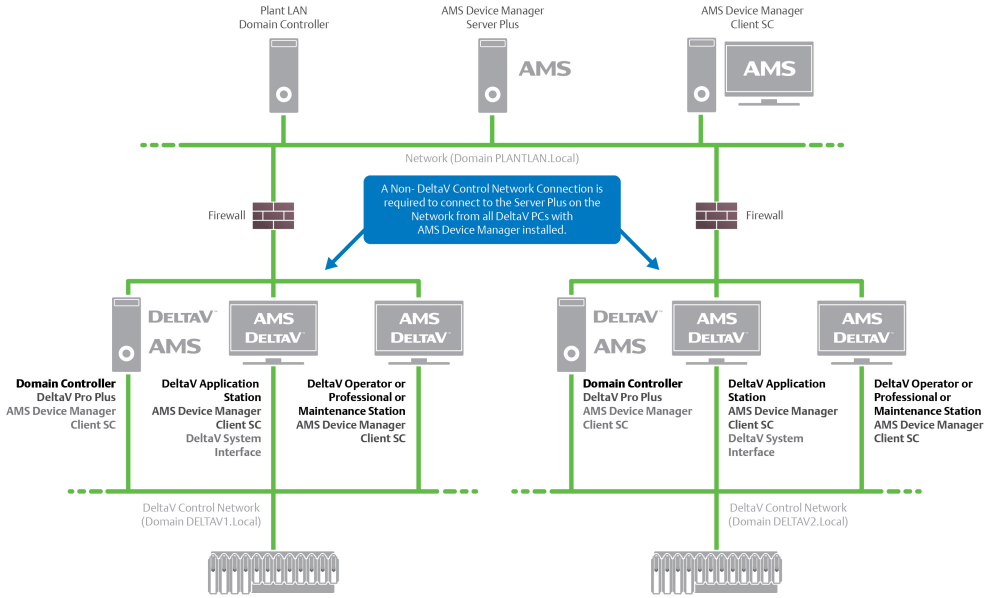
General Deployment Information

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.

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).

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. DeltaV can be versions 12.3, 12.3.1, 13.3, 13.3.1, or 14.3.*
- *Each DeltaV network is treated as a separate network and therefore the Cross Domain requirements in KBA NA-0800-0113 might apply.*
- *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.*

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. Devices from each Zone can be connected to an AMS Device Manager station and then made available to other AMS Device Manager stations from different Zones for access.

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.

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.

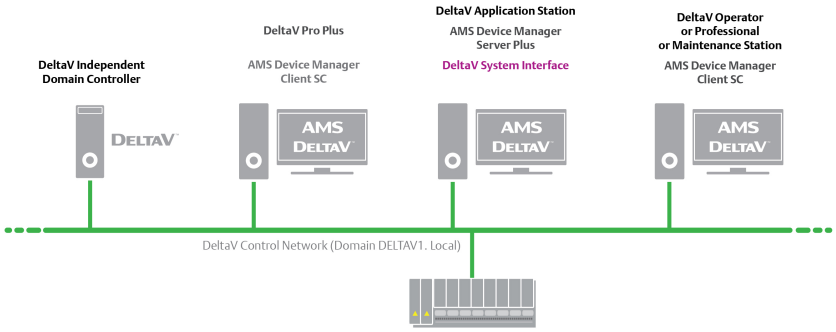
Security

- 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).

AMS Device Manager with DeltaV Control Networks-Independent Domain Controller



Primary Use

- This architecture is for a customer installation when the DeltaV system is set up with an Independent Domain Controller.
- This deployment is available with DeltaV 14.3 or greater systems.
- The version of AMS Device Manager must be compatible with the DeltaV version for this deployment (i.e. DeltaV 14.3 and AMS Device Manager 14.0).

Network Domain Deployment

- The IDDC is also supported with the Multiple Domain Networks and Single distributed system DeltaV deployments.
- 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.

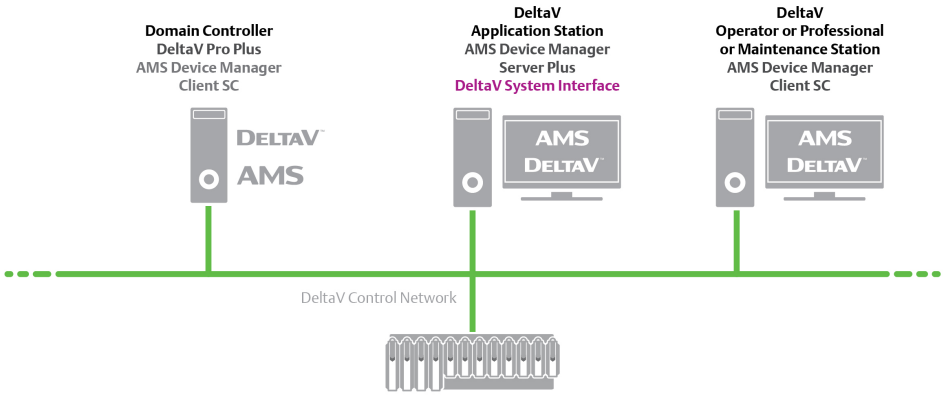
Security

- 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).

AMS Device Configurator supported on DeltaV Control Network



Note

When installed as AMS Device Configurator with DeltaV, an AMS Device Manager license is NOT required.

Primary Use

This architecture is for an installation when an AMS Device Manager license has not been purchased. This deployment is standard with all DeltaV 11.3 or greater systems. The version of AMS Device Manager must be compatible with the DeltaV version for this deployment (for example, AMS Device Manager 14.0 and DeltaV 14.3).

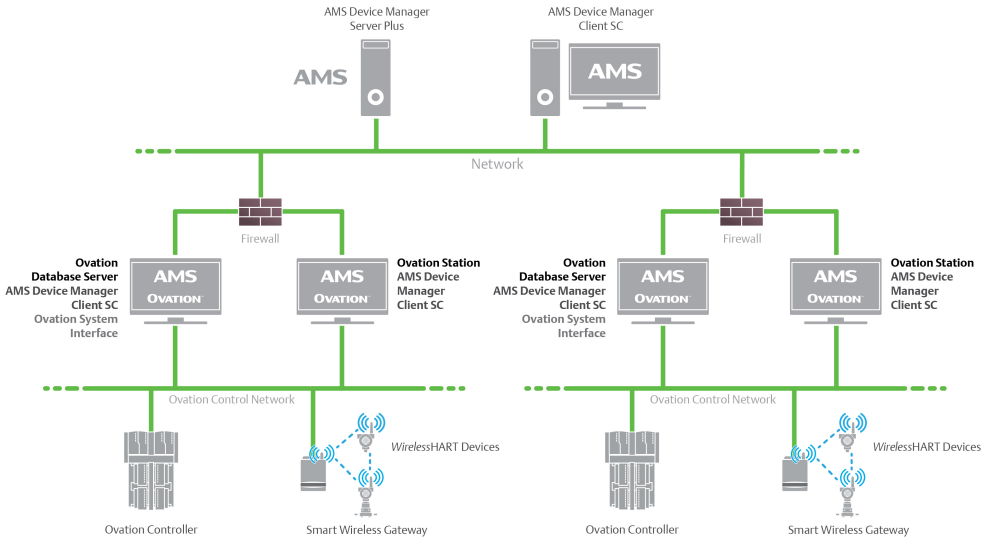
Security

- If an AMS Device Manager license file is not found, the AMS Device Configurator application is automatically installed.
- If you are using a DeltaV database user account that is not a Windows user account, you need to upgrade AMS Device Configurator to AMS Device Manager with an AMS Device Manager license.
- Purchase of an AMS Device Manager license, enables support for the other DeltaV deployments shown in this document.

Appendix B
Ovation system interface deployment concepts

AMS Device Manager on the Ovation Control Network

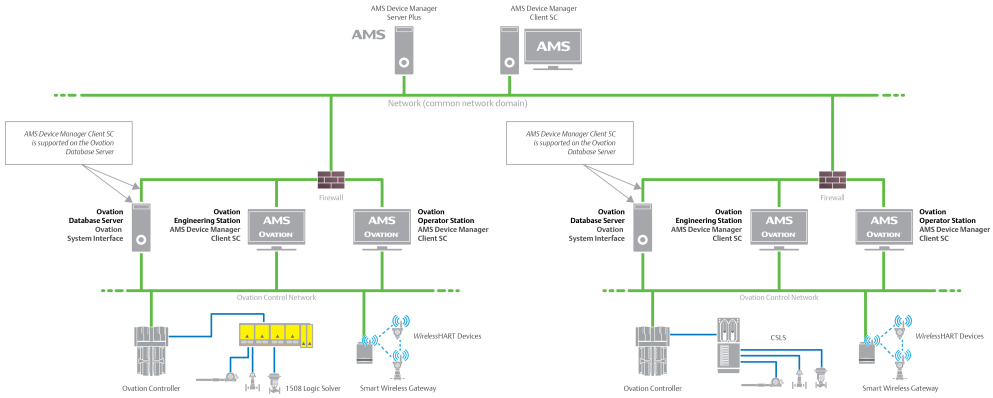
This deployment is only supported in a Workgroup environment.



Notes

- *All AMS Device Manager installations must be at the same version.*
- *The Ovation System Interface must be configured on an AMS Device Manager Client SC installed on the Ovation Station.*
- *The Ovation fieldbus engineering software must be installed for FOUNDATION fieldbus support.*
- *This deployment supports HART, PROFIBUS DPV1, and FOUNDATION Fieldbus devices.*

AMS Device Manager on multiple Ovation systems



Notes

- *All AMS Device Manager installations must be at the same version.*
- *The Ovation fieldbus engineering software must be installed for FOUNDATION fieldbus support.*
- *This deployment supports HART, PROFIBUS DPV1, and FOUNDATION fieldbus devices.*
- *Deploying the AMS Device Manager software across multiple domains (cross domains) is NOT supported. The Ovation system does not support Trust relationships.*

Appendix C
Other deployment concepts

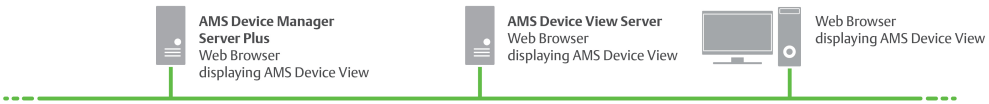
AMS Device View

AMS Device View consists of two components, the AMS Device View server, and a web browser which accesses it. AMS Device View can be deployed on an AMS Device Manager system following these requirements:

- Only one AMS Device Manager database is allowed.
- 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.

Deployed on AMS Device Manager Server Plus Station

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

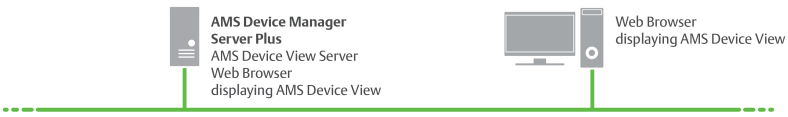


Deployed on a non-AMS Device Manager PC

Note

Emerson does not recommend installing AMS Device View on a domain controller unless DeltaV or Ovation are also on the same server.

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



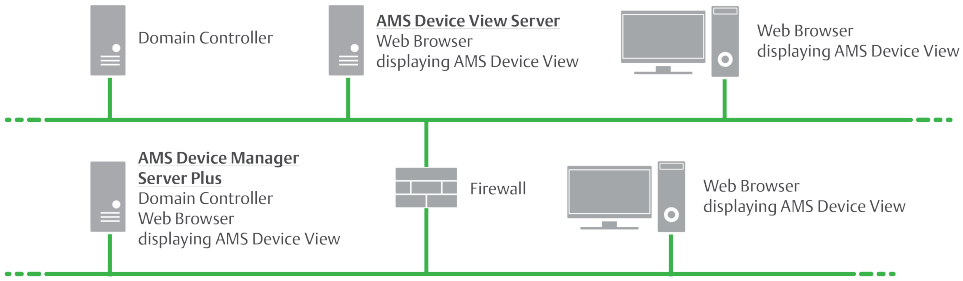
- A mix of domains and workgroups is not supported. The AMS Device Manager Server Plus and AMS Device View server must be both on a domain, or both on a workgroup.
- The following restrictions apply when the Windows login to AMS Device View is a local user account (and not a domain account)

- 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.
- The user accounts logging into AMS Device View must be added to the AMSDeviceManager Windows group on the AMS Device View server (if this PC has the AMS Device Manager Client SC already installed, this is done automatically)
- 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

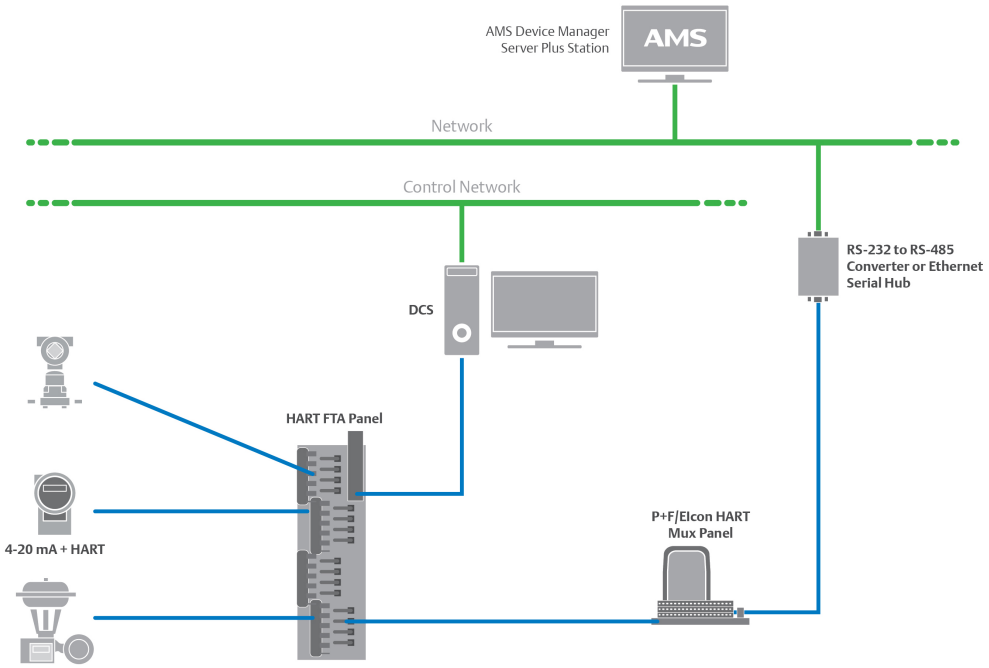
Note

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



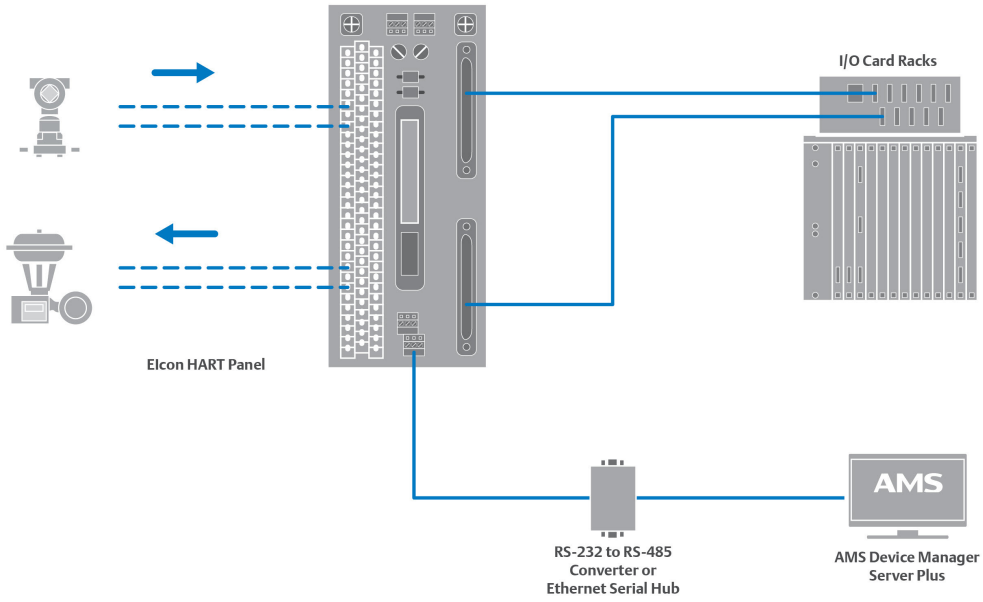
HART Interface Solution – External Interfaces



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.*

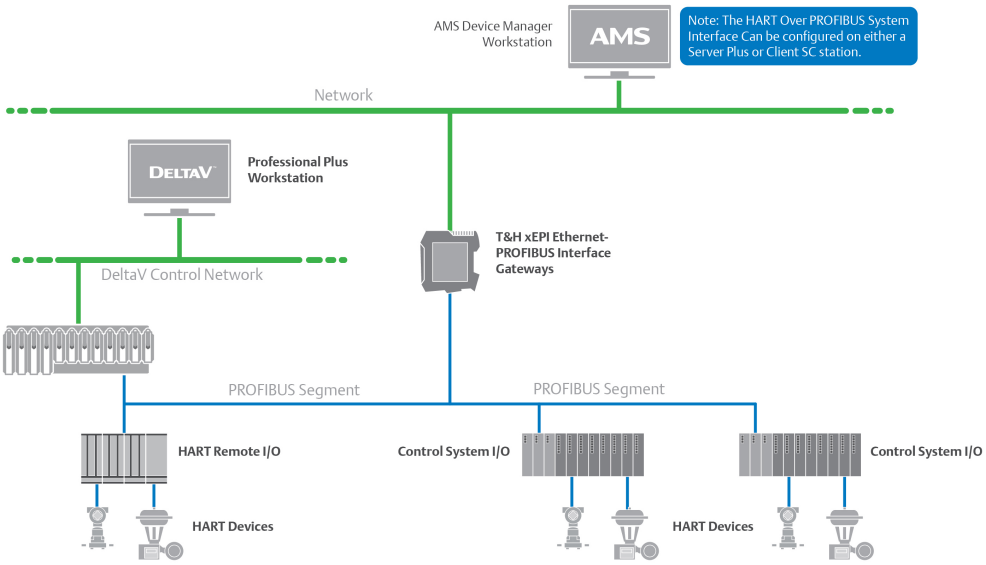
HART Custom Solution – Integrated HART Panel Incorporating Multiplexer and Field Termination Panel (FTP)



Notes

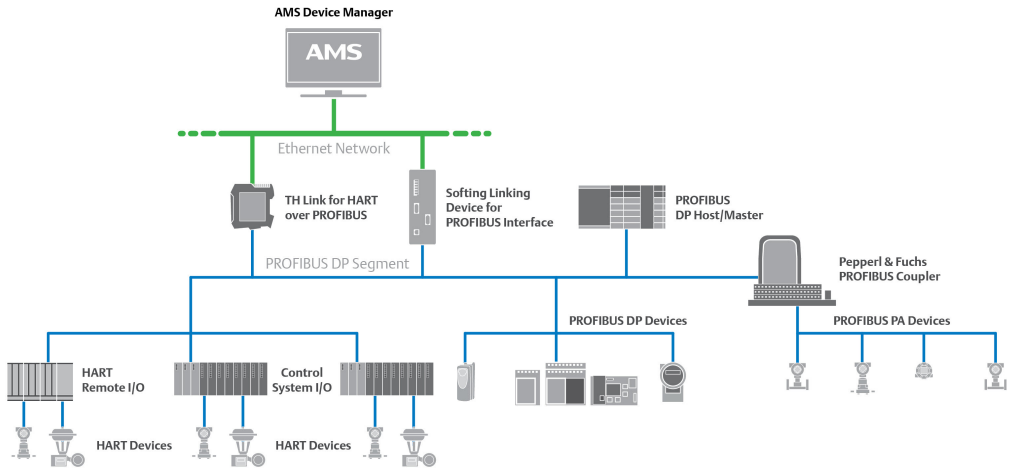
- *This deployment is typically used on new installations or upgrades where the digital control system is purchased with a P+F/Elcon panel.*
- *This deployment can be used to replace existing term panels to add multiplexers to an existing system.*
- *This deployment provides AMS Device Manager access 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.*

HART Over PROFIBUS

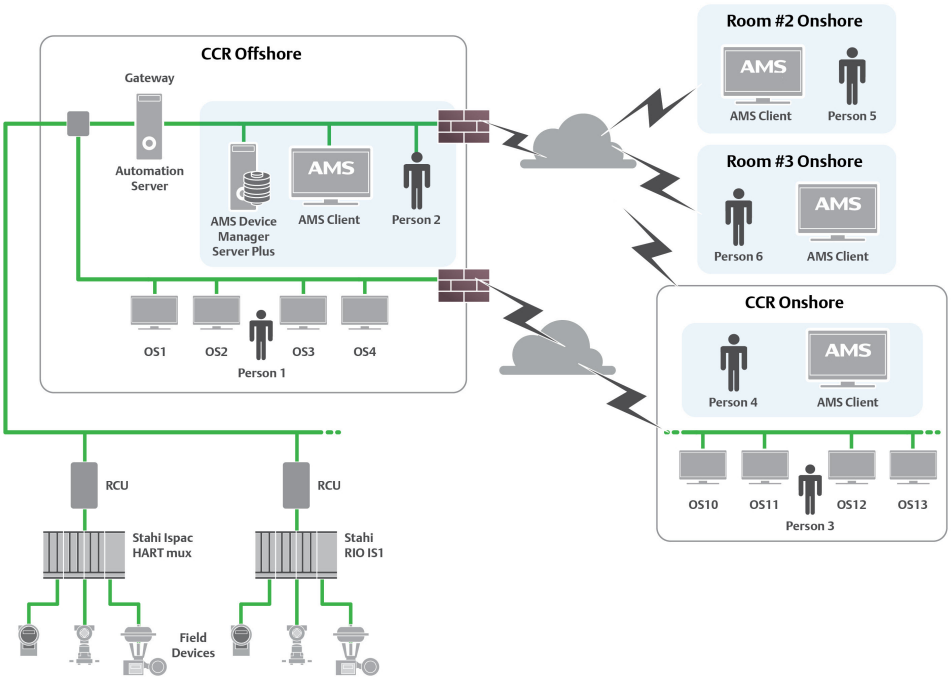


The documentation specific to the PROFIBUS remote I/O subsystem has device connection and network setup instructions.

HART Over PROFIBUS plus PROFIBUS Interface

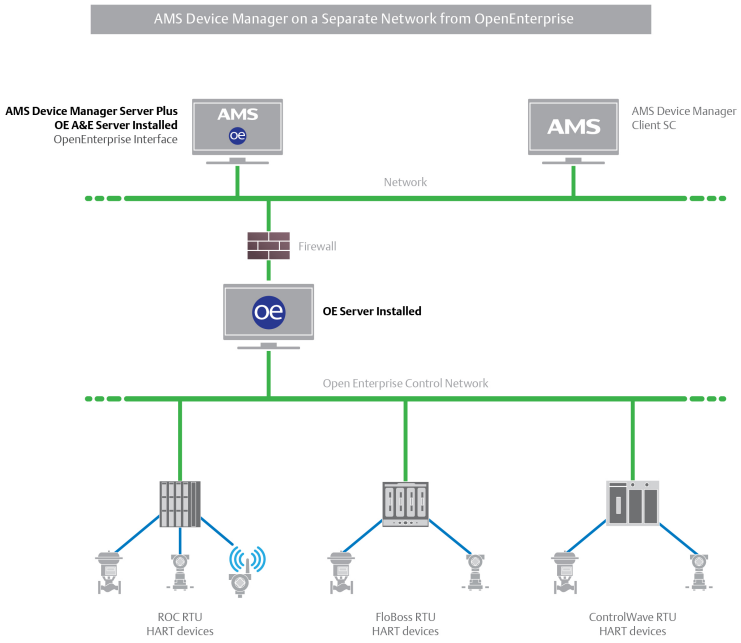


Kongsberg



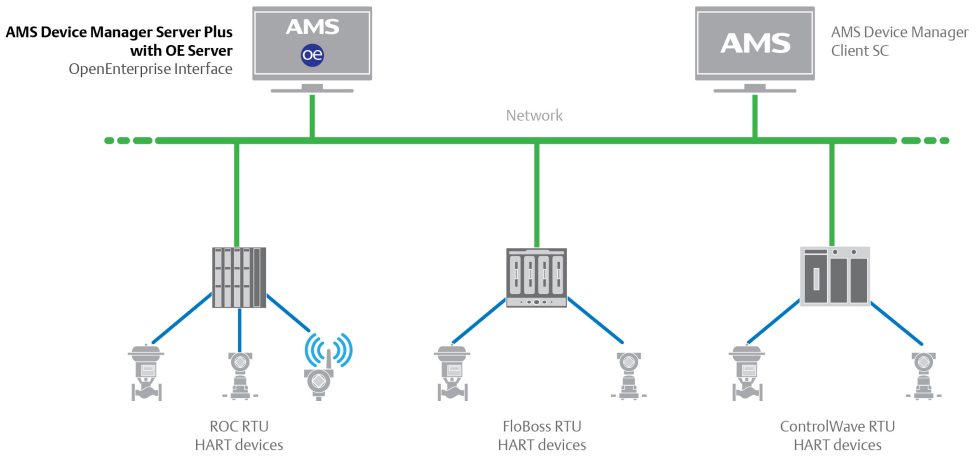
In this diagram, the AMS Device Manager Server Plus Station is installed at an offshore facility, which is connected through a LAN to onshore AMS Device Manager Client SC Stations. The onshore stations can access live HART devices using SNAP-ON applications such as the AMS ValveLink SNAP-ON. Between the onshore and offshore stations, there may be a firewall (see *KBA NA-0400-0046*).

AMS Device Manager on a separate network from OpenEnterprise

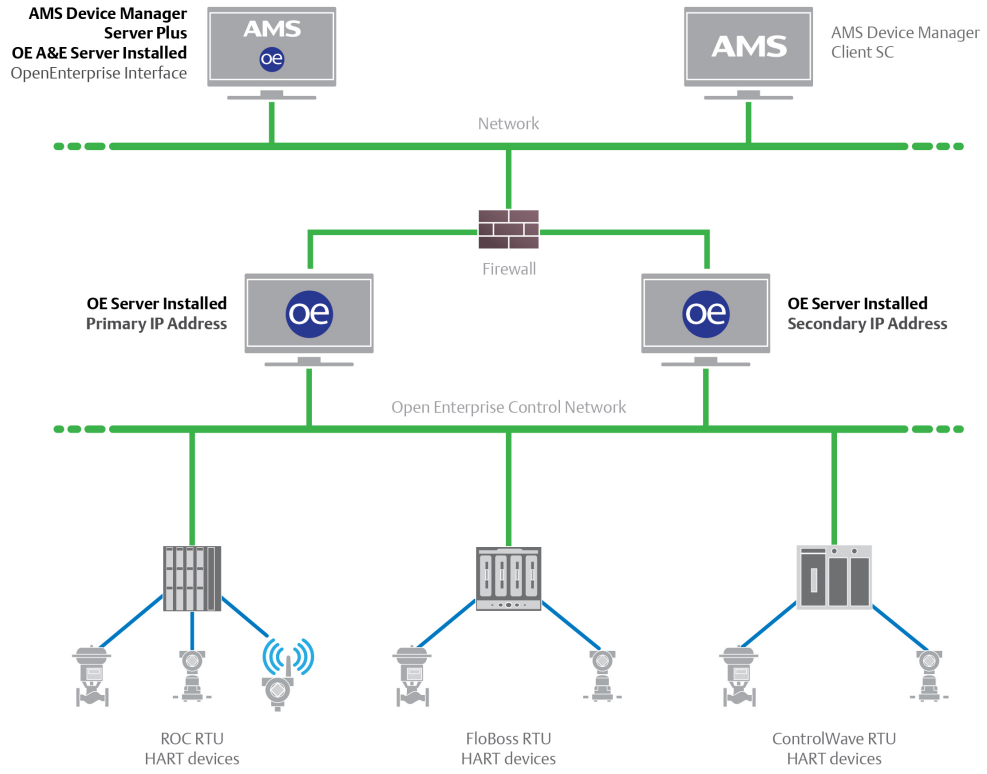


AMS Device Manager with OpenEnterprise Server installed on the same PC

Figure C-4:



AMS Device Manager using a redundant OpenEnterprise network



HSE linking devices

An AMS Device Manager distributed system can be configured to access FF HSE linking devices in a dedicated network environment. This configuration is recommended and requires a dedicated network interface card (NIC) for connecting to the FF HSE linking devices. This arrangement provides the best performance because the FF HSE linking devices are not required to share the network with other network traffic. In this case, manually assign the TCP/IP address of the linking device.

The alternative is to configure an AMS Device Manager distributed system to access FF HSE linking devices from an Ethernet network that assigns TCP/IP addresses using DHCP.

Notes

- If a static TCP/IP address is assigned to a linking device, a valid gateway address must also be provided. The gateway address is usually the TCP/IP address of the dedicated NIC. If the gateway address is invalid, a delay will be seen in AMS Device Manager when rebuilding the hierarchy. In addition, no links or FOUNDATION fieldbus devices will be displayed after performing the Rebuild Hierarchy operation.
- If both the FF HSE Interface and the Ovation System Interface (with FOUNDATION fieldbus devices enabled) are installed on the same PC, configure each on a unique IP address using separate network interface cards.

Appendix D
Version compatibility

As of the initial release of AMS Device Manager 14.0, the following SNAP-ON applications are supported:

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

SNAP-ON application	SNAP-ON application version	AMS Device Manager version 14.0
AMS ValveLink	13.4	x
AlertTrack	6.13.16	x
Rosemount MV Engineering Assistant	5.5.1	x
	6.2.1	x
	6.3	x
	6.4	x
AMS Wireless	13.1.1	x
Flowserve ValveSight Logix MD HART	1.0.0.0	x
Flowserve ValveSight Logix MD+	1.0.0.2	x
Flowserve ValveSight Logix3400MD	1.1.1.5	x
Flowserve ValveSight D3 HART	1.0.0.0	x
ValVue HART	2.81.1	x
ValVue FF	2.32.1	x
Meter Verification	3.2	x
QuickCheck	8.14.51	x
Turck FFPowerAlert	1.0.0.3	x
DCMLink	2.0.606.0	x

Table D-2: DeltaV/AMS Device Manager compatibility matrix

DeltaV Versions	AMS Device Manager version 14.0
12.3	x
12.3.1	x
13.3	x
13.3.1	x
14.3	x

Note

AMS Device Manager supports DeltaV version 12.3 and later in co-deployed installations only.

Table D-3: Ovation/AMS Device Manager compatibility matrix

Ovation versions	AMS Device Manager version 14.0
3.5.1	x
3.6.x	x

Index

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Emerson
12001 Technology Drive
Eden Prairie, MN 55344 USA
T 1(952)828-3000
www.Emerson.com