

AMS Suite: Intelligent Device Manager Version 11.1.1 Installation Guide



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.

Copyright and Trademark Information

© Emerson Process Management. 2011. All rights reserved.

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

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

HART® and WirelessHART® are registered trademarks of the HART Communications Foundation of Austin, Texas, USA.

FOUNDATION™ is a mark of the Fieldbus Foundation of Austin, Texas, USA.

All other marks are property of their respective owners.

Document History

Part Number	Date	Description
10P58249001	Jan 2007	Update, software version 9.0
10P5824A001	Dec 2008	Update, software version 10.0
	Apr 2009	Update, software version 10.1
10P5824A501	Nov 2009	Update, software version 10.5
	Apr 2010	Update, software version 11.0
10P5824B101	Aug 2010	Update, software version 11.1
	Jan 2011	Update, software version 11.1.1

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 Suite: Intelligent 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 Project Operations, Emerson Process Management, 12301 Research Boulevard, Austin, Texas 78759.

Software License Agreement for AMS Suite: Intelligent 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., 12301 Research Boulevard, Austin, Texas 78759, 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

Chapter 1	Introduction	9
	To install a standalone AMS Device Manager system	9
	To install a Distributed AMS Device Manager system.....	9
	To install AMS Device Manager on a DeltaV system.....	9
	To install AMS Device Manager on an Ovation system	10
	To install AMS Device Manager Web Services	10
	About this guide	10
	Before you begin	11
	Upgrading an AMS Device Manager system	11
	Upgrading from AMS Device Manager 9.0 or later.....	12
	Upgrading from AMS Wireless Configurator	12
	Restoring a database	16
	Uninstalling AMS Device Manager	16
Chapter 2	System requirements	19
	Hardware requirements.....	19
	PC processing speed, memory, and disk space	19
	Serial interfaces	20
	USB interfaces	20
	Network requirements	21
	Software requirements.....	22
	Operating systems	22
	Support for Remote Desktop Services.....	23
	Other software requirements	24
	Windows security requirements	27
	AMS Device Manager installation.....	27
	AMS Device Manager use.....	28
	AmsServiceUser.....	28
	Requirements for system interface networks	29
	Wireless.....	29
	DeltaV	30
	Ovation	34
	PROVOX	38
	FF HSE	38
	ROC.....	39
	RS3.....	40
	STAHL	40
	HART Multiplexer Network	41

8000 BIM	41
HART Over PROFIBUS	42
Kongsberg	42
Siemens.....	43
Chapter 3 Installing AMS Device Manager	45
Requirements and constraints	46
Upgrading from a previous version of AMS Device Manager	47
CONSOLIDATING DATABASES	48
Consolidating Service Notes	49
Determining computer names.....	49
Installing Server Plus Station software	50
Installing Client SC Station software	52
Adding a user to the AMSDeviceManager group	54
Licensing a Distributed System	55
Configuring a Distributed System	56
Installing SNAP-ON applications	56
Modifying a Distributed System.....	57
Changing station types.....	58
Changing a Client SC Station to access a different Server Plus Station.....	58
Adding Client SC Stations	59
Replacing an AMS Device Manager Station PC.....	59
Renaming an AMS Device Manager PC.....	61
Adding a new communication interface	62
Adding more tags than currently licensed.....	63
Installing AMS Device Manager on domain controllers.....	63
Domain controller security requirements	64
Mobile Workstation.....	64
Licensing AMS Device Manager 11.1.1 on DeltaV stations	65
Installing AMS Device Manager 11.1.1 on DeltaV stations.....	65
Server Plus.....	66
Client SC.....	69
DeltaV actions	71
DeltaV Upgrade Wizard	72
Uninstalling DeltaV software	72
Uninstalling AMS Device Manager software.....	72
Licensing AMS Device Manager 11.1.1 on Ovation stations.....	73
Installing AMS Device Manager 11.1.1 on Ovation stations.....	73
Server Plus.....	74
Client SC.....	76
Uninstalling Ovation software	78

Chapter 4	Configuring communication interfaces.....	79
	HART modems	79
	Configuring AMS Device Manager for a HART modem	80
	Connecting a HART modem	80
	After a Modem is installed	82
	Field Communicators	83
	Configuring AMS Device Manager for a Field Communicator	84
	Connecting a Field Communicator	84
	Model 275 HART Communicator	85
	Configuring AMS Device Manager for a HART Communicator	86
	Connecting a HART Communicator to AMS Device Manager	86
	Documenting calibrators.....	88
	Configuring AMS Device Manager for a documenting calibrator	88
	Connecting a documenting calibrator	88
	Connecting devices to a documenting calibrator	88
	HART Multiplexer Network Interface.....	89
	Preparing a HART Multiplexer Network Interface	89
	Configuring AMS Device Manager for a HART Multiplexer Network	90
	System interfaces	93
	Wireless.....	94
	DeltaV	96
	Ovation	99
	FF HSE	102
	ROC	103
	PROVOX	104
	RS3.....	107
	STAHL HART	109
	8000 BIM.....	111
	HART Over PROFIBUS.....	112
	Kongsberg Maritime	114
	Siemens	115
	Determining the system interface structure and device data	115
	AMS Device Manager Web Services	117
	AMS Device Manager Web Services and AMS Asset Portal 3.2 or earlier.....	118
	AMS Suite: Asset Performance Management	118
Chapter 5	Starting to Use AMS Device Manager	119
	After installation.....	119
	Changing Windows Firewall settings.....	119
	Usernames and passwords.....	119
	Logging in to User Manager	120
	Assigning an “admin” password.....	120
	Adding a username.....	121

Changing passwords.....	122
Changing rights and permissions.....	122
Using AMS Device Manager	123
Adding devices to an AMS Device Manager installation	125
Attaching a Roving Station to a Server Plus Station	125
Chapter 6 Troubleshooting installation.....	127
Error messages	127

1 Introduction

To install a standalone AMS Device Manager system

- Read “Before you begin” on page 11.
- Confirm that your system meets AMS Device Manager requirements starting on page 19.
- For a new installation of a standalone AMS Device Manager system, follow the Server Plus installation steps in section 3, “Installing AMS Device Manager” beginning on page 45.
- For upgrading from AMS Device Manager 9.0 or later, review Table 1 on page 13 and follow the appropriate steps.

To install a Distributed AMS Device Manager system

- Read “Before you begin” on page 11.
- Confirm that your system meets AMS Device Manager requirements starting on page 19.
- For a new installation of a multistation, distributed AMS Device Manager system, follow the Server Plus and Client SC installation steps in section 3, “Installing AMS Device Manager” beginning on page 45.
- For upgrading from AMS Device Manager 9.0 or later, review Table 1 on page 13 and follow the appropriate steps.

To install AMS Device Manager on a DeltaV system

- Read “Before you begin” on page 11.
- Confirm that your system meets minimum requirements for a co-deployment (refer to the documentation provided with your DeltaV system).
- For a new installation of AMS Device Manager on a DeltaV system, follow the installation steps starting on page 65.

To install AMS Device Manager on an Ovation system

- Read “Before you begin” on page 11.
- Confirm that your system meets minimum requirements for a co-deployment (refer to the documentation provided with your Ovation system).
- For a new installation of AMS Device Manager on an Ovation system, follow the installation steps starting on page 73.

To install AMS Device Manager Web Services

- Read “Before you begin” on page 11.
- Confirm that your system meets AMS Device Manager requirements starting on page 19.
- Follow the installation steps on page 117.

About this guide

This *AMS Suite: Intelligent Device Manager Installation Guide* contains the following information:

- Section 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.
- Section 2, “System requirements” — Lists the system requirements for AMS Device Manager, including hardware, software, and security requirements. This section also defines additional requirements for system interface networks.
- Section 3, “Installing AMS Device Manager” — Describes the procedures for installing AMS Device Manager software. Installing AMS Device Manager on a DeltaV or Ovation network is also detailed.
- Section 4, “Configuring communication interfaces” — Describes how to configure the AMS Device Manager network and install network communication devices (HART modems, HART multiplexers, Field Communicators, 275 HART Communicator, documenting calibrators, and system interface networks).
- Section 5, “Starting to Use AMS Device Manager” — Describes how to start using AMS Device Manager and how to access additional information.
- Section 6, “Troubleshooting installation” — Provides troubleshooting steps you can take if you have problems installing AMS Device Manager.

For more information, refer to AMS Device Manager Books Online or contact your local Emerson Process Management Sales/Service Office.

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 in your system
- AMS Device Manager security requirements (see “Starting to Use AMS Device Manager” on page 119)
- Database backup/restore procedures (see “Backing up a database” on page 15 and “Restoring a database” on page 16)


Upgrading 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). **Before you upgrade, you should back up your database as a precaution against loss of data (see page 15).** 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.

Prior to upgrading your AMS Device Manager application, you should uninstall any SNAP-ON applications on the AMS Device Manager station. You should also stop any programs or processes that access AMS Device Manager Servers (see Table 1). You do not need to remove most of the system interfaces, such as RS3, PROVOX, Ovation, and others.

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**.

After you have completed the upgrade, start the application and right-click each of the network icons. Select **Rebuild Hierarchy** followed by **Scan | New Devices**.

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 all the stations you need to monitor are selected.

Install the latest version of the SNAP-ON applications that were removed prior to upgrading; see “Installing SNAP-ON applications” on page 56.

NOTICE

AMS Device Manager does not support automatic upgrading from version 8.x or earlier. Contact customer support for instructions for your situation.

Upgrading from AMS Device Manager 9.0 or later

Table 1 provides steps for most AMS Device Manager users upgrading from AMS Device Manager 9.0 and later.

Upgrading from AMS Wireless Configurator

- ▶ To install an AMS Device Manager Server Plus or Client SC Station on a PC that has AMS Wireless Configurator installed:
 1. Open the Windows Control Panel and use Add or Remove Programs (XP) or Uninstall a program (Windows Vista/7) to remove AMS Wireless Configurator.
 2. Obtain new license codes for AMS Device Manager (see “Licensing a Distributed System” on page 55).
 3. Install AMS Device Manager (see “Installing Server Plus Station software” on page 50 or “Installing Client SC Station software” on page 52).
 4. If you installed a Server Plus Station in step 3, restore your backed up database (see “Restoring a database” on page 16).

If you installed a Client SC Station in step 3, you may need to consolidate your backed-up AMS Wireless Configurator database with an existing database (if so, refer to “Consolidating databases” on page 48).

Table 1: Upgrading AMS Device Manager

Current Setup	Desired 11.1.1 Setup	
	Server Plus Station	Client SC Station
Server Plus Station	<ul style="list-style-type: none"> • Check in all calibration routes • Back up existing database (page 15) • Uninstall SNAP-ON applications, if installed • Uninstall T+H TACC components, if installed (refer to TACC guides on the AMS Device Manager DVD) • Remove any configured HART Over PROFIBUS but not HART Over PROFIBUS / RouterDTM System Interfaces • Stop any programs or processes that access AMS Device Manager Server³ • Stop AMS Asset Portal Data Collection, if running • Stop AMS Device Manager Server in system tray if running • Install Server Plus Station software (page 50) • Get new license codes, if required (page 55) • Reapply the DeltaV System Interface, if applicable (page 11) • Install required SNAP-ON applications (page 56)^{1,2} • Install new T+H TACC components, if applicable (page 113) • Configure HART Over PROFIBUS/ Router DTM System Interfaces, if applicable (page 112) • Install latest version of Web Services, if required (page 117) • Add all Windows Users (local or domain) to the AMSDeviceManager Windows group • If you plan to continue using AMS Asset Portal, restart Data Collection, but if you have purchased AMS Suite: Asset Performance Management, contact PlantWeb Services for assistance. 	<ul style="list-style-type: none"> • Check in all calibration routes • Back up existing database (page 15) • Consolidate existing databases, if necessary (page 48) • Uninstall SNAP-ON applications • Uninstall T+H TACC components, if installed (refer to TACC guides on the AMS Device Manager DVD) • Remove any configured HART Over PROFIBUS but not HART Over PROFIBUS / RouterDTM System Interfaces • Stop any programs or processes that access AMS Device Manager Server³ • Stop AMS Device Manager Server in system tray if running • Uninstall previous AMS Device Manager software (page 16) • Install Client SC Station software (page 52) • Install required SNAP-ON applications (page 56)¹ • Configure required communication interfaces (page 79) • Install new T+H TACC components, if applicable (page 113) • Configure HART Over PROFIBUS/ Router DTM System Interfaces, if applicable (page 112) • Add all Windows Users (local or domain) to the AMSDeviceManager Windows group

Table 1: Upgrading AMS Device Manager (Continued)

Current Setup	Desired 11.1.1 Setup	
	Server Plus Station	Client SC Station
Client SC Station	<ul style="list-style-type: none"> • Check in all calibration routes • Back up existing database (page 15) • Uninstall SNAP-ON applications, if installed • Uninstall T+H TACC components, if installed (refer to TACC guides on the AMS Device Manager DVD) • Remove any configured HART Over PROFIBUS but not HART Over PROFIBUS / RouterDTM System Interfaces • Stop any programs or processes that access AMS Device Manager Server³ • Stop AMS Device Manager Server in system tray if running • Uninstall previous AMS Device Manager software (page 16) • Install Server Plus Station software (page 50) • Get new license codes (page 55) • Configure required communication interfaces (page 79) • Install required SNAP-ON applications (page 56)^{1,2} • Install new T+H TACC components, if applicable (page 113) • Configure HART Over PROFIBUS/ Router DTM System Interfaces, if applicable (page 112) • Install latest version of Web Services, if required (page 117) • Add all Windows Users (local or domain) to the AMSDeviceManager Windows group • If you plan to continue using AMS Asset Portal, restart Data Collection, but if you have purchased AMS Suite: Asset Performance Management, contact PlantWeb Services for assistance. 	<ul style="list-style-type: none"> • Uninstall SNAP-ON applications • Uninstall T+H TACC components, if installed (refer to TACC guides on the AMS Device Manager DVD) • Remove any configured HART Over PROFIBUS but not HART Over PROFIBUS / RouterDTM System Interfaces • Stop any programs or processes that access AMS Device Manager Server³ • Stop AMS Device Manager Server in system tray if running • Install Client SC Station software (page 52) • Reapply the DeltaV System Interface, if applicable (page 11) • Install required SNAP-ON applications (page 56)¹ • Install new T+H TACC components, if applicable (page 113) • Configure HART Over PROFIBUS/ Router DTM System Interfaces, if applicable (page 112) • Add all Windows Users (local or domain) to the AMSDeviceManager Windows group

Table 1 Notes:

¹ SNAP-ON applications must be uninstalled before installing the latest version.

² AMS ValveLink SNAP-ON application users need to obtain a new license file if upgrading from the ValveLink SNAP-ON for DeltaV to the ValveLink SNAP-ON for AMS Device Manager.

Upgrading AMS ValveLink SNAP-ON application users must edit their permissions in AMS User Manager to retain the same permissions as in previous versions. See “Changing rights and permissions” on page 122.

³ Processes that must be stopped before upgrading include:

- AMSPlantServer
- AMSFileServer
- AMSConnectionServer
- AMSOPC
- AMSGenericExports
- AmsFFServer
- AmsFFAtDeviceBroker
- AMSLicenseServer
- AmsDeviceAlertServer
- AmsHseServer
- AMSDevTypeRemote
- AMSPBServer

Backing up a database

► To back up a database:

Note

If you are backing up an AMS Device Manager 10.5.x database, confirm that the NK-1000-0154 hotfix has been applied (see the NK-1000-0154_Readme.txt file in the 10_5_Hotfix folder on the AMS Device Manager Installation DVD).

1. Run Database Verify/Repair to check the database for duplicate, missing, and corrupt records (select **Start | All Programs | AMS Device Manager | Database Utilities | Database Verify Repair**).
-

Note

For a very large database, the Verify/Repair operation can take a considerable length of time.

2. Back up your database (select **Start | All Programs | AMS Device Manager | Database Utilities | Database Backup**). Save your backup file in a location on your local drive not in the AMS folder.
-

Note

If performing a database backup on a Windows Vista/7/Windows 2008 Server PC with User Account Control enabled, log in with a username included in the AmsDeviceManager Windows group to avoid multiple error messages.

Restoring a database

- To restore a database:
1. Close AMS Device Manager and any related applications (for example, Alert Monitor, Server Plus Connect), if open.
 2. Stop AMS Device Manager Servers (**Start | All Programs | AMS Device Manager | Terminate Servers**).
 3. If the database backup file is located on a network drive, copy it to a local drive.
 4. Select **Start | All Programs | AMS Device Manager | Database Utilities | Database Restore**.
 5. Select the database backup file you want to restore and click **Open**.

Note

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 Windows Vista/7/Windows 2008 Server PC with User Account Control enabled, log in with a username included in the AmsDeviceManager Windows group to avoid multiple error messages.

Uninstalling AMS Device Manager

You must uninstall AMS Device Manager software if you are upgrading from any versions earlier than 9.0. If you are upgrading from any of these versions, contact customer support for instructions for your situation. You do not need to uninstall AMS Device Manager software if you are upgrading from version 9.0 or later. (Exception: If AMS Device Manager is installed on multiple Server 2003/2008 domain controllers, you must uninstall AMS Device Manager on all domain controllers before attempting to upgrade/install.) The installation program modifies the earlier version and migrates the existing database to the new version. Table 1 on page 13 provides the steps to upgrade to AMS Device Manager 11.1.1.

Note

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

▶ To uninstall AMS Device Manager:

1. Back up your existing database. Save your backup file in a location outside the AMS folder.
2. Save your license.dat file in a location outside the AMS folder.
3. Stop the AMS Device Manager Server by right-clicking the icon in the system tray and selecting **Stop AMS Device Manager Server**.
4. Open the Windows Control Panel and use Add or Remove Programs (XP) or Uninstall a program (Windows Vista/7) to remove AMS Device Manager.

See “Consolidating databases” on page 48 for information about consolidating multiple AMS Device Manager databases.

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 may have additional requirements.

Hardware requirements

PC processing speed, memory, and disk space

The recommended *free hard disk space* specified below is the amount needed for AMS Device Manager installation, not the amount needed for daily operation (there are no recommended minimum amounts for daily operation). If you receive a message during installation that you do not have enough hard disk space, free up as much space as possible and then retry the installation.

Station Type	Recommended Requirements w/AMS Device Manager only	Recommended Requirements w/AMS Suite APM
Server Plus Station	Intel® Core™2 Quad, 2 GHz or greater 3 GB memory or greater 2 GB or more of free hard disk space	Intel® Core™2 Quad, 3 GHz or greater 3 GB memory or greater 4 GB or more of free hard disk space
Client SC Station	Intel® Core™2 Duo, 2.4GHz or greater 2 GB memory or greater 2 GB or more of free hard disk space	N/A
<p>Notes:</p> <p>The recommended free hard disk space represents the amount needed for AMS Device Manager installation, not the amount needed for daily AMS Device Manager operation. There are no minimums for daily operation.</p> <p>Additional hard disk space is required for migrating the database if you are upgrading from an earlier version of AMS Device Manager. The amount of space required depends on the size of the existing database.</p> <p>Additional space may be required on the Server Plus Station for the database, depending on the size of your database.</p> <p>Additional hard disk space is required for SNAP-ON applications.</p> <p>Set virtual memory to 2–3 times the size of the physical memory.</p> <p>The minimum monitor requirements are 1024x768 resolution and 16-bit color.</p>		

If you use AMS Asset Portal version 3.2 or earlier, for optimal performance, it should be installed on a non-AMS Device Manager PC. If you choose to co-deploy with AMS Device Manager, the PC must meet these requirements:

- Intel® Core™2 Quad, 3.0 GHz or greater
- 3 GB memory or greater
- 4 GB or more free hard disk space

AMS Suite: Asset Performance Management is a new product offering that replaces AMS Asset Portal version 3.2 or earlier. The AMS Suite: Asset Performance Management Client Framework can be installed on an AMS Device Manager 11.1.1 station that meets the AMS Asset Portal 3.2 requirements. Other components of AMS Suite: Asset Performance Management must be installed on additional non-AMS Device Manager PCs. For more information about AMS Suite: Asset Performance Management, contact your local Emerson Sales/Service Office.

Serial interfaces

- An RS-232 serial interface is required for a serial HART multiplexer network, Model 275 HART Communicator, or documenting calibrator.
- A serial HART modem requires a serial port with a dedicated interrupt.

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 adapters.
- 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).

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. The Microsoft Windows Management Instrumentation and Workstation services must be running on the PC during installation.
- AMS Device Manager does not support deployment between a network workgroup and a network domain.

For information about working with network firewalls, refer to “Changing Windows Firewall settings” on page 119.

Software requirements

Operating systems

Operating System ¹	Supported Native Language Operating Systems	Supported Multilingual User Interfaces (MUIs)
Windows XP, Professional, Service Pack 3	English, German, French, Russian, Japanese, Simplified Chinese, Portuguese ²	German, French, Russian, Japanese, Simplified Chinese, Portuguese ²
Windows 7 Professional	English, German, French, Russian, Japanese, Simplified Chinese, Portuguese ²	German, French, Russian, Japanese, Simplified Chinese, Portuguese ²
Windows Vista Ultimate, Service Pack 1 or Service Pack 2	English, German, French, Russian, Japanese, Simplified Chinese, Portuguese ²	German, French, Russian, Japanese, Simplified Chinese, Portuguese ² (Service Pack 2 only)
Windows Server 2003, Standard Edition, Service Pack 2	English, German, French, Russian, Japanese, Simplified Chinese, Portuguese ²	German, French, Russian, Japanese, Simplified Chinese, Portuguese ²
Windows Server 2003 R2, Standard Edition, Service Pack 2	English, German, French, Russian, Japanese, Simplified Chinese, Portuguese ²	
Windows Server 2008, Standard Edition, Service Pack 1 and Service Pack 2	English, German, French, Russian, Japanese, Simplified Chinese, Portuguese ²	German, French, Russian, Japanese, Simplified Chinese, Portuguese ² (Service Pack 2 only)
¹ Only 32-bit versions of the operating systems are supported.		
² Portuguese is not supported at initial release, but will be available soon after. Contact your local Emerson Process Management Sales/Service Office.		

Notes

- Intermixing of operating system families is not supported. You can use combinations of Windows XP and Server 2003 PCs or Windows Vista/Windows 7 and Server 2008 PCs. No other combinations are supported.
- A Server operating system (Windows Server 2003/2008) and server-class PC (for example, Dell PowerEdge) are recommended if the database is expected to be greater than 4 GB due to the advanced SQL Server version required (see page 25); 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. Contact your hardware vendor for recommendations on server-class PCs and server operating systems.

- 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 “Changing Windows Firewall settings” on page 119 for additional operating system configuration considerations.

Support for Remote Desktop Services

Remote Desktop Services (also known as Terminal Services) is a component of Microsoft Windows (both server and client versions) that allows you to access applications and data on a remote computer over a network, even from a client computer that is running an earlier version of Windows.

Terminal Server is the server-side component of Remote Desktop Services. It authenticates clients and makes applications available remotely. AMS Device Manager can be used in Remote Desktop Services environment if the following conditions are met:

- Terminal Server must be set up prior to AMS Device Manager installation.
- Use of Remote Desktop Services is limited to 5 concurrent sessions when AMS Device Manager is installed on Windows server-class computers with Terminal Server installed. Using this feature, you can administer a server from virtually any computer on your network. No license is required for up to 2 simultaneous remote connections in addition to the Terminal Server console session.
- Use of Remote Desktop Services is limited to 1 session when AMS Device Manager is installed on non-server-class computers.

Note

Do not attempt to install AMS Device Manager using Remote Desktop Services; this is not a supported installation method and produces undesirable results.

- AMS Device Manager is not supported on a Windows Server PC where Terminal Server is set to Relaxed Security.

-
- If multiple users are running AMS Device Manager in a Terminal Services/ Remote Desktop session, and one of the users runs Terminate Servers, the AMS Device Manager application and AMS Device Manager Servers shut down for all users.

Note

In a Remote Desktop Services environment, only 1 AMS ValveLink SNAP-ON application session is permitted at any given time. The AMS Wireless SNAP-ON application is not supported in a Remote Desktop Services environment.

Contact Microsoft for Remote Desktop and Terminal Server licensing information. Questions about AMS Device Manager licensing requirements should be directed to your Emerson Sales Representative.

Other software requirements

Web browser

AMS Device Manager requires Microsoft Internet Explorer (IE) Version 6.0, SP 1 or later. If you do not have a supported version of Internet Explorer, contact your IT department for assistance.

AMS Device Manager Web Services

Microsoft Internet Information Services (IIS) and AMS Device Manager 11.1.1 Server Plus software must be installed on your system before you can install AMS Device Manager Web Services. If you do not have IIS installed, contact your IT department for assistance.

Note

Some control systems do not allow IIS to be installed on the same PC. Check your control system documentation to determine IIS compatibility.

Note

If you want to install AMS Device Manager Web Services on a DeltaV station, it must be a DeltaV Application or ProfessionalPLUS station.

.NET Framework

AMS Device Manager 11.1.1 requires and installs Microsoft .NET Framework 3.5 Service Pack 1. Microsoft .NET Framework 3.5 SP1 is a cumulative update that includes the following versions:

- 2.0
- 2.0 SP2
- 3.0
- 3.0 SP2
- 3.5

Database—Microsoft SQL Server 2005

AMS Device Manager 11.1.1 uses a named instance, Emerson2005, of SQL Server 2005 Service Pack 3 for its database. The default password for this named instance is 42Emerson42. The size of your database determines which edition of SQL Server 2005 you must use:

- *If your database is less than 4 GB, you can use SQL Server 2005 Express Service Pack 3. The AMS Device Manager setup installs this version.*
- *If your database is greater than 4 GB or will be at some future time, you must install SQL Server 2005 Enterprise Service Pack 3 or Standard Edition Service Pack 3, before you install AMS Device Manager. (You must purchase one of these separately if you do not already have it.) These versions of SQL Server require server operating systems.*

Note

The AMS Device Manager database must be located on the AMS Device Manager Server Plus Station. Any other location is not supported.

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.

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

- If no SQL Server is installed, the AMS Device Manager installation program will install SQL Server 2005 Express Service Pack 3 and create an Emerson2005 named instance with a password of 42Emerson42.

- If an instance of SQL 2005 Express Service Pack 3 is installed, but not the Emerson2005 named instance, the AMS Device Manager installation program will create the Emerson2005 named instance with a password of 42Emerson42.
- If the SQL Server 2005 Service Pack 3, Emerson2005 named instance is already installed, the AMS Device Manager installation program will continue with the next part of the installation program. Access to the SQL Server system administrator ('sa') account is required. If you don't have access, contact your network administrator for more information.
- If you have previously installed SQL Server 2005 Standard Service Pack 3 or Enterprise Service Pack 3, you should create an SQL named instance of Emerson2005 prior to installing AMS Device Manager (refer to your SQL Server documentation). Otherwise, the AMS Device Manager installation will install SQL 2005 Express Service Pack 3. If your PC lacks Service Pack 3 for SQL Standard or Enterprise, contact your network administrator.

A Microsoft SQL Server 'sa' account password is required for AMS Device Manager operation. Therefore, the AMS Device Manager setup creates a password (42Emerson42) for the Emerson2005 named instance. For security reasons, it is recommended that you change the SQL password.

▶ To change an SQL Server 'sa' account password on your AMS Device Manager station:

1. Insert AMS Device Manager program DVD in the DVD drive of the target PC.
2. Select **Start | Run** from the Windows taskbar.
3. In the text box, type CMD and click **OK** to open a DOS command prompt.
4. At the DOS command prompt, type:
D:\TECH_SUPPORT_UTILITIES\CHANGE_SA_PASSWORD\SQLPASWD_SQL2005 <oldpassword> <newpassword>

Where:

D is the DVD drive letter

<oldpassword> is the default (42Emerson42) or other current SQL password

<newpassword> is the password you want to use

5. Press ENTER. You should see the message "The SA password in SQL has been changed from *oldpassword* to *newpassword*."
6. Close the DOS command prompt.

Note

Your local Windows security policies may prevent you from changing the 'sa' password again until a predetermined length of time has elapsed.

Software supported for Drawings and Notes

- Microsoft Word 2003, XP, and 2007
- Microsoft Excel 2003, XP, and 2007
- WordPad

Windows security requirements

AMS Device Manager installation

Installation of AMS Device Manager has these security requirements:

- Local or domain administrator rights for the PC(s) on which AMS Device Manager is to be installed.
- If you are installing AMS Device Manager on a PC that has the correct version of SQL Server and the Emerson2005 named instance (see “Database—Microsoft SQL Server 2005” on page 25), you need to know the SQL Server ‘sa’ account password, if a password other than the default (42Emerson42) has been set.
- Before you can install AMS Device Manager, you must open the Windows Control Panel | Folder Options dialog box and, on the **View** tab, uncheck the **Use simple file sharing** (XP) option. If you do not do this, the AMS Device Manager installation will not complete. You must be a user with proper rights to effectively disable this option. (To avoid any AMS Device Manager operational issues, keep this option unchecked.)

Note

You can verify that this option is properly set by looking at your PC registry settings. The option is correctly set (disabled) if the “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\forceguest” registry key is set to zero (0). Contact your IT department for assistance.

Other network security requirements may also apply to the installation. Contact your network administrator for more information.

AMS Device Manager use

The AMS Device Manager installation creates the **AMSDeviceManager** Windows group on the PC. Members of this group have all the permissions necessary to operate AMS Device Manager. You must be a member of this group to operate AMS Device Manager. Windows users must be members of the **AMSDeviceManager** group before their properties can be changed in User Manager. To add a new user, see the “Usernames and passwords” procedures beginning on page 119.

AmsServiceUser

A Windows user account called **AmsServiceUser** is automatically created on each AMS Device Manager station and added to the **Users** Windows user group unless the station is installed on a Windows domain controller. If AMS Device Manager is installed on a domain controller, all AMS Device Manager installations where the PC is part of that domain get the **Domain\AmsServiceUser** account added to the **AmsDeviceManager** Windows user group.

Note

This account is made a member of the **AMSDeviceManager** Windows group on all AMS Device Manager stations as well as a member of the **Users** Windows user group on non-domain controller stations. 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. Do not use the Windows User Manager to change this password as AMS Device Manager will no longer launch.

If the **AmsServiceUser** account becomes unusable for any reason, the following procedures give you steps to remove and recreate the **AmsServiceUser** account.

► To remove the **AmsServiceUser** account and unregister the AMS Device Manager Servers:

1. Select **Start | Run** from the Windows taskbar.
2. In the text box, type **C:\AMS\BIN\AMSUSERACCOUNT.EXE -REMOVE** (where C is the drive containing the AMS folder).
3. Click **OK**.

- ▶ To recreate the **AmsServiceUser** account and register the AMS Device Manager Servers:
1. Select **Start | Run** from the Windows taskbar.
 2. In the text box, type `C:\AMS\BIN\AMSSUSERACCOUNT.EXE` (where C is the drive containing the AMS folder).
 3. Click **OK**.

Requirements for system interface networks

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

Wireless

The Wireless System Interface requires:

- An Ethernet adapter to connect to the gateway.
- One or more (up to 16) wireless gateways that allow communication between the AMS Device Manager station and a collection of wireless devices.
- *WirelessHART* devices. Refer to the AMS Device Manager Supported Device List for a list of supported *WirelessHART* devices. The Supported Device List can be accessed after AMS Device Manager installation is complete (select **Start | All Programs | AMS Device Manager | Help | Supported Device List**).
- A valid SSL certificate (if using the optional Security Setup utility) allowing the AMS Device Manager station to securely communicate with the gateway. Contact your local Emerson Process Management Sales/Service Office for more information about the Security Setup utility.

DeltaV

DeltaV System Interface station software requirements:

- AMS Device Manager 11.1.1 can be installed on the following DeltaV 9.3.1, 10.3.1, or 11.3.1 stations:

DeltaV Workstations	AMS Device Manager Software
ProfessionalPLUS Station	Server Plus or Client SC
ProfessionalPLUS as Remote Client Server	Server Plus or Client SC
Local Application Station	Server Plus or Client SC
Remote Application Station	Server Plus or Client SC
Local "Operate" Station	Server Plus or Client SC
<ul style="list-style-type: none"> Professional Operator Base Maintenance 	
Operator Station as Remote Client Server	Client SC only
Remote "Operate" Station	Client SC only
<ul style="list-style-type: none"> Professional Operator Base 	

- The DeltaV System Interface must be configured on a licensed AMS Device Manager station.

To install AMS Device Manager on a DeltaV network, see the procedures in “Installing AMS Device Manager 11.1.1 on DeltaV stations” on page 65.

- AMS Device Manager 11.1.1 software may also be installed on a separate PC connected to a DeltaV ProfessionalPLUS Station through a separate Ethernet connection as follows:
 - Server Plus – only when AMS Device Manager is not installed on any DeltaV stations.
 - Client SC – only when the Server Plus is co-deployed with DeltaV.
- AMS Device Manager 11.1.1 can also be used with DeltaV 7.4.2 and 8.4.2, but it must be installed on a separate PC.
- Supported HART I/O hardware:
 - Analog Input HART Module, 8-channel, Series 1, Version 2.21 or higher
 - Analog Input HART Module, 8-channel, Series 2, Version 1.26 or higher

- Analog Input HART Module, 16-channel, Version 1.17 or higher
- Analog Output HART Module, Series 1, Version 2.25 or higher
- Analog Output HART Module, Series 2, Version 1.26 or higher
- Supported Intrinsically Safe HART I/O hardware:
 - Analog Input HART Module, 8-channel, Version 2.39 or higher
 - Analog Output HART Module, 8-channel, Version 2.00 or higher

-
- Supported Zone I/O:
 - Analog Input or Analog Output, Version 1.14 or higher
 - Supported FOUNDATION fieldbus I/O:
 - Fieldbus H1, Series 1, Version 1.8 or higher (does not support fieldbus alerts)
 - Fieldbus H1, Series 2, Version 2.2 or higher
 - Supported CHARM I/O:
 - CHARM I/O Carrier (CIOC), Version 11.3 or higher
 - Supported PROFIBUS DP I/O:
 - PROFIBUS Series 2+, Version 1.31 or higher
 - Supported Wireless I/O:
 - Wireless I/O card (WIOC), Version 11.3 or higher
 - Smart Wireless Gateway, Version 3.95 or higher
 - Security—The DeltaV Admin password must be entered in the AMS Device Manager Network Configuration utility (see “Configuring AMS Device Manager for a DeltaV System Interface” on page 98).

If you want to run additional system interfaces, HART modems, or HART multiplexers on AMS Device Manager while using the DeltaV System Interface, contact product support for compatibility information.

DeltaV supports:

- FOUNDATION fieldbus devices
- Wired HART Revision 5 and 6 devices
- *WirelessHART* version 7 devices
- PROFIBUS DP devices
- Devices connected to DeltaV Safety Instrumented System (SIS) logic solvers

Note

Some HART version 6 and 7 commands are not supported by the DeltaV system. Although AMS Device Manager recognizes additional revisions of HART devices when using other HART communication devices, it will not recognize them when they are connected to DeltaV.

DeltaV versions 7.2 and later can access devices connected to RS3 and PROVOX I/O systems through the DeltaV Interface for RS3 I/O and DeltaV Interface for PROVOX I/O, respectively. The devices are displayed in the DeltaV network hierarchy in AMS Device Manager. For installation and setup information, refer to the DeltaV Books Online.

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



To run the utility:

1. Select **Start | Run** from the Windows taskbar.
2. In the text box, type C:\AMS\BIN\DELTAVFASTSCANUTILITY.EXE (where C is the drive containing the AMS folder).
3. Uncheck the box for the appropriate DeltaV network.
4. Click **Save Changes**.

The AMS ValveLink SNAP-ON application is supported for DeltaV I/O cards, but not for RS3 and PROVOX I/O cards. See “PROVOX” on page 38 for I/O requirements.

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

Ovation

Ovation System Interface station software requirements:

- AMS Device Manager 11.1.1 can be installed on the following Ovation 3.2 and 3.3.1 stations:

Ovation Workstations	AMS Device Manager Software
3.2 Operator Station	Server Plus or Client SC
3.2 Engineer Station	Server Plus or Client SC
3.3.1 Operator Station	Server Plus or Client SC
3.3.1 Engineer Station	Server Plus or Client SC
3.3.1 System Database Server	Client SC only

- The Ovation System Interface must be configured on a licensed AMS Device Manager station.

To install AMS Device Manager on an Ovation network, see the procedures in “Installing AMS Device Manager 11.1.1 on Ovation stations” on page 73.

- AMS Device Manager 11.1.1 software (Server Plus or Client SC) may also be installed on a separate PC connected to an Ovation station through a separate Ethernet connection.
- To use AMS Device Manager 11.1.1 with earlier versions of Ovation, contact your Emerson Process Management Sales/Service Office.

The Ovation System Interface requires that:

- The Ovation System Software is version 3.2 or 3.3.1.
- The Ovation Fieldbus Engineering Tool (FET) is installed on the Ovation Station which is linked by the AMS Device Manager Ovation System Interface.
- One or more Ovation controllers be configured with HART I/O modules. The HART I/O Modules may be on local or remote Ovation I/O.
- All FOUNDATION fieldbus devices communicate with an Ovation controller through an Ovation fieldbus gateway.
- The FOUNDATION fieldbus device support be enabled for only one Ovation network on an AMS Device Manager station.
- All *Wireless*HART devices communicate through a Smart Wireless Gateway.

For device support, you can install 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 software and the Ovation System Interface can be installed on an Ovation Engineer Station.
 - 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 Base Station. See the Ovation documentation for information about communication settings required in the Ovation Engineer or Operator Station.
 - AMS Device Manager does not support burst mode messages from HART devices on Ovation Stations.
- For FOUNDATION fieldbus devices:
 - If you want to access FOUNDATION fieldbus device information on your Ovation system, AMS Device Manager must be installed on an Ovation Engineer Station that also has the FET server installed.
 - 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 Engineer/AMS Device Manager station. The AMS Device Manager Ovation System Interface must also be installed on this station.
- For HART and FOUNDATION fieldbus devices:
 - If you want to access HART and FOUNDATION fieldbus device information on your Ovation system, AMS Device Manager can be installed on a Windows XP-based Ovation drop, which includes Ovation Engineer Stations.
- 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 SIS 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 to set up an Ovation System Interface.

Note

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 impacted if the hosts 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.

Each Ovation controller uses a unique TCP/IP address. AMS Device Manager communicates with HART devices, *WirelessHART* 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
- Supported FOUNDATION fieldbus I/O:
 - Gateway 5X00151G01 and H1 Series 2 Module 5X00152G01, Version 1
 - Module 5X00301 with cavity insert 1X00458H01 or Module 5X00301 with Personality Module 5X00327, Version 1
- Supported Intrinsically Safe controller:
 - Ovation SIS Logic Solver, KJ2201X1-PW1, Version 1

Additional Ovation requirements for Windows XP PCs

If AMS Device Manager is installed on a separate Windows XP PC, a registry setting must be changed on the Ovation server to enable TCP/IP forwarding.

NOTICE

If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system.

► To change the default registry settings:

1. Select **Start | Run** from the Windows taskbar.
2. In the text box, type REGEDIT and click **OK**.
3. In the Registry Editor, view the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
4. Set the following registry values:
Value Name: IPEnableRouter
Value type: REG_DWORD
Value Data: 1

Note

A data value of 1 enables TCP/IP forwarding for all network connections installed and used by this computer.

5. Click **OK**.
6. Close the Registry Editor.

PROVOX

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

FF HSE

The FF HSE interface requires:

- One or more (up to 8) commissioned FF HSE Linking Devices that conform to the FOUNDATION fieldbus HSE and H1 specifications (for a list of supported linking devices, see the Release Notes). 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, refer to 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.

- Commissioning using the device manufacturer’s commissioning/ decommissioning utility.
- FF HSE Linking Device configuration with unique TCP/IP addresses.
- An AMS Device Manager station with 1 or 2 Ethernet network interface cards (NIC). Two NICs are recommended to configure a dedicated FF HSE segment, to reduce the amount of competing network communications.

NOTICE

If you have an Ovation network installed, use a different TCP/IP address for the FF HSE network.

ROC

AMS Device Manager connects to the ROC Interface using a polling engine that is installed separately from and not supplied with AMS Device Manager. The ROC field servers and ROCs must be added to the polling engine before AMS Device Manager can communicate with the ROCs. The ROC Interface requires one or more of the following controllers:

- ROC809\827 Series 1 with W68126, Version 1.53/2.16 firmware
- ROC809\827 Series 2 with W68126, Version 3.00/3.10 firmware
- Smart Wireless Module (or Gateway), version 1.00
- ROC 809L version 1.00

To use the controllers, the HART I/O module AI/AO Card (W38260) Rev. A with W68153, version 1.10 firmware is also required.

To obtain the required polling engine, contact your Emerson Process Management Sales/Service Office.

If you plan to use *WirelessHART* devices, you also need a Smart Wireless Module for the ROC800 Series as well as the Smart Wireless User Program. To obtain these items, contact your Emerson Process Management Sales/Service Office.

Note

ROC polling services is not supported on Windows 7/2008. You must use Windows XP/2003.

AMS Device Manager supports the ROC FF and ControlWave linking devices, however these display in the FF HSE hierarchy. For more information, see “FF HSE” on page 38.

RS3

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

The STAHL HART interface requires:

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

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. See 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.

HART Multiplexer Network

A HART multiplexer network requires:

- One serial communication port for each HART multiplexer network.
- An RS-485 converter (see the Release Notes for supported models).
- One of the following types of multiplexers or I/O:
 - Arcom
 - Elcon
 - 8000 BIM
 - Pepperl+Fuchs
 - Spectrum Controls I/O (this is an I/O module that connects to an Allen-Bradley Programmable Logic Controller - displays as a multiplexer in AMS Device Manager)

See the Release Notes for additional requirements for specific types of multiplexers. For more information about multiplexer networks, refer to KBA NA-0400-0084.

8000 BIM

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

HART Over PROFIBUS

Note

Prior to moving to AMS Device Manager 11.1.1 from previous versions supporting HART Over PROFIBUS, contact your Emerson Sales Representative 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 Windows XP, Windows 7, or Windows Server 2003.
 - A control system that supports PROFIBUS DP V1 is configured and operational.
 - At least one Trebing & Himstedt (T+H) PROFIBUS Gateway for communications is configured and T+H AMS Device Manager Communications Components (TACC) Version 2 or higher software is installed.
-

Note

T+H TACC 2.2.2.0 software supports installation on Windows 7, but only in a Workgroup environment. Domains are not supported.

- At least one PROFIBUS DP remote I/O subsystem that supports HART communications is connected to the control system. Contact your Emerson Sales Representative for a list of supported I/O subsystems.
- 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.

Refer to the *TH AMS Device Manager Communication Components HART Over PROFIBUS User Guide* on AMS Device Manager installation DVD for more information.

Kongsberg



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) 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.

Only the following PROFIBUS DP and HART I/O modules are supported:

Manufacturer	Description / Module Type	Notes
STAHL	PROFIBUS DP I.S.1 type 9440	Supports up to 16 connected I/O modules
STAHL	HART Analog Input type 9461 HART Analog Output type 9466	Supports up to 8 connected HART instruments
STAHL	ISpac HART Multiplexer type 9192	Configurations possible for up to 32 connected HART devices. Up to 128 RS485 addresses (ISpac multiplexers) are possible on a single RS485 segment



Siemens

The Siemens System Interface lets you use AMS Device Manager to communicate with HART devices on a Siemens PCS 7 Control Network. An AMS Device Manager Server Plus or Client SC station must be installed on the same station as the Siemens PCS 7 ES/MS Station. The AMS Device Manager Network Configuration utility is used to configure the Siemens System Interface.

The Siemens System Interface requires that:

- The Siemens Network is licensed.
- A Siemens System v7 with SP1 or higher is installed on the ES / MS Station and the DeviceCom interface is accessible from the AMS Device Manager.
- Siemens PCS 7 project file is copied from the live system.

3 Installing 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 section 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. 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 in the following order:

1. On the PC to be the Server Plus Station, install the Server Plus Station Software (see “Installing Server Plus Station software” on page 50).
2. On each PC to be used as a Client SC Station, install the Client SC Station software (see “Installing Client SC Station software” on page 52).

If you are installing AMS Device Manager on a domain controller PC, see “Installing AMS Device Manager on domain controllers” on page 63.

If you are installing AMS Device Manager on a DeltaV station, see “Installing AMS Device Manager 11.1.1 on DeltaV stations” on page 65.

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, refer to “Upgrading from AMS Wireless Configurator” on page 12.

Requirements and constraints

Ensure that all the system requirements specified in Section 2, “System requirements” and stated below are met prior to installing a distributed system. If you are installing an AMS Device Manager distributed system using a domain controller, there are other requirements. See “Installing AMS Device Manager on domain controllers” on page 63.

- 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.
- A user with Windows system administrator rights is required to set up a distributed system.
- 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.
- 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 must be recorded. See “Determining computer names” on page 49.
- All Windows usernames with associated passwords for any Windows user that will be running AMS Device Manager must be added to the AmsDeviceManager Windows user group on all AMS Device Manager stations in a distributed network (see “Adding a user to the AMSDeviceManager group” on page 54).
- 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 are based on the clock in the PC that generated that event.
- All stations must use like operating systems. That is, you can pair stations using Windows XP Professional and Windows Server 2003 or Windows Vista/7 and Windows Server 2008. No other configurations are supported.
- All stations must use the same application and version for entering Drawings/ Notes (such as Microsoft Word 2003, XP, and 2007 or Microsoft Excel 2003, XP, and 2007).
- Be sure you have the correct version of SQL Server for your Server Plus Station (based on your database size—see page 25).
- All stations must use the same revision of AMS Device Manager software.

Note

Consult with your network/system administrator about security issues and any other network operation issues or special requirements for your LAN.

During installation, the **AMSDeviceManager** Windows group is given write access to the AMS folder, subfolders, and files with all the permissions necessary to start and operate AMS Device Manager. An administrator is required to add Windows User IDs to this group to allow operation of AMS Device Manager (see “Adding a user to the AMSDeviceManager group” on page 54).

The installation creates a share of the AMS folder which grants the **Everyone** Windows group Full Control permissions. 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.

For information on installing AMS Device Manager on domain controllers, see “Installing AMS Device Manager on domain controllers” on page 63.

Note

AMS Device Manager 11.1.1 testing has revealed a potential installation problem with at least one virus scan/PC security application whereby the installation stops without warning (see KBA NA-0900-0062). Contact your IT department for assistance.

Upgrading from a previous version of AMS Device Manager

Before you install version 11.1.1, refer to Table 1 on page 13.

AMS Device Manager version 11.1.1 supports a migration path for versions 9.0 and later. Back up your databases before you begin the migration process.

AMS Device Manager does not support automatic upgrading from version 8.x or earlier. For these earlier versions, you must back up your database, uninstall your earlier version, install version 11.1.1, and then restore your database. If you have any questions or encounter any unexpected issue, contact customer support.

Prior to upgrading your AMS Device Manager application, you should uninstall any SNAP-ON applications on the AMS Device Manager station. After upgrading AMS Device Manager, install the latest versions of any licensed SNAP-ON applications, see “Installing SNAP-ON applications” on page 56.

Configure any required system interface networks and then open AMS Device Manager. 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 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.

Consolidating databases

If you have multiple Server Plus Stations and are consolidating their databases for use in a distributed system, use the following procedures.

► To consolidate databases:

1. Back up the current database on all stations containing a database you want to consolidate (see Table 1 on page 13).
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 box 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 of 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 box for instructions.
3. When the databases have been consolidated, perform a database backup of the consolidated database.
 4. The AMS Device Manager 11.1.1 Server Plus Station can be installed using one of the following methods (see “Installing Server Plus Station software” on page 50).

Method 1

Install AMS Device Manager 11.1.1 as a station upgrade, if upgrading from version 9.0 or later which automatically migrates the consolidated database.

Method 2

Uninstall the current 8.x or earlier station software and install version 11.1.1 as a new Server Plus Station. Restore the consolidated database.

Consolidating 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 SNAP-ONS And Tools\Tech_Support_Uutilities\DrawingsAndNotesUtility folder on the AMS Device Manager installation DVD.

Determining 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 “Configuring a Distributed System” on page 56). Due to database limitations, 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:

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.

Table 1: Computer name log example

Station	Computer Name
Server Plus Station	
Client SC Station # 1	
Client SC Station # 2	
Client SC Station # 3	
Client SC Station # ...	
Client SC Station # n	

Installing Server Plus Station software

If you are installing an AMS Device Manager distributed system using a domain controller, there are other requirements. See “Installing AMS Device Manager on domain controllers” on page 63.

Note

If you are upgrading your software and changing the station type, you must uninstall the earlier version of AMS Device Manager before upgrading to 11.1.1. (See Table 1 on page 13.)

▶ To install software on the Server Plus Station:

1. Exit/close all Windows programs, including any running in the background (including virus scan software).
2. Insert the AMS Device Manager program DVD 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**.

Note

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.

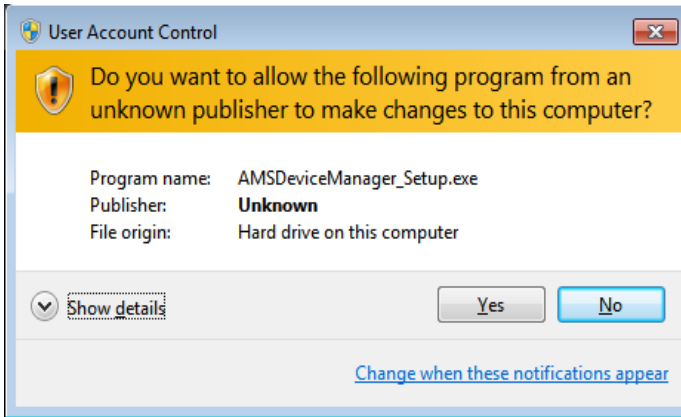
4. Click **Server Plus Station**.
5. Follow the prompts.

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 Windows Vista/7 or Windows Server 2008 PC, and User Account Control (UAC) is enabled, the User Account Control dialog box (similar to below) 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**.

Note

All licensing for a distributed system is done on the Server Plus Station.

6. When the Licensing Wizard appears, click **Next** to obtain license codes or click **Cancel** if you are upgrading and do not need to relicense (see Table 1 on page 13). See “Licensing a Distributed System” on page 55.
7. Configure the Server Plus Station to recognize each station connected in the system (see “Configuring a Distributed System” on page 56). This step is essential for the other stations to access the Server Plus Station.
8. Set up and configure the system interface networks (see “Configuring communication interfaces” on page 79).
9. Install the latest versions of any licensed SNAP-ON applications, if appropriate (see “Installing SNAP-ON applications” on page 56).
10. Open AMS Device Manager, right-click each of the network icons and select **Rebuild Hierarchy** followed by **Scan | New Devices**.

11. 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.

During installation, the **AMSDeviceManager** Windows group is given write access to the AMS folder, subfolders, and files with all the permissions necessary to start and operate AMS Device Manager. An administrator is required to add Windows User IDs to this group to allow operation of AMS Device Manager (see “Adding a user to the AMSDeviceManager group” on page 54).

The installation creates a share of the AMS folder which grants the **Everyone** Windows group Full Control permissions. 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.

Installing Client SC Station software

The following steps install the Client SC Station software.

Verifying 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:

1.  At the AMS Device Manager Server Plus Station, select **Start | Run** from the Windows taskbar.
2. In the text box, type CMD and click **OK** to open a DOS command prompt.
3. At the DOS prompt, type PING <Client SC Station Computer Name>.
4. Press ENTER.
5. 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 typed the correct address in the command line. Also verify that your network is functioning properly. Contact your IT department if you cannot establish connectivity.

- To install software on a Client SC Station:
1. Clear all applications from the Windows Startup folder until after installation is finished. Exit/close all Windows programs including any running in the background (such as virus scan software).
 2. Insert the AMS Device Manager program DVD in the DVD drive of the PC to be used as a Client SC Station.
 3. When the AMS Device Manager setup starts, click Install AMS Device Manager.

Note

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.

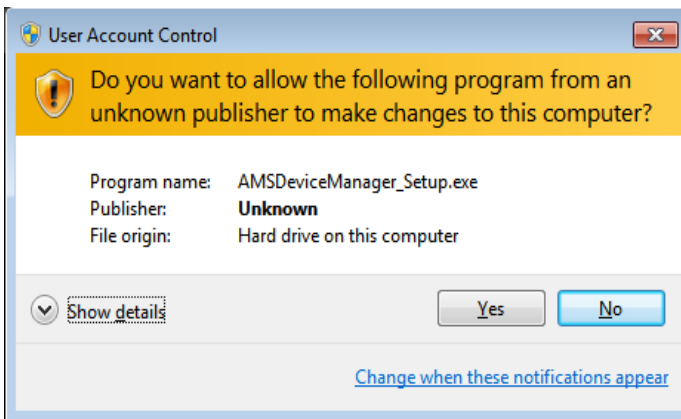
4. Click **Client SC Station**.
5. Follow the prompts.

NOTICE

Do not interrupt the installation process, otherwise 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 Windows Vista/7 or Windows Server 2008 PC, and User Account Control (UAC) is enabled, the User Account Control dialog box (similar to below) 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**.

6. Set up and configure the communication interfaces (see "Configuring communication interfaces" on page 79).

7. Install the latest versions of any licensed SNAP-ON applications, if appropriate (see “Installing SNAP-ON applications” on page 56).
8. Open AMS Device Manager, right-click each locally configured network icon and select **Rebuild Hierarchy** and then **Scan | New Devices**.
9. 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.

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.

Adding a user to the AMSDeviceManager group

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

Note

The following procedure requires Local or Domain Administrator permissions.

► To add a user to the **AMSDeviceManager** group:

1. (XP) Right-click the **My Computer** desktop icon.
(Windows Vista/7) Click Start and right-click **Computer**.
2. Select **Manage** from the context menu.
3. Select **Computer Management (Local) | System Tools | Local Users and Groups | Groups**.
4. Double-click the **AMSDeviceManager** group.
5. Click **Add**.
6. Enter the Windows User ID you want to add to the group and click **OK**.
7. Click **OK**.
8. Windows Vista/7/2008 Server requires that you log out of Windows and log back in to make the change effective.

This process is different when using a domain controller (see “Adding a user to the AMSDeviceManager group on a domain controller” on page 64).

Licensing a Distributed System

All licensing for an AMS Device Manager Distributed System is done on the Server Plus Station. The Licensing Wizard starts automatically near the end of the installation process—follow the prompts to gather the 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 fax, e-mail, or by downloading from the AMS Device Manager registration website at:

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

If you use the internet registration method to relicense your AMS Device Manager system, be sure to request a new license file.

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.

Note

During the licensing process, you must have read access to the PC disk drive you installed on (C: drive by default) so that the Licensing Wizard can verify the hard disk serial number.

► To run the Licensing Wizard:

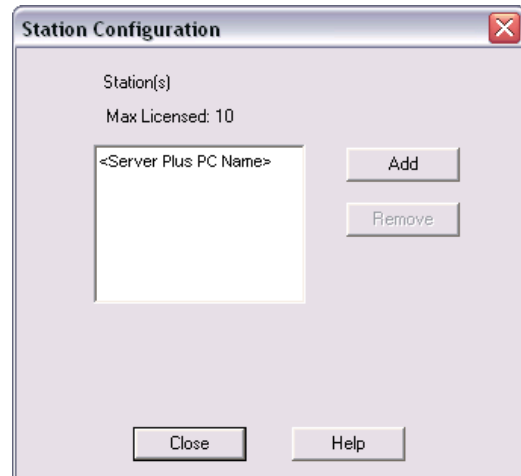
1. Select **Start | All Programs | AMS Device Manager | Licensing | Licensing Wizard**.
2. Follow the instructions in the Licensing Wizard.
3. If you are installing new license information on an existing station, start AMS Device Manager to see the changes.

Configuring 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.

► To configure your distributed system:

1. On the Server Plus Station, select **Start | All Programs | AMS Device Manager | Station Configuration** from the Windows taskbar.
2. In the Station Configuration dialog box, click **Add**.
3. Enter the computer name of the Client SC Station PC (see “Determining computer names” on page 49), 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. 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.



Installing 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. To determine if a SNAP-ON is supported on your system, refer to the SNAP-ON_Compatibility_Matrix.pdf located in the SNAP-ONS And Tools/SNAP-ONS/Installs folder on the installation DVD.

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.

Note

Before you install a SNAP-ON application on a Client SC, ensure that the Server Plus Station is installed and available on the network and that the Client SC Station can access it.

► To install a SNAP-ON application:

1. Make sure the Windows Control Panel is not open and exit all Windows programs, including any programs that may be running in the background such as virus protection software.

2. Insert the AMS Device Manager program DVD in the DVD drive of the PC.
3. Browse to the D:\SNAP_ONS*<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).
4. Click **OK**.
5. Follow the prompts.

Note

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.

Note

All SNAP-ON applications, with the exception of AMS ValveLink and AMS Wireless, use the Windows user account name to determine the user privileges. Therefore, the AMS Device Manager user must have a user account configured with the same name as the Windows user account. For all SNAP-ON applications except AMS ValveLink and AMS Wireless, this user must also have Device Write permission (see “Logging in to User Manager” on page 120).

AMS ValveLink SNAP-ON application user privileges must be enabled in AMS Device Manager User Manager.

Note

If a SNAP-ON application is not installed in the C:\Program Files folder, the AMSDeviceManager group must be given access to the location.

Modifying a Distributed System

Once your distributed system is installed, any changes to its physical configuration may require special procedures in AMS Device Manager. To change station types in an existing system, see “Changing station types” on page 58. For other types of changes, see the following:

- Changing station types (page 58).
- Changing a Client SC Station to access a different Server Plus Station (page 58).
- Adding a PC (Client SC Station) to an existing distributed system (page 59).
- Replacing a PC (page 59).
- Renaming a PC (page 61).
- Adding a new communication interface (page 62).
- Adding more tags than currently licensed (page 63).
- Installing on domain controllers (page 63).

Changing station types

If you are changing station types, perform the following appropriate procedures. You may also need to reset your users' permissions (see "Changing rights and permissions" on page 122).

▶ To change an AMS Device Manager Server Plus Station to a Client SC Station:

1. Back up the database (page 14).
2. Uninstall the previous Server Plus Station software (page 16).
3. Ensure that a connection can be made to an available Server Plus Station.
4. Install the Client SC Station software (page 52).
5. Restore the database on another Server Plus Station (page 16).

▶ To change an AMS Device Manager Client SC Station to a Server Plus Station:

1. Get new license codes (page 55).
2. Uninstall the previous Client SC Station software (page 16).
3. Install the Server Plus Station software (page 50).

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

▶ To 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. Select **Start | All Programs | AMS Device Manager | Server Plus Connect**.
3. In the **Server Plus Connect** dialog box, 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 Books Online.

The Server Plus Connect utility cannot be used on Client SC Stations installed on DeltaV or Ovation workstations. In these configurations, to change a Client SC Station to access a different Server Plus Station:

1. Uninstall AMS Device Manager on the Client SC Station (see page 16).
2. Reinstall AMS Device Manager on the Client SC Station and indicate the new Server Plus Station, see “Installing Client SC Station software” on page 52.

Adding 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, obtain new license codes. After you receive your new license codes, run the Licensing Wizard on the Server Plus Station (see “Licensing a Distributed System” on page 55) and then continue with step 2.
2. To install AMS Device Manager on the added Client SC Stations, see “Installing Client SC Station software” on page 52.
3. Update the Client SC Station configuration on the Server Plus Station (see “Configuring a Distributed System” on page 56).
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.

Replacing an AMS Device Manager Station PC

Replacing a Server Plus Station PC

► To replace a Server Plus Station PC:

1. Obtain new license codes, see “Licensing a Distributed System” on page 55. (License codes are assigned to a single hard disk serial number.)
2. Back up the database (see page 14) and save the backup file in a secure location.
3. Uninstall AMS Device Manager from the old PC (see page 16). 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 PC has a different computer name, all active alerts in the Alert Viewer 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 “Changing a Client SC Station to access a different Server Plus Station” on page 58).

5. Install Server Plus Station software on the new PC (see “Installing Server Plus Station software” on page 50).
6. When the Licensing Wizard appears, enter the new license codes.
7. Set up the server configuration to recognize each Client SC Station connected in the system (see “Configuring a Distributed System” on page 56).
8. Restore the database using the backup file you saved in step 2 (see “Restoring a database” on page 16).

Replacing a Client SC Station PC

► To replace a Client SC Station with a new PC:

1. Uninstall AMS Device Manager from the old PC (see “Uninstalling AMS Device Manager” on page 16). Disconnect the PC from the network, if appropriate.
2. Connect the new PC to the network.
3. On the Server Plus Station, select **Start | All Programs | AMS Device Manager | Station Configuration** from the Windows taskbar.
4. In the Station Configuration dialog box, select the name of the old PC and click **Remove**.
5. In the Station Configuration dialog box, click **Add**.
6. Enter the computer name of the new Client SC Station PC (see “Determining computer names” on page 49), 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 “Installing Client SC Station software” on page 52).

Renaming an AMS Device Manager PC

- To rename a Server Plus Station PC:
1. Back up your AMS Device Manager database (see “Backing up a database” on page 15).
 2. Record all of the devices contained in the Device Monitor List. After renaming the PC, you must re-enter them in step 9.
 3. Uninstall AMS Device Manager on the Server Plus Station and all Client SC Stations in a distributed system (see “Uninstalling AMS Device Manager” on page 16).
 4. Rename the Server Plus Station PC:
 - Right-click the Windows desktop **My Computer** icon.
 - Select **Properties**.
 - Click **Change Settings** (Windows Vista/7 only).
 - On the **Computer Name** tab, click **Change**.
 - Enter a new computer name and click **OK**.
 - Click **OK**.
 5. Install AMS Device Manager on the Server Plus Station and all Client SC Stations in a distributed system (see “Installing Server Plus Station software” on page 50 and “Installing Client SC Station software” on page 52).
 6. Restore the database backed up in step 1 (see “Restoring a database” on page 16).
 7. Reinstall the required system interfaces (see “Configuring communication interfaces” on page 79) and SNAP-ON applications (see “Installing SNAP-ON applications” on page 56).
 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 on the Server Plus Station (see AMS Device Manager Books Online).
- To rename a Client SC Station PC:
1. Renaming the PC clears the Device Monitor List, so record all devices contained in the Device Monitor List.
 2. Uninstall AMS Device Manager on the Client SC Station PC (see “Uninstalling AMS Device Manager” on page 16).

3. Rename the Client SC Station PC:
 - Right-click the Windows desktop **My Computer** icon.
 - Select **Properties**.
 - Click **Change Settings** (Windows Vista/7 only).
 - On the **Computer Name** tab, click **Change**.
 - Enter a new Computer Name and click **OK**.
 - 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 “Configuring a Distributed System” on page 56).
5. Install AMS Device Manager on the Client SC Station PC (see “Installing Client SC Station software” on page 52).
6. Reinstall the required system interfaces (see “Configuring communication interfaces” on page 79) and SNAP-ON applications (see “Installing SNAP-ON applications” on page 56).
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 (see AMS Device Manager Books Online).

Adding a new communication interface

- To add a new communication interface (for example, an additional system interface):
1. Obtain a new license code for the desired communication interface.
 2. Run the Licensing Wizard on the Server Plus Station (see “Licensing a Distributed System” on page 55).
 3. Configure the new communication interface (see “Configuring communication interfaces” on page 79).

Adding more tags than currently licensed

- To add more tags than currently licensed:
1. Obtain new license codes to cover the number of tags needed.
 2. Run the Licensing Wizard on the Server Plus Station (see “Licensing a Distributed System” on page 55).
 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 you install an AMS Device Manager distributed system on domain controller stations and non-domain controller stations on the same network, install either the AMS Device Manager Server Plus or Client SC on a domain controller first, and then the other stations on other domain controllers or non-domain controllers.

Note

If a Server Plus is installed on a domain controller, all Client SC Stations that are part of that domain must be clients of this Server Plus. Only one AMS Device Manager distributed system is allowed on a single domain.

- If AMS Device Manager will be used in a cross-domain configuration and AMS Device Manager will not be installed on a domain controller, create the AmsServiceUser account on any domain-resident PCs prior to installing AMS Device Manager on them. Refer to KBA NA-0800-0113.

Note

AMS Device Manager is not supported on a Windows Server 2008 read-only domain controller.

Domain controller security requirements

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

Adding a user to the AMSDeviceManager group on a domain controller

Note

The following procedure requires network administrator permissions.

- To add a user to the **AMSDeviceManager** group:
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**.

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 “Hardware requirements” on page 19), it functions like a station connected to a wired Ethernet LAN. However, no system interfaces should be configured on a mobile workstation, as this can cause database issues regarding the path of the connected HART 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 11.1.1 on DeltaV stations

When DeltaV 11.3 or later is acquired, AMS Device Manager 11.1.1 is packaged with it to ensure that both products are available to install.

NOTICE

If you have licensed your AMS Device Manager 11.1.1 software, you see a full-function application when you launch the product. If not licensed, 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 a number of 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 Process Management 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 65.

Installing AMS Device Manager 11.1.1 on DeltaV stations

AMS Device Manager 11.1.1 can only be co-deployed on DeltaV 9.3 and newer stations. To ensure a proper installation, DeltaV must be installed before AMS Device Manager. In a typical deployment, the AMS Device Manager Server Plus software would be installed on the DeltaV ProfessionalPLUS Station, Application Station, or Maintenance Station. AMS Device Manager Client SC software would be installed on other supported DeltaV station types in the network. This deployment gives all connected stations access to both AMS Device Manager and DeltaV databases.

Note

AMS Device Manager software, either Server Plus or Client SC, must be installed on a DeltaV ProfessionalPLUS Station to ensure proper licensing functionality, proper user synchronization between DeltaV and AMS Device Manager, and proper Device Description (DD) installation.

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 “Licensing AMS Device Manager 11.1.1 on DeltaV stations” on page 65).

Note

Upgrading an existing DeltaV station containing custom FOUNDATION fieldbus device definitions may require special installation procedures. Refer to the documentation that came with your DeltaV upgrade software.

Note

If you are installing AMS Device Manager on any domain controller stations, refer to “Installing AMS Device Manager on domain controllers” on page 63.

Note

AMS Device Manager is not supported on a non-DeltaV node within a DeltaV domain.

Server Plus

► To install Server Plus software on the DeltaV ProfessionalPLUS Station:

1. Exit/close all Windows programs, including any running in the background (including virus scan software).

Note

If the ValveLink SNAP-ON for DeltaV is installed, it must be uninstalled and the AMS ValveLink SNAP-ON application for AMS Device Manager installed at the appropriate time (see “Installing SNAP-ON applications” on page 56 and AMS Device Manager Books Online). Information about migrating ValveLink SNAP-ON for DeltaV data is located in AMS ValveLink SNAP-ON Help.

2. Insert the AMS Device Manager program DVD in the DVD drive of your PC.
3. When the AMS Device Manager setup starts, click **Install AMS Device Manager**.

Note

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**.

4. Click **Server Plus Station**.

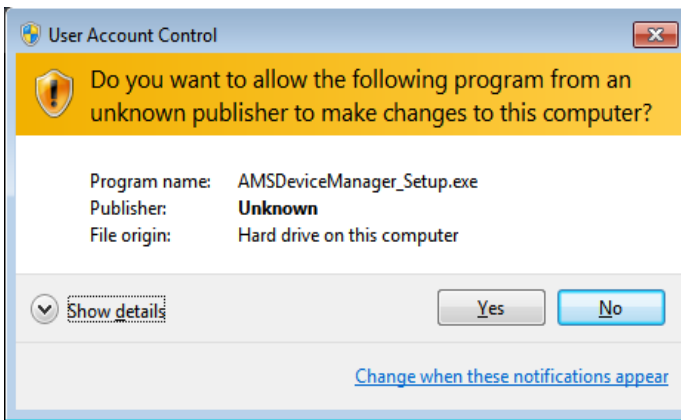
5. Follow the prompts.

NOTICE

Do not interrupt the installation process, otherwise 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 Windows Vista/7 or Windows Server 2008 PC, and User Account Control (UAC) is enabled, the User Account Control dialog box similar to below 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**.

Note

All licensing for a distributed system is done on the Server Plus Station.

6. When the Licensing Wizard appears, click **Next** to obtain license codes or click **Cancel** if you are upgrading and do not need to relicense (see Table 1 on page 13). See "Licensing a Distributed System" on page 55.
7. Set up the server configuration to recognize each station connected in the system (see "Configuring a Distributed System" on page 56). This step is essential for the other AMS Device Manager stations to access the Server Plus Station.

-
8. Configure the DeltaV Network system Interface (see “Configuring AMS Device Manager for a DeltaV System Interface” on page 98) so that AMS Device Manager can detect and work with devices on the DeltaV network.

Note

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

9. Set up and configure any other required communication interfaces (see “Configuring communication interfaces” on page 79).
10. Install the latest versions of any licensed SNAP-ON applications, if appropriate (see “Installing SNAP-ON applications” on page 56).
11. After you have installed your AMS Device Manager application, SNAP-ON applications, and communication interfaces, open AMS Device Manager, right-click each of the network icons, and select **Rebuild Hierarchy** followed by **Scan | New Devices**.

During installation, the **AMSDeviceManager** group is given write access to the AMS folder, subfolders, and files with all the permissions necessary to start and operate AMS Device Manager. Administrative privileges are required to add Windows User IDs to this group to allow operation of AMS Device Manager (see “Adding a user to the AMSDeviceManager group” on page 54).

The installation creates a share of the AMS folder which grants the **Everyone** group Full Control permissions. 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.

Client SC

The following steps install the Client SC Station software on other supported DeltaV stations in the network.

- ▶ To install Client SC Station software:
1. Clear all applications from the Windows Startup folder until after installation is finished. Exit/close all Windows programs including any running in the background (such as virus scan software).
 2. Insert the AMS Device Manager program DVD in the DVD drive of your PC.
 3. When the AMS Device Manager setup starts, click **Install AMS Device Manager**.

Note

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.

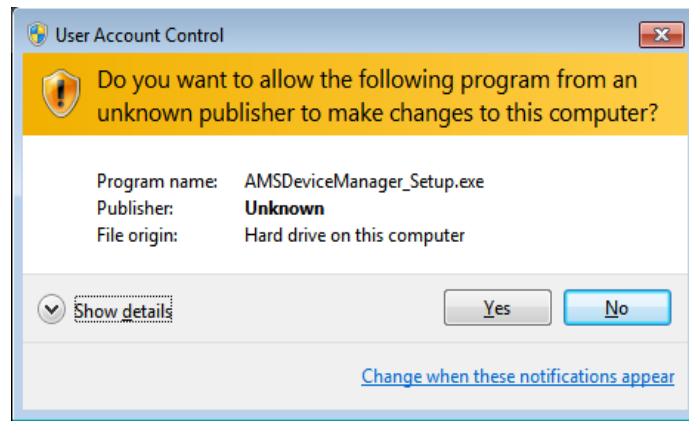
4. Click **Client SC Station**.
5. Follow the prompts.

NOTICE

Do not interrupt the installation process, otherwise 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 Windows Vista/7 or Windows Server 2008 PC, and User Account Control (UAC) is enabled, the User Account Control dialog box (similar to below) 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**.

Note

If you install a Client SC Station on a DeltaV 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.

6. Set up and configure any required communication interfaces, including the DeltaV Network System Interface (see “Configuring communication interfaces” on page 79).
-

Note

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

7. Install the latest versions of any licensed SNAP-ON applications, if appropriate (see “Installing SNAP-ON applications” on page 56).
-

Note

If the ValveLink SNAP-ON for DeltaV is installed, it must be uninstalled and the AMS ValveLink SNAP-ON for AMS Device Manager installed (see “Installing SNAP-ON applications” on page 56 and AMS Device Manager Books Online). Information about migrating ValveLink SNAP-ON for DeltaV data is located in AMS ValveLink SNAP-ON Help.

8. After you have installed your AMS Device Manager application, SNAP-ON applications, and communication interfaces, open AMS Device Manager, right-click each network icon, and select **Rebuild Hierarchy** and then **Scan | New Devices**.

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.

9. License your AMS Device Manager distributed system (see “Licensing a Distributed System” on page 55).
10. Configure your AMS Device Manager distributed system (see “Configuring a Distributed System” on page 56).
11. Install necessary SNAP-ON applications (see “Installing SNAP-ON applications” on page 56).

DeltaV actions

After installing AMS Device Manager on a DeltaV Station as previously described, you must perform a download of the DeltaV workstation. Downloading a DeltaV 10.x or later workstation adds DeltaV database account users to the AMS Device Manager database and the Windows AMSDeviceManager group which makes them available to AMS Device Manager User Manager. Downloading a DeltaV 9.x workstation adds DeltaV users to the AMS Device Manager database, but the users must be manually added to the Windows AMSDeviceManager group. Contact your IT department for assistance.

Note

Each time a ProfessionalPLUS Station is downloaded, some DeltaV user permissions overwrite AMS Device Manager user permissions (System Administrator, Device Write, Device SIS Write, Device Assignment).

► To download the DeltaV Station:

1. Open DeltaV Explorer.
2. Expand the tree view to find the station.
3. Right-click the station icon and select **Download | Setup Data**.
4. Click **Yes** to confirm the station download. A window opens to show progress of the download operation.

5. When the download completes, click **Close**.
6. Open AMS Device Manager User Manager on the AMS Device Manager Server Plus to confirm users were downloaded.

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.

Uninstalling 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.

Uninstalling AMS Device Manager software

After you uninstall AMS Device Manager, the “DeltaVAdmin” user account is not automatically removed from all locations and must be manually removed:

- Open Windows Control Panel and select **Administration Tools | Computer Management | Local Users and Groups | Users**.
- Open Windows Control Panel and select **Administration Tools | Local Security Policy | Local Policies | User Rights Assignment | Log on as batch job**.

Licensing AMS Device Manager 11.1.1 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.

There are a number of licensing considerations when you install AMS Device Manager on an Ovation station. To ensure that your installation functions as you expect, please contact your Emerson Process Management 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 73.

Installing AMS Device Manager 11.1.1 on Ovation stations

AMS Device Manager 11.1.1 can be installed on Ovation 3.2 and newer stations as outlined on page 34. 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 deployment, the AMS Device Manager Server Plus software would be installed on the Ovation station that also has the Fieldbus Engineering Tool (FET) installed. AMS Device Manager Client SC software would be installed on other supported Ovation station types 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 “Licensing AMS Device Manager 11.1.1 on Ovation stations” on page 73).

Note

If you are installing AMS Device Manager on any domain controller stations, refer to “Installing AMS Device Manager on domain controllers” on page 63.

Server Plus

- To install Server Plus software on the Ovation station:
1. Exit/close all Windows programs, including any running in the background (including virus scan software).
 2. Insert the AMS Device Manager program DVD in the DVD drive of your PC.
 3. When the AMS Device Manager setup starts, click **Install AMS Device Manager**.

Note

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**.

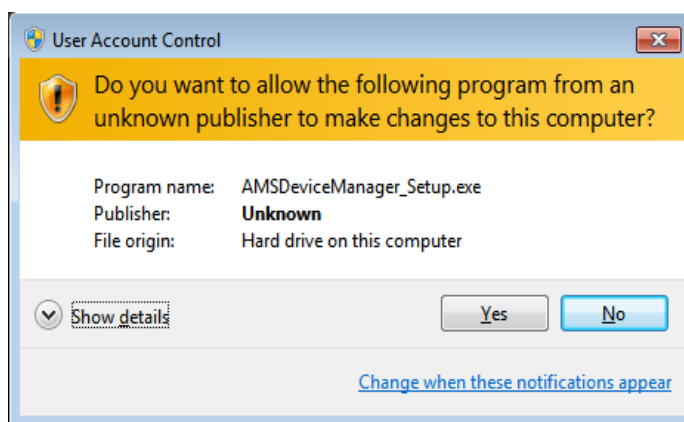
4. Click **Server Plus Station**.
5. Follow the prompts.

NOTICE

Do not interrupt the installation process, otherwise 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 Windows Vista/7 or Windows Server 2008 PC, and User Account Control (UAC) is enabled, the User Account Control dialog box (similar to below) 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**.

Note

All licensing for a distributed system is done on the Server Plus Station.

6. When the Licensing Wizard appears, click **Next** to obtain license codes or click **Cancel** if you are upgrading and do not need to relicense (see Table 1 on page 13). See “Licensing a Distributed System” on page 55.
 7. Set up the server configuration to recognize each station connected in the system (see “Configuring a Distributed System” on page 56). This step is essential for the other AMS Device Manager stations to access the Server Plus Station.
 8. Configure the Ovation Network System Interface (see “Configuring AMS Device Manager for an Ovation System Interface” on page 100) so that AMS Device Manager can detect and work with devices on the Ovation network.
-

Note

Do not configure an Ovation Network System Interface for the same Ovation system on more than one AMS Device Manager station.

9. Set up and configure any other required communication interfaces (see “Configuring communication interfaces” on page 79).
10. Install the latest versions of any licensed SNAP-ON applications, if appropriate (see “Installing SNAP-ON applications” on page 56).
11. After you have installed your AMS Device Manager application, SNAP-ON applications, and communication interfaces, open AMS Device Manager, right-click each of the network icons, and select **Rebuild Hierarchy** followed by **Scan | New Devices**.

During installation, the **AMSDeviceManager** group is given write access to the AMS folder, subfolders, and files with all the permissions necessary to start and operate AMS Device Manager. Administrative privileges are required to add Windows User IDs to this group to allow operation of AMS Device Manager (see “Adding a user to the AMSDeviceManager group” on page 54).

The installation creates a share of the AMS folder which grants the **Everyone** group Full Control permissions. 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.

Client SC

► To install Client SC Station software on an Ovation station:

1. Clear all applications from the Windows Startup folder until after installation is finished. Exit/close all Windows programs including any running in the background (such as virus scan software).
2. Insert the AMS Device Manager program DVD in the DVD drive of your PC.
3. When the AMS Device Manager setup starts, click **Install AMS Device Manager**.

Note

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**.

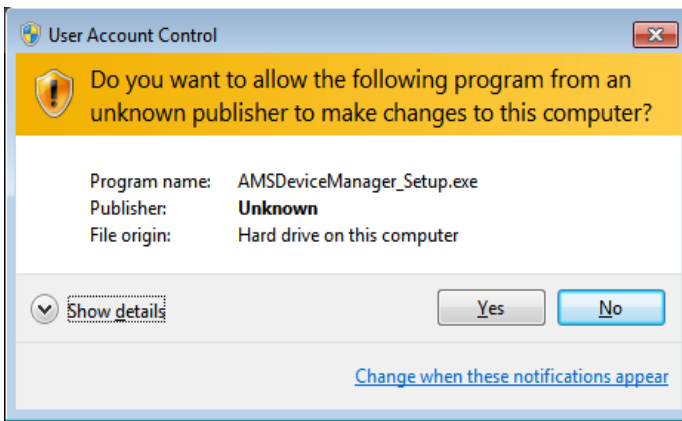
4. Click **Client SC Station**.
5. Follow the prompts.

NOTICE

Do not interrupt the installation process, otherwise 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 Windows Vista/7 or Windows Server 2008 PC, and User Account Control (UAC) is enabled, the User Account Control dialog box (similar to below) 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**.

Note

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.

6. Set up and configure any required communication interfaces, including the Ovation Network System Interface (see “Configuring communication interfaces” on page 79).
-

Note

Do not configure an Ovation Network System Interface for the same Ovation system on more than one AMS Device Manager station.

7. Install the latest versions of any licensed SNAP-ON applications, if appropriate (see “Installing SNAP-ON applications” on page 56).

-
8. After you have installed your AMS Device Manager application, SNAP-ON applications, and communication interfaces, open AMS Device Manager, right-click each network icon, and select **Rebuild Hierarchy** and then **Scan | New Devices**.

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.

9. License your AMS Device Manager distributed system (see “Licensing a Distributed System” on page 55).
10. Configure your AMS Device Manager distributed system (see “Configuring a Distributed System” on page 56).
11. Install necessary SNAP-ON applications (see “Installing SNAP-ON applications” on page 56).

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.

4 Configuring communication interfaces

AMS Device Manager communicates with HART, *WirelessHART*, FOUNDATION fieldbus, and PROFIBUS DP devices through various communication 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.

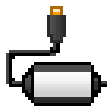
You need to configure the network interfaces that are relevant to each station. You should only configure a particular physical network on one station within the distributed network to avoid the potential for simultaneous device configuration.

This section describes how to configure for:

- HART modems (page 79)
- Field Communicators (page 83)
- HART communicators (page 85)
- Documenting calibrators (page 88)
- HART multiplexer networks (page 89)
- System interfaces (page 93)

This section provides general information about installing these interfaces. For specific information, refer to the manufacturers' documentation.

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 and do not require an external power supply. Bluetooth HART modems require a self-contained power source (AAA batteries) 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 (COM1 or COM2 only) 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 (see “Configuration notes” below).

Note

Only 1 modem can be configured on an AMS Device Manager station.

Configuring AMS Device Manager for a HART modem

- To configure for a HART modem:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **HART Modem** and click **Install**.
 4. Follow the prompts in the Add HART Modem Wizard.
 5. Connect a HART modem, see “Connecting a HART modem” on page 80.
 6. See “After a Modem is installed” on page 82.

Configuration notes

- If you select a multidrop installation, you can connect up to 16 devices on the same modem. However, if you intend to use only one device at a time, it will speed performance if you do not select the multidrop option and if you set all devices to a configurable polling address of 0.
- If any devices use a *WirelessHART* adapter, select the checkbox and enter the polling address of the adapter.
- Changes will take effect when AMS Device Manager is started.

Connecting a HART modem

NOTICE

If you are working with a modem on a workbench, ground your device to avoid possible damage to your PC.

- To connect a HART modem:
1. Establish a communication connection between the HART modem and your PC. Be sure you attach it to the port that you configured for it (see page 80).
 2. Tighten the thumbscrews (if present) to secure the connection between the modem and PC port.

3. Attach the HART devices. For many HART input devices (such as transmitters), you need to connect a 250 Ω to 300 Ω resistor in series with the power source. Be very careful when connecting an output device in a non-DCS loop configuration to avoid device damage. Always consult the device product manual for detailed connection information.

Note

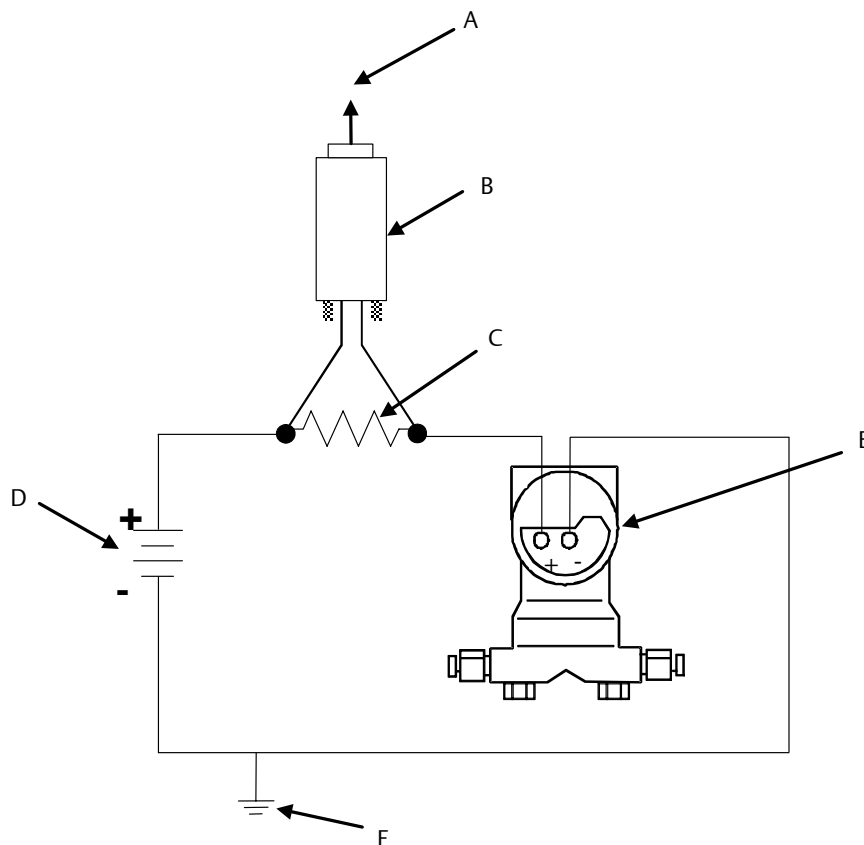
Follow output device manufacturers' recommendations for loop wiring.

4. Attach the modem leads across the resistor, if required.
5. Attach a power supply to the HART device, if necessary. Figure 1 shows how a HART device should typically be wired to a modem.
6. Verify that the transmitter has power.
7. After configuring the modem, reboot the PC to complete the installation.

Note

If a device is connected to the modem but its icon is not displayed, see "After a Modem is installed" on page 82.

Figure 1. Device Wiring Diagram



- A To PC COMM port connection
- B HART modem
- C 250 ohm resistor
- D 24vDC power source
- E Transmitter
- F Optional ground connection

After a Modem is installed

AMS Device Manager continuously polls the modem connection and automatically recognizes a device once the device and modem are installed.

AMS Device Manager shows the installed device connected to the modem after you have completed the procedure on page 80. If you do not see the device, do the following:

- Check your connections again.
- Make sure the modem is properly installed.

- Make sure the modem is properly configured in AMS Device Manager.
- Make sure the device loop wiring is correct with the required resistance for input devices (nominal 250 - 300 ohms).
- Verify that the field device is working.
- Verify polling address.

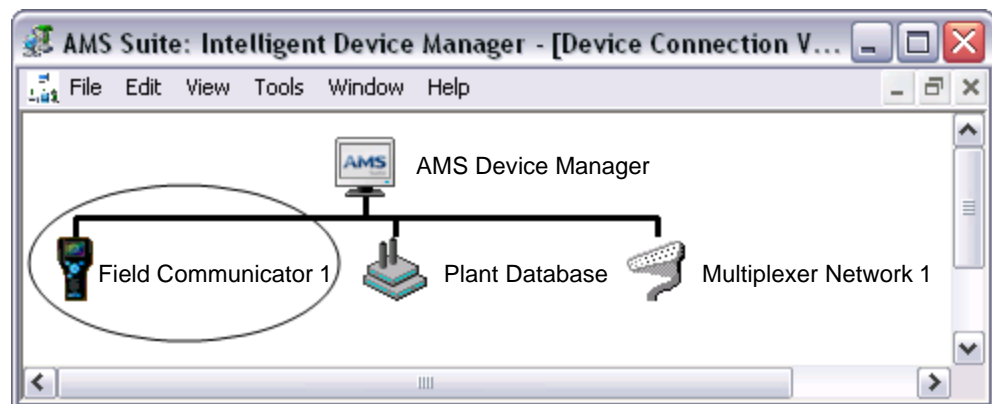
Field Communicators



The 475 and 375 Field Communicators are portable, handheld communicators from Emerson Process Management used in the field or in the shop to configure, test, and diagnose HART and FOUNDATION fieldbus devices. For information on using the 475 or 375, refer to the user's manual that came with your Field Communicator.

The Handheld 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. 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. Once the Field Communicator is configured in the network, you can see its icon (Figure 2).

Figure 2. Field Communicator icon in Device Connection View



Configuring AMS Device Manager for a Field Communicator

- ▶ To configure AMS Device Manager for a Field Communicator:
 1. Close AMS Device Manager if it is running.
 2. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 3. In the Network Configuration dialog box, click **Add**.
 4. In the Select Network Component dialog box, select **Field Communicator** and click **Install**.
 5. Follow the prompts in the Add Field Communicator Network Wizard.
 6. In the Connection dialog box, select the appropriate Field Communicator connection option.

The IrDA adapter is a plug-and-play interface, so you do not need to specify a communications port. The Bluetooth interface requires use of the Microsoft Bluetooth components and an adapter if your PC is not Bluetooth-ready (see the Release Notes for a list of supported Bluetooth adapters). If you have Bluetooth components from another provider installed, you will be instructed to use Microsoft Bluetooth components. For more information, see AMS Device Manager Books Online. Bluetooth is not natively supported in Windows Server 2003/2008.

Connecting a Field Communicator

- ▶ To connect a Field Communicator:
 1. Ensure that your network has been configured for a Field Communicator (see page 84).
 2. Ensure that an IrDA adapter (and drivers, if necessary) or Bluetooth components (and adapter, if necessary) are installed on the PC. Refer to your IrDA interface operating instructions. See the Release Notes for a list of supported IrDA and Bluetooth adapters.
 3. If using an IrDA adapter align it with the IrDA interface on the field communicator. If using Bluetooth connectivity, follow the instructions supplied with your PC or Bluetooth adapter hardware.
 4. Turn on the Field Communicator.

5. From the Field Communicator Main Menu, select **Listen For PC** mode and the correct connection type and tap **OK**. After making these selections, AMS Device Manager will conduct all interaction between the Field Communicator and the PC.
6. Launch AMS Device Manager.
7. Double-click the Field Communicator icon in AMS Device Manager or right-click the icon and select **Open** from the context menu.

Note

You cannot access live device data through a Field Communicator connected to AMS Device Manager.

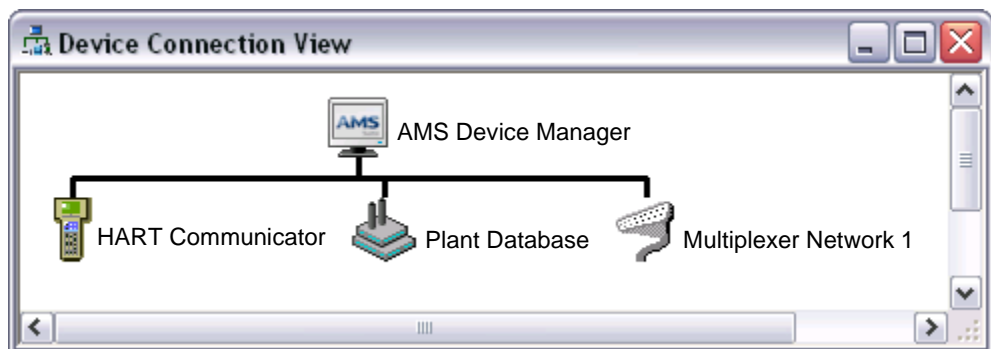
See AMS Device Manager Books Online for more information about connecting and using a Field Communicator with AMS Device Manager. For general information on using the 375 or 475 Field Communicators, refer to the user's manual that came with your Field Communicator.

Model 275 HART Communicator



The Handheld Communicator Interface is a licensable option that lets you transfer HART data between a Model 275 HART Communicator and the database using a communication adapter and serial cable. Communication between AMS Device Manager and a connected HART Communicator is initiated by the AMS Device Manager software. Once the HART Communicator is configured in the network, you can see its icon in AMS Device Manager (Figure 3).

Figure 3. HART Communicator Icon in Device Connection View



For general information on using the communicator, refer to your *HART Communicator Manual*.

Configuring AMS Device Manager for a HART Communicator

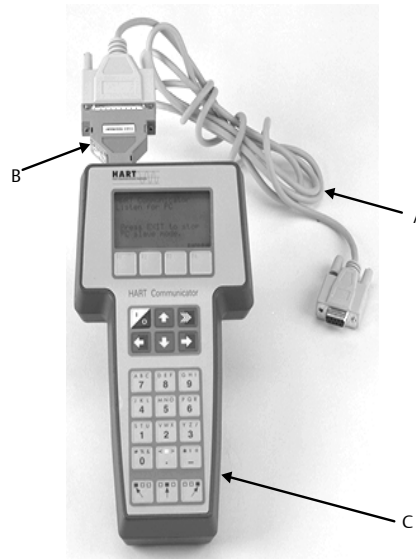
- To configure for a HART Communicator:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component dialog box, select **HART Communicator** and click **Install**.
 4. Follow the prompts in the Add HART Communicator Wizard.
 5. When finished, verify that the correct COM port is assigned by selecting the HART Communicator name in the Network Configuration dialog box and clicking **Properties**. If necessary, change the COM port in the Properties for the HART Communicator dialog box.

Connecting a HART Communicator to AMS Device Manager

To work properly, your HART Communicator must be at module revision level 3.6 or higher. When you turn on the Communicator, the revision level is displayed briefly. To see the revision level at other times, select **Utility | System Information | Module | Software | OS Revision** from the Communicator menus.

To upgrade your HART Communicator operating system software, contact your Emerson Process Management Sales/Service Office.

- To connect a HART Communicator to AMS Device Manager using the Handheld Communicator Interface Kit:
1. Make sure your network has been configured for a HART Communicator (see above).
 2. Plug the Communication Adapter (included with the Handheld Communicator Interface Kit) into the 9-pin serial port on the rear connection panel of HART Communicator.
 3. Plug the 25-pin serial port cable into the other end of the Communication Adapter (Figure 4).

Figure 4. HART Communicator connections

- A Serial cable
B Communication adapter
C HART Communicator

4. Connect the serial port cable to an available serial port on the back of the PC. (Depending on the PC to which you are connecting, you must have either a 9-pin or a 25-pin plug on the end of the cable that connects to the PC. Use a foil-shielded 9- to 25-pin communication adapter if required.)

Be sure you connect the cable to the COM port you selected when you configured the network.

5. Turn on the HART Communicator and set it to Listen for PC. (From the Communicator Offline Menu, select **Utility | Listen for PC.**) Once this option is set, AMS Device Manager will conduct all interaction between the HART Communicator and the PC.
6. Start AMS Device Manager. The HART Communicator icon appears in AMS Device Manager.
7. Right-click the HART Communicator icon to see its context menu.

See AMS Device Manager Books Online for more information about using the HART Communicator with AMS Device Manager. For general information on using the HART Communicator, see your *HART Communicator Product Manual*.

Note

You cannot access live device data through a HART Communicator connected to AMS Device Manager.

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.

Refer to the current Release Notes for a list of supported documenting calibrators and pertinent information about individual calibrators.

Configuring AMS Device Manager for a documenting calibrator

► To configure AMS Device Manager for a documenting calibrator:

1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
2. In the Network Configuration dialog box, click **Add**.
3. In the Select Network Component Type dialog box, select **Calibrator** and click **Install**.
4. Follow the prompts in the Add Calibrator Wizard.
5. When finished, verify that the correct COM port is assigned by selecting the calibrator name in the Network Configuration dialog box and clicking **Properties**. If necessary, change the COM Port on the Properties for the Calibrator dialog box.

Connecting a documenting calibrator

For instructions on how to connect the calibrator to the PC, see the calibrator documentation.

Connecting devices to a documenting calibrator

For instructions on how to connect devices to the documenting calibrator, see the calibrator documentation.

HART Multiplexer Network Interface



With the optional HART Multiplexer Network Interface, AMS Device Manager can communicate with HART devices through a HART multiplexer. HART multiplexers can link many installed HART field devices to an AMS Device Manager PC, 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 31 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. For a list of supported multiplexers, see the Release Notes. For specific information about a supported multiplexer, see the manufacturer's documentation.

Note

This information refers to Arcom, Elcon, 8000 BIM, Spectrum Controls, Honeywell, and Pepperl+Fuchs multiplexers. STAHL multiplexer interfaces are described on page 40.

NOTICE

For the PC to communicate with a HART multiplexer, you must place either an RS-232 to RS-485 converter or a supported ethernet serial hub between the multiplexer and the PC. For supported peripherals, see the Release Notes.

Preparing a HART Multiplexer Network Interface

Preparing a HART multiplexer interface includes:

- Connecting the multiplexer(s) to the PC
- Configuring AMS Device Manager for a multiplexer network
- Setting the HART master mode and the multiplexer gender settings
- Connecting the field devices to the multiplexers

Connecting a HART multiplexer to a PC

To connect a HART multiplexer to AMS Device Manager, refer to the multiplexer documentation.

Configuring AMS Device Manager for a HART Multiplexer Network

- To configure AMS Device Manager for a HART multiplexer network:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **Multiplexer Network** and click **Install**.
 4. Follow the Multiplexer Network Wizard instructions to add the HART multiplexer network.

Configuration notes

- Select the appropriate PC communications port.
- If necessary, adjust the Baud Rate, Network Timeout, Communication Retries, HART Busy Retries, and Multiplexer address range. See AMS Device Manager Books Online for the Connection dialog box for more information.
- Select the appropriate HART Master Mode setting. This parameter setting must be the same for all multiplexers on the network.

Note

You can connect up to 31 multiplexers on the same network. You can improve network performance by limiting the range to the minimum value that includes the multiplexer addresses and configuring the multiplexers to use a range of consecutive addresses.

NOTICE

After completing the configuration, verify that the baud rates match in AMS Device Manager, the multiplexer, and the RS-232 to RS-485 converter. To change the baud rate for a multiplexer network in AMS Device Manager, select its name in the Network Configuration dialog box and click Properties. Enter the correct baud rate and click Apply.

For more information about multiplexer networks, refer to KBA NA-0400-0084.

Setting multiplexers as Primary or Secondary Masters

Check the properties of each multiplexer in AMS Device Manager to be sure the gender settings match the HART Master Mode setting in Network Configuration.

NOTICE

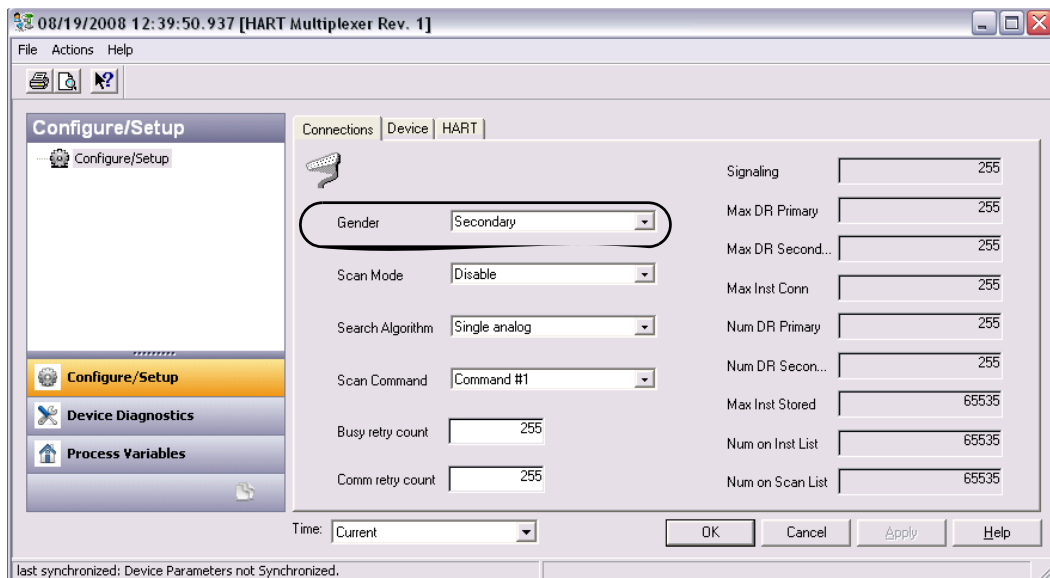
Do not configure two HART Primary masters (such as AMS Device Manager and a control system)—this is an invalid setting and can produce unpredictable results.

- To set a multiplexer gender as Primary or Secondary:
1. Right-click the multiplexer icon.
 2. Select **Configure/Setup** from the context menu.
 3. Set the Gender field (Figure 5) as needed for the type of multiplexer.
 4. Click **OK**.

Note

The Multiplexer Network and all associated multiplexers must have matching gender settings. Otherwise, AMS Device Manager may not function as expected.

Figure 5. Multiplexer configuration



Connecting a field device to a HART multiplexer

Connecting a device to a HART multiplexer involves:

- Physical wiring.
- A multiplexer power cycle, rebuild loop operation, or reset operation to update the device connection in the multiplexer.
- A Rebuild Hierarchy and Scan New Devices operation in AMS Device Manager to identify the device connections and update the display of the appropriate icons in AMS Device Manager.

Note

If you initiate a Scan New Devices operation before a multiplexer recognizes that a device has been added, an inaccurate or incomplete list of devices may be displayed.

► To connect a HART device to a multiplexer:

1. Connect the device(s) to a loop on the HART multiplexer.
For instructions, refer to the appropriate hardware product documentation. Generic wiring diagrams are available in AMS Device Manager Books Online.
2. After you have connected all desired devices to the multiplexer, start AMS Device Manager.
3. Reset the multiplexer by doing one of the following:
 - Power off the multiplexer and then power it back on.
 - Right-click the multiplexer icon and select **Methods | Diagnostics and Test | Reset**.
4. Right-click the multiplexer network icon and select **Rebuild Hierarchy**.

This enables AMS Device Manager to show the network hierarchy and all connected devices.

The Rebuild Hierarchy operation updates information about the network structure by querying the connected multiplexers. If it finds multiple multiplexers or field devices having the same device identifier, it may display the duplicate device icon (see figure at right) to represent such devices.



AMS Device Manager cannot properly communicate with a multiplexer network that contains duplicate devices. To correct this condition, you must physically remove one of the duplicate devices, reset the multiplexer or perform a Rebuild Loop operation, and then perform another Rebuild Hierarchy operation followed by a Scan New Devices operation. Because a duplicate device identifier is an abnormal condition in the device, any occasion should be reported to the device manufacturer.

Note

AMS Device Manager may not detect all duplicate device conditions. If you see an undetected duplicate device condition, report it to the device manufacturer.

5. Right-click the multiplexer network icon and select **Scan | New Devices**.


This causes AMS Device Manager to read the updated device information into the database.

Note

If a Scan New Devices operation is not performed when appropriate (such as after a Rebuild Hierarchy operation), some AMS Device Manager operations will be slower.

Perform step 3 through step 5 for other types of loop changes, such as removing or replacing devices.

Nonresponding device icon

A nonresponding device icon  in the multiplexer hierarchy indicates AMS Device Manager is currently unable to communicate with a device attached to a multiplexer network. Possible reasons for a nonresponding device:

- A problem with the wiring between the device and the multiplexer, or device loop wiring.
- A device problem.

System interfaces

With an optional system interface, AMS Device Manager can communicate with devices through existing plant wiring. Each system interface is licensed and installed separately, and each has unique characteristics and works somewhat differently with AMS Device Manager.

AMS Device Manager provides system interfaces for the following systems:

- Wireless (see page 94)
- DeltaV™ (see page 96)
- Ovation™ (see page 99)
- FF HSE (see page 103)
- ROC (see page 103)
- PROVOX (see page 104)

- RS3™ (see page 107)
- STAHL (see page 109)
- 8000 BIM (see page 111)
- HART Over PROFIBUS (see page 112)
- Kongsberg Maritime (see page 114)
- Siemens (see page 115)

Wireless



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

Configuring AMS Device Manager for a Wireless Network

- ▶ To configure AMS Device Manager for a Wireless Network:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **Wireless Network** and click **Install**.
 4. Follow the Add Wireless Network Wizard instructions. Enter the DNS Name or IP address of a gateway and click **Add**.
 5. If this is the first time a gateway has been configured, a Certificate Form is displayed. The Certificate Form is required to set up SSL secure communications. After the Certificate Form is completed, the gateway will be added to the Connections Properties page.
 6. If required, enter the username and password to access the gateway's setup utility. Then enter information to allow the gateway and AMS Device Manager to exchange encrypted data.
 7. Start AMS Device Manager. See "Determining the system interface structure and device data" on page 115.
 8. For more information about using a Wireless Network, see AMS Device Manager Books Online.

Adding a gateway

For a list of supported wireless gateways, refer to the AMS Device Manager Release Notes. Do not configure a Wireless System Interface if a DeltaV or Ovation System Interface will be using the same wireless gateway.

Note

The same wireless gateway cannot be configured in two different Wireless Networks on a single workstation.

- To add a wireless gateway to a Wireless Network:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. Select a Wireless Network and click **Properties**.
 3. Click the **Connection** tab.
 4. Enter the name or IP address of the gateway and click **Add**.
 5. If required, enter the username and password to access the gateway's setup utility. Then enter information to allow the gateway and AMS Device Manager to exchange encrypted data.
 6. Click **OK**.
 7. Click **Close**.
 8. Start AMS Device Manager. See "Determining the system interface structure and device data" on page 115.

Note

Optional SSL encryption software is available from Emerson to secure wireless communication with the gateway.

Removing a gateway

- To remove a wireless gateway from a Wireless Network:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. Select a Wireless Network and click **Properties**.
 3. Click the **Connection** tab.
 4. Select the appropriate gateway in the list and click **Delete**.

5. Click **Yes**.
6. Click **Close**.
7. Start AMS Device Manager. See “Determining the system interface structure and device data” on page 115.

DeltaV



A DeltaV control network is an isolated Ethernet 10BaseT 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 30.

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 and documentation.

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.

▶ To run the utility:

1. Select **Start | Run** from the Windows taskbar.
2. In the text box, type `C:\AMS\BIN\DELTAVFASTSCANUTILITY.EXE` (where C is the drive containing the AMS folder).
3. Uncheck the box for the appropriate DeltaV network.
4. Click **Save Changes**.

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

Preparing the DeltaV system

To prepare a DeltaV control system to communicate with a standalone 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.
- Verify that the DeltaV node responds to a ping command from the AMS Device Manager PC (see “Verifying DeltaV node response” on page 97).
- 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.

Verifying DeltaV node response

► If AMS Device Manager is installed on a remote station or PC, use the ping command to verify that the DeltaV node responds to communications sent to it by AMS Device Manager:

1. At the station or PC where AMS Device Manager is installed, open a DOS command prompt (**Start | All Programs | Accessories | Command Prompt**).
2. At the DOS prompt, type PING <DeltaV Node Name>.
3. Press ENTER.
4. Verify that the DeltaV node responds to the ping command. The ping command should return a reply message.
5. If the ping command fails, verify that you typed the correct Node Name in the command line. Also verify that your network is functioning properly. Installation is complete only after you receive a valid ping reply.

Configuring AMS Device Manager for a DeltaV System Interface

- To configure AMS Device Manager for a DeltaV System Interface:

Note

You must only configure the DeltaV Interface on a licensed AMS Device Manager station. Computer administrator privileges are required to install a DeltaV Interface.

Do not configure a DeltaV Interface to the same DeltaV ProfessionalPLUS on more than one AMS Device Manager station in a distributed system.

Ensure that all stations in the AMS Device Manager distributed system are running when you configure the DeltaV System Interface.

1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
2. In the Network Configuration dialog box, click **Add**.
3. In the Select Network Component Type dialog box, select **DeltaV Network** and click **Install**.
4. Click **Next**.
5. On the **General** dialog box, enter a name for the DeltaV Network. Click **Next**.
6. On the **Connection** dialog box, enter the computer name of the DeltaV ProfessionalPLUS Station.
7. Enter the DeltaVAdmin password and password confirmation, if it has been changed from the default.

Note

The DeltaVAdmin password is an administrative password given to each DeltaV system. The same password must be used to access all DeltaV networks configured on this station. If no password is entered, a connection will be attempted using the default DeltaV password.

8. Select the options to enable HART, FOUNDATION fieldbus, *WirelessHART* and PROFIBUS DP device support, as needed.
9. Click **Next**.
10. On the **Advanced** tab, enter a high address for the PROVOX I/O Scan Range if your DeltaV system uses a PROVOX migration controller.
11. Click **Finish** to save the configuration.

12. Click **Close**.
13. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

If you have multiple DeltaV Zones which include additional Server Plus Stations, the Server Plus Connect utility lets you access those other Server Plus Stations from a Client SC Station. For more information, see the AMS Device Manager Books Online.

To install AMS Device Manager on a DeltaV network, refer to “Installing AMS Device Manager 11.1.1 on DeltaV stations” on page 65.

Ovation



The Ovation System Interface lets AMS Device Manager communicate with HART, FOUNDATION fieldbus, and *WirelessHART* 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 to the Ovation controller through a fieldbus gateway device. *WirelessHART* 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 a Fieldbus Engineering Tool (FET) installed on and 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.

Note

AMS ValveLink Diagnostics for the DVC6000f may not work with Ovation. Contact Ovation for a possible modification to support the DVC6000f.

Note

Installation of AMS Device Manager on an Ovation database server is not supported.

Preparing the Ovation system

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

Configuring AMS Device Manager for an Ovation System Interface

You can configure the AMS Device Manager Ovation System Interface on a standalone AMS Device Manager station (that is, without Ovation software). You can also install AMS Device Manager Server Plus software on an Ovation Operator or Engineering Station and set up the Ovation System Interface using AMS Device Manager Network Configuration utility. If AMS Device Manager is installed on an Ovation Engineering Station that also has FET installed, you can right-click a FOUNDATION fieldbus device and select from a set of AMS Device Manager commands. Your Ovation username must also be an AMS Device Manager user with Device Write and Device SIS Write permissions.

When you configure the Ovation System Interface on an Ovation Operator Station, HART, *WirelessHART*, and FOUNDATION fieldbus devices are supported. On a standalone PC, only HART and *WirelessHART* devices are supported. You can either use the Ovation Database Server as your network gateway to access HART devices or set up a network route. Communication with *WirelessHART* devices is enabled through a Smart Wireless Gateway. For communicating with FOUNDATION fieldbus devices, Ovation FOUNDATION fieldbus communication tools must be installed locally on the same machine as AMS Device Manager.

► To set up a network route:

1. Select **Start | All Programs | Accessories | Command Prompt** from the Windows taskbar.
2. Type in: "route -p add <controller> mask 255.255.255.0 <Ovation DB Server> metric 1".

Where <controller> is the TCP/IP address of the controller and <Ovation DB Server> is the TCP/IP address of the database server. In both addresses, change the last number to 0. For example, if the controller address is 123.123.123.1, the address in the route should be 123.123.123.0.

3. Close the Command Prompt window.

► To configure AMS Device Manager for an Ovation interface:

1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
2. In the Network Configuration dialog box, click **Add**.
3. In the Select Network Component Type dialog box, select **Ovation Network** and click **Install**.
4. Click **Next**.
5. In the General dialog box, enter a name for the Ovation Network. Click **Next**.

6. In the Connection dialog box, enter the name of the computer on the Ovation Network that contains the Ovation system Oracle database. If you do not want Ovation FOUNDATION fieldbus devices to be accessible in AMS Device Manager, clear the **Enable Fieldbus Device Support** checkbox. If you want Ovation FOUNDATION fieldbus devices to be accessible in AMS Device Manager, but do not want FOUNDATION fieldbus device alerts recorded or displayed in AMS Device Manager, leave the **Enable Fieldbus Device Support** checkbox selected and clear the **Enable Fieldbus Device Alert Support** checkbox. If the Ovation OPC Alarm and Event Server option is not installed on the Ovation system, FOUNDATION fieldbus device alert support should not be enabled. Select the **Enable Wireless HART Support** checkbox and add the IP address of the Smart Wireless Gateway to enable communication with *WirelessHART* devices.

Note

You cannot enable FOUNDATION fieldbus access for more than one Ovation network on an AMS Device Manager station.

7. The data fields in the Timings dialog box contain default values which you cannot change. Click **Help** for more information about the fields on this dialog box.
8. Click **Finish** to complete the Ovation Network interface setup.
9. Click **Close**.
10. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

Note

You must have computer administrator privileges to install an Ovation network.

Note

If you install both the Ovation System Interface and the FF HSE Interface on the same PC, you must configure each on a unique IP address.

FF HSE



The FF HSE Interface lets you use AMS Device Manager to configure and view alerts for FOUNDATION fieldbus devices connected to FOUNDATION fieldbus linking devices (such as the Rosemount 3420, the ROC for FOUNDATION fieldbus devices, and the ControlWave linking devices).

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 Rosemount 3420 linking device, a ROC FF linking device, or a ControlWave 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.

Configuring AMS Device Manager for an FF HSE Interface

- To configure AMS Device Manager for an FF HSE Interface:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **FF HSE Network** and click **Install**.
 4. Click **Next**.
 5. Follow the HSE Network Wizard instructions. Choose the network interface card that will be connected to the same network as the HSE linking device.
 6. Select the **Enable processing and acknowledgement of FF device alerts** checkbox to display device alerts in Alert Monitor and record alerts in Audit Trail.

7. Click **Finish** to save the configuration.
8. Click **Close**.
9. Start AMS Device Manager. See “Determining the system interface structure and device data” on page 115.

Note

If you install both the FF HSE Interface and the Ovation System Interface (with fieldbus devices enabled) on the same PC, you must configure each on a unique IP address.

ROC



The Remote Operations Controller (ROC) Interface lets you use AMS Device Manager to view and configure HART and *WirelessHART* devices connected to remote operations controllers.

Installing and configuring the ROC Polling Services

- ▶ Before configuring AMS Device Manager for a ROC network, you must install the ROC polling services as well as the Smart Wireless User Program (if you are using *WirelessHART* devices) on the AMS Device Manager station on which the ROC network is to be installed, and then do the following:

Note

ROC polling services will not install if the AMS Device Manager database password is not the default database password.

1. Launch the ROC Polling Service Manager by selecting **Start | All Programs | Emerson Process Management | Flow Computer Division | ROC Polling Manager**.
2. Add the ROCs and/or ROC field servers to the ROC Polling Service Manager. Do not use `?`, `*`, `\`, `|`, `'`, `"`, or `!` characters in the ROC controller name.

To obtain the required ROC polling services and the Smart Wireless User Program, contact your Emerson Process Management Sales/Service Office.

Note

ROC polling services is not supported on Windows Vista/7/2008. You must use Windows XP/2003.

Configuring AMS Device Manager for a ROC Interface

- ▶ To configure AMS Device Manager for a ROC Interface for HART:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **ROC Network** and click **Install**.
 4. Follow the ROC Network Wizard instructions.
 5. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

Note

To configure a ROC for FOUNDATION fieldbus devices, refer to the FF HSE interface information (“FF HSE” on page 38).

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.

Note

The AMS ValveLink SNAP-ON application is not supported.

Preparing 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 below).
- Verify that the HDL responds (see page 106).

Generating and transferring 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 “Configuring AMS Device Manager for a PROVOX Interface” on page 106).

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 program DVD.

2. Copy the HLT file from the ENVOX PC to the AMS folder on your AMS Device Manager PC, using file transfer protocol (FTP).

Verifying HDL response

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

1. At the AMS Device Manager PC, select **Start | Run** from the Windows taskbar.
2. In the text box, type CMD and click **OK** to open a DOS command prompt.
3. At the DOS prompt, type 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.

4. Press ENTER.
5. 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 typed 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.

Configuring AMS Device Manager for a PROVOX Interface

- ▶ To configure AMS Device Manager for a PROVOX network interface:

1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
2. In the Network Configuration dialog box, click **Add**.
3. In the Select Network Component Type dialog box, select **PROVOX Network** and click **Install**.
4. Follow the PROVON Network Wizard instructions.
5. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

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).

Preparing 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 “Verifying communication with the RNI” on page 108).
- Verify that the RNI responds.

Setting RNI username and password

► To set up a username and password for the system interface on your RNI:

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.

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>
>
>
```

Note

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.

Note

AMS ValveLink SNAP-ON application is not supported.

3. Save and close USERFILE.CFG.

Verifying communication with the RNI

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

1. At the **AMS Device Manager PC**, open a DOS command prompt (**Start | All Programs | Accessories | Command Prompt**).
2. At the DOS prompt, type `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.
5. If the ping command fails, verify that you typed the correct address in the command line. Also verify that your network is functioning properly.

Note

Your installation is complete only after you receive a valid ping reply.

Configuring AMS Device Manager for an RS3 Interface

- ▶ To configure AMS Device Manager for an RS3 interface:
 1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **RS3 Network** and click **Install**.
 4. Follow the RS3 Network Wizard instructions.
 5. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

STAHL HART



A STAHL HART 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.

Preparing the STAHL system

No additional steps are needed to prepare the STAHL network for communication with AMS Device Manager. After configuring the STAHL HART interface, AMS Device Manager scans the STAHL network to determine its configuration and connected HART devices. Refer to the STAHL documentation for device connection and network setup instructions.

Configuring AMS Device Manager for a STAHL HART Interface

- ▶ To configure AMS Device Manager for a STAHL network interface:
 1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. In the Network Configuration dialog box, click **Add**.
 3. In the Select Network Component Type dialog box, select **Stahl Network** and click **Install**.

4. Follow the prompts in the Add Stahl Network Wizard (see “Configuration notes” on page 110).
5. Start AMS Device Manager to determine the network structure. See “Determining the system interface structure and device data” on page 115.

Configuration notes

- The STAHL network may need to be set to Secondary HART Master if the control system is set to Primary HART Master.

Note

The HART master selection for HART multiplexers, as shown in their Configuration Properties, must match this setting (see “Setting multiplexers as Primary or Secondary Masters” on page 91).

NOTICE

Do not configure two HART primary masters (such as AMS Device Manager and a control system)—this is an invalid setting and can produce unpredictable results.

- In the Connection dialog box, select the communications port of the PC to which you are going to attach the STAHL Network. If necessary, adjust the Baud Rate and Device timeout value. See AMS Device Manager Books Online for details. Click **Next**.
- In the Advanced dialog box, adjust the RS-485 scan address range. To optimize performance, set the address range to include only the addresses where systems are located.
- To verify the baud rate or other information, select the STAHL Network name in the Network Configuration dialog box and click **Properties**. If necessary, change the information shown on the three tabs.
- Changes will take effect when AMS Device Manager is restarted.

8000 BIM



The 8000 BIM interface displays HART field devices connected to an 8000 BIM by means of either:

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

Configuring AMS Device Manager for an 8000 BIM Interface

► To configure AMS Device Manager for an 8000 BIM interface:

1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
2. In the Network Configuration dialog box, click **Add**.
3. In the Select Network Component Type dialog box, select **8000 BIM Network** and click **Install**.
4. Follow the 8000 BIM Network Wizard instructions.
5. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

If no icons are displayed under the 8000 BIM network icon after a Rebuild Hierarchy operation, perform the appropriate procedure for your operating system:

► For Windows XP/Windows Vista/7 or Windows Server 2003/2008:

1. (XP/2003) Select **Start | All Programs | Accessories | Communications | Network Connections**.
(Windows Vista/7/2008) Select **Start | Settings | Network Connections**.
2. Select **Advanced | Advanced Settings** from the Network Connections toolbar menu.
3. Under Connections, move the Ethernet card connected to the 8000 BIM network to the first spot in the network connection order.
4. Click **OK**.
5. Reboot the PC.

Note

If AMS Device Manager is unable to detect the eBIMs, change the order of the network adapters in the station Network Properties so the Network Interface Card (NIC) connected to the 8000 BIM system is listed first. Then restart the PC.

HART Over PROFIBUS



The HART Over PROFIBUS System Interface lets you use AMS Device Manager to view and configure HART Rev. 5 or HART Rev. 6 field devices that are connected to PROFIBUS remote I/O subsystems via the T+H PROFIBUS Gateway. The T+H PROFIBUS Gateway comes in two basic hardware configurations: Ethernet PROFIBUS Interface (xEPI) and PCMCIA. The interface addresses the gateway by either its DNS or IP address.

The HART Over PROFIBUS System Interface supports the AMS ValveLink SNAP-ON application if using a compatible PROFIBUS remote I/O subsystem.

Preparing the PROFIBUS remote system

Refer to the documentation specific to your PROFIBUS remote I/O subsystem for device connection and network setup instructions.

Configuring AMS Device Manager for a HART Over PROFIBUS Interface

- To configure AMS Device Manager for a HART Over PROFIBUS Interface:
1. Close AMS Device Manager if it is running.
 2. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 3. Click **Add**.
 4. From the Select Network Component Type dialog box, select **HART Over PROFIBUS** and click **Install**.
 5. Follow the HART Over PROFIBUS Network Wizard instructions.
 6. Start AMS Device Manager to set up the network structure. See “Determining the system interface structure and device data” on page 115.

Note

Refer to the Release Notes if all your devices are not displayed after performing a Rebuild Hierarchy and Scan New/All operation.

Refer to the *TH AMS Device Manager Communication Components HART Over PROFIBUS User Guide* on AMS Device Manager installation DVD for more information.

Kongsberg Maritime



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 Network is deployed where there is access to the Kongsberg Automation Server with IIS. It is not necessary to install the Kongsberg Automation Server on an AMS Device Manager station, however, communications performance is better with this deployment type. For deployment scenarios that require AMS Device Manager Client Stations to cross External Firewalls, refer to KBA NA-0400-0046.

If you install additional Kongsberg Networks, they must be linked to unique Automation Server URLs. The Kongsberg Network supports communications with HART instruments connected to STAHL ISpac HART Multiplexers and STAHL PROFIBUS DP Remote I/O modules for HART. The Kongsberg Interface supports Advanced Valve Diagnostics using the AMS ValveLink SNAP-ON application.

Configuring AMS Device Manager for a Kongsberg System Interface

- To configure AMS Device Manager for a Kongsberg System Interface:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. Click **Add**.
 3. In the Select Network Component Type dialog box, select **Kongsberg Network** and click **Install**.
 4. Follow the Kongsberg Network Wizard instructions.
 5. Choose the Kongsberg Automation Server URL. The URL connection to the Automation Server is tested and if not found, a corresponding message is displayed.
 6. If the URL connection is found, click **Finish**.
 7. Close the Network Configuration dialog box.
 8. Start AMS Device Manager. See “Determining the system interface structure and device data” on page 115.

Preparing the Kongsberg control system

Refer to the Kongsberg Maritime system documentation for setup instructions.



Siemens

The Siemens System Interface lets you use AMS Device Manager to communicate with HART devices on a Siemens PCS 7 Control Network. An AMS Device Manager Server Plus Station or Client SC Station must be installed on the same station as the Siemens PCS 7 ES/MS Station. The AMS Device Manager Network Configuration utility is used to configure the Siemens network interface.

Configuring AMS Device Manager for a Siemens System Interface

- To configure AMS Device Manager for a Siemens System Interface:
1. Select **Start | All Programs | AMS Device Manager | Network Configuration** from the Windows taskbar.
 2. Click **Add**.
 3. In the Select Network Component Type dialog box, select **Siemens Network** and click **Install**.
 4. Follow the Siemens Network Wizard instructions.
 5. Choose the **Rebuild Hierarchy Timeout** and **HART Response Timeout** values.
 6. Close the Network Configuration dialog box.
 7. Start AMS Device Manager. See “Determining the system interface structure and device data” on page 115.

For additional information, refer to the Siemens Control Network documentation.

Determining the system interface structure and device data

Rebuilding the hierarchy

At the first AMS Device Manager startup following the addition of a system interface, AMS Device Manager displays an icon representing the highest level of the system network hierarchy. When you double-click this icon, AMS Device Manager will direct you to initiate a **Rebuild Hierarchy** operation to populate the hierarchy with the appropriate levels and icons.

Reading device parameter data

After the initial Rebuild Hierarchy operation, AMS Device Manager displays the system interface hierarchy. The structure, however, does not yet contain parameter data for the connected devices. You must manually initiate a **Scan | New Devices** operation to read the device parameter data into the database.


- To initiate a scan for device data:
1. Right-click the top-level icon of the system interface hierarchy.
 2. Select **Scan | New Devices** from the context menu.

Note

The scan operation can take a long time, especially when performed at the highest level of the hierarchy.

During the initial **Scan | New Devices** operation, AMS Device Manager surveys the network to identify the devices it can communicate with. The operation also reads parameter data and updates the database.

Resolving a nonresponding device icon

A nonresponding device icon  indicates that AMS Device Manager is currently unable to communicate with a device attached to a host system. Typically, this condition occurs when the host system is improperly configured or a device is improperly wired. After correcting the problem, you can attempt to identify the device by initiating one of the following:

- Another **Scan | New Devices** operation
- An **Identify Device** operation followed by a **Scan Device** operation

If AMS Device Manager can identify the device following one of these operations, it will replace the nonresponding device icon with the appropriate device icon. Right-click the new device icon and select **Scan Device** to update the database with the parameters for that device.

If you removed the device from the host system, perform a Rebuild Hierarchy followed by a **Scan | New Devices** operation.

Most system interfaces have the ability to display nonresponding device icons. For those interfaces that do have this ability, you can configure the network to either display or not display the nonresponding device icons. For more information, refer to AMS Device Manager Books Online.

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. For more information, refer to AMS Device Manager Books Online.

Installing AMS Device Manager Web Services on a station

Note

Microsoft Internet Information Services (IIS) and AMS Device Manager 11.1.1 must be installed on your system before you can install AMS Device Manager Web Services. Some control systems do not allow IIS to be installed on the same PC. Check your control system documentation to determine IIS compatibility.

Note

If you want to install AMS Device Manager Web Services on a DeltaV station, it must be a DeltaV Application or ProfessionalPLUS station.

► To install AMS Device Manager Web Services:

Note

Local administrator permission is required for installation of AMS Device Manager Web Services.

1. Ensure that appropriate Windows Firewall security settings have been made according to “Changing Windows Firewall settings” on page 119.
2. Exit/close all Windows programs, including any running in the background (including virus scan software).
3. Insert the AMS Device Manager program DVD in the DVD drive of the PC.
4. Browse to D:\AMSWEBSERVICES.
(where D is the DVD drive letter)
5. Double-click SETUP.EXE.
6. Follow the prompts.

AMS Device Manager Web Services and AMS Asset Portal 3.2 or earlier

AMS Asset Portal acquires device data as it is connecting to AMS Device Manager Web Services. To use AMS Device Manager Web Services with AMS Asset Portal for devices, the following requirements must be met:

- Server Plus software must be installed on the PC.
- Microsoft Internet Information Services (IIS) must be installed on the PC prior to installing AMS Device Manager Web Services. Use the Windows **Add or Remove Programs** and **Add/Remove Windows Components** functions to install IIS (see the Windows operating system documentation or Windows online Help for more information).
- Copy the XML stylesheets from the AMS\Db\xml\Stylesheet folder to the appropriate AMS Asset Portal folder.
- The Data Provider Web Service is required to use AMS Asset Portal. The URL to find the Web Service is: `http://<PCname>/amsdevicemanagerws/amsdataproverservice.asmx`

AMS Suite: Asset Performance Management

AMS Suite: Asset Performance Management is a new product offering that replaces AMS Asset Portal. The AMS Suite: Asset Performance Management Client Framework can be installed on an AMS Device Manager 11.1.1 station. Other components of AMS Suite APM must be installed on additional non-AMS Device Manager PCs. For more information about AMS Suite APM, contact your local Emerson Sales/Service Office.

5 Starting to Use AMS Device Manager

After installation

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

Changing 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 and KBA NA-0400-0046. For assistance configuring your Windows Firewall, contact your IT department.

Note

On a Windows Vista/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.

Usernames and passwords

Each user needs a unique login consisting of a username and a password. Ask your system administrator for your login. The User Login dialog box appears when you start AMS Device Manager. You must enter a valid username and password and select the appropriate Login Type from the drop-down list. For more information about the User Login dialog box, see AMS Device Manager Books Online.

Note

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

The AMS Device Manager application allows an initial login with the username “admin” and no password, which has AMS Device Manager System Administration rights.

NOTICE

To protect your data, assign a password to the admin username after you install AMS Device Manager. See “Assigning an “admin” password” on page 120.

User permissions are set up and maintained in User Manager. You need AMS Device Manager System Administration rights to log in to User Manager. The sections that follow provide guidance in managing usernames and passwords.

Logging in to User Manager

- To log in to the User Manager:
1. From the Windows taskbar, select **Start | All Programs | AMS Device Manager | User Manager**.
 2. In the User Manager Login dialog box, enter the “admin” username (or any other username with AMS Device Manager System Administration rights) and password.
 3. Select a **Login Type** from the drop-down list.
 4. Click **OK**.

Assigning an “admin” password

- To assign a password to the admin username:
1. Log in to User Manager.
 2. Select **admin** and click **Edit User**.
 3. Enter a password and confirm it.
 4. Click **OK**.

Note

The admin username cannot be deleted or disabled, but the password can be changed.

Adding a username

► To add a username at any time:

For a Standard User (see below for a Windows User):

1. Log in to AMS Device Manager User Manager (see above) and click **Add User**.
2. Select the **Standard User** option and click **Next**.
3. Enter a username and password and confirm the password.
4. Select the appropriate General and AMS ValveLink SNAP-ON application permissions for this user. See Books Online for more information.
5. Click **Next**.
6. Verify the new user information and click **Finish** to add the new username to the list of users.
7. Repeat for each additional Standard User.
8. Click **Close**.

For a Windows User:

1. Add the Windows Username to the **AMSDeviceManager** group (see your network administrator).
2. Log in to AMS Device Manager User Manager (see above) and click **Add User**.
3. Select the **Windows User** option and click **Next**.
4. Select the username from the list of users, and click **Next**.
5. Select the appropriate General and AMS ValveLink SNAP-ON application permissions for this user. See Books Online for more information.
6. Click **Next**.
7. Verify the new user information and click **Finish** to add the new username to the list of users.
8. Repeat for each additional Windows User.

Note

Once added, usernames cannot be deleted, but they can be disabled and the users' permissions can be changed (see "Changing rights and permissions" on page 122).

9. Click **Close**.

Changing passwords

- ▶ To change the password for a **Standard User**:
 1. Launch AMS Device Manager.
 2. On the User Login dialog, enter a valid username and password.
 3. Click the **Change Password** button.
 4. Enter a new password, confirm it, and click **OK**.

Note

You can also change the password of a Standard User in User Manager.

- ▶ To change the password for a Windows User:
 1. Simultaneously press the CTRL, ALT, and DEL keys.
 2. In the Windows Security dialog, click **Change Password**.
 3. Enter your existing password and a new password with confirmation.
 4. Click **OK**.

Changing rights and permissions

NOTICE

If you upgraded your system from AMS Device Manager 9.0 or later, the previous usernames, passwords, and permissions were migrated but the new AMS Device Manager 11.1.1 user permissions are not set. You may need to reset the user permissions.

- ▶ To change user rights and permissions:
 1. Log in to User Manager.
 2. Select the desired username.
 3. Click **Edit User**.
 4. Select or clear the rights and permissions for this user as desired.
 5. To enable or disable the username, click **Enable/Disable User**.
 6. Click **OK**.
 7. Click **Close**.

Using AMS Device Manager

After AMS Device Manager is installed, the following user information tools are available to you by selecting **Start | All Programs | AMS Device Manager | Help**:

- AMS Device Manager Books Online
- AMS Suite: Intelligent Device Manager Installation Guide
- Work Processes Guide
- Release Notes

These files are copied to your PC during AMS Device Manager installation.

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.

AMS Device Manager Books Online is accessed in two ways:

- Click the **Help** menu on the AMS Device Manager toolbar and select **AMS Device Manager Books Online**.
- OR-
- Select **Start | All Programs | AMS Device Manager | Help | 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 the  button 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 Suite: Intelligent Device Manager Installation Guide* and the *Work Processes Guide*.

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:

- Select **Start | All Programs | AMS Device Manager | Help | <document>** from the Windows taskbar.

Release Notes

The Release Notes provide the most up-to-date 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:

- From the Start menu (**Start | All Programs | AMS Device Manager | Help | Release Notes**)
- By double-clicking the RELNOTES.TXT file located in the AMS folder after installation or on DVD

We recommend that you read the Release Notes prior to using AMS Device Manager and print a copy for future reference.

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 installation DVD. 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.

Adding devices to an AMS Device Manager installation

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 from the Internet. Copy this URL into your Internet browser: <http://www2.emersonprocess.com/en-US/documentation/deviceinstallkits/Pages/deviceinstallkitsearch.aspx> and enter device search information.

Attaching 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 box (**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.

6 Troubleshooting installation

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 Process Management Sales/Service Office. Additional Support Center Contact Information can be found on the Internet at:

<http://www.emersonprocess.com/systems/support/ratecard.htm>

For more information about multiplexer networks, refer to KBA NA-0400-0084.

Error messages

ERROR MESSAGE /
INDICATION: Bluetooth adapter stops working.

POSSIBLE
SOLUTION: 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.

ERROR MESSAGE /
INDICATION: If the SQL Server installation fails.

POSSIBLE
SOLUTION: Manually install the required SQL Server version and/or service pack (SP) located on the AMS Device Manager DVD in the SQL2005ExpressAndSP3 folder as follows:

- If SQL 2005 with the Emerson2005 named instance is not installed on your PC, run Install_SQL2005ExpressAndSP3.bat.

The SQL Server manual installation process requires user input that you must provide. After you install the SQL Server with SP3, restart the AMS Device Manager installation process.

POSSIBLE
SOLUTION: There could be a mismatch between versions of SQL and Windows XP. If your PC is running Windows XP SP2 or earlier, upgrade it to Windows XP SP3 before running the SQL Server SP3 installation.

ERROR MESSAGE / INDICATION:	AMS Device Manager has detected an incorrect version of the database. The version detected is x.x, the correct version should be y.y.
POSSIBLE CAUSE:	Database Verify/Repair was not run prior to upgrading AMS Device Manager to the current release or AMS Device Manager has detected a fault that occurred during the Verify/Repair operation.
POSSIBLE SOLUTION:	Run the database conversion utility (AmsConvertDb.exe) from the AMS\Bin folder: <ul style="list-style-type: none">• Open the AMS\Bin folder• Double-click AmsConvertDb.exe. If the database conversion utility does not complete successfully, contact your local Emerson Process Management Sales/Service Office.

ERROR MESSAGE / INDICATION:	Cannot find server or DNS Error.
POSSIBLE SOLUTION:	Open port 80 on the Server Plus Station where AMS Device Manager Web Services is configured. See “Changing Windows Firewall settings” on page 119.

ERROR MESSAGE / INDICATION:	Unable to connect to live device.
POSSIBLE SOLUTION:	Add AmsFFServer.exe to the exception list. See “Changing Windows Firewall settings” on page 119.

ERROR MESSAGE / INDICATION:	Unable to launch the AMS Device Manager application from the Client SC Station.
POSSIBLE SOLUTION:	Open port 135. See “Changing Windows Firewall settings” on page 119.

ERROR MESSAGE / INDICATION:	“Connecting to OPC Server Failed” when attempting to launch the OPC Client application.
POSSIBLE SOLUTION:	Add AMSOPC.exe to the exception list. See “Changing Windows Firewall settings” on page 119.

ERROR MESSAGE / INDICATION: Unable to launch the AMS Device Manager application from the Client SC Station.

POSSIBLE SOLUTION: Add sqlserver.exe and sqlbrowser.exe to the exception list. See “Changing Windows Firewall settings” on page 119.

ERROR MESSAGE / INDICATION: 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.

POSSIBLE SOLUTION: Add AMSServicesHost.exe to the exception list. See “Changing Windows Firewall settings” on page 119.

Index

Numerics

8000 BIM System Interface 111–112
requirements 41

A

adding field devices 125
admin password 120
admin password, assign 120
administrator rights 27, 120
Adobe Reader 124
AMS Device Manager
distributed system 9
standalone station 9, 10
Starting to use 119–125
uninstalling 16
upgrading 47
AMS Device Manager database
backing up 15
consolidating 48
restoring 16
AMS Device Manager Web Services
description 117
installing 10
requirements 24
AMS Device Manager Web Services and AMS Asset
Portal 118
AMS Suite
Asset Performance Management 118
AMSDeviceManager user group
adding users 54
adding users on a domain controller 64

B

Bluetooth HART modem 79
Books Online, AMS Device Manager 123

C

clock synchronization 46
communication interfaces, configuring 79
communications port, modem 79
computer name 49
configuring AMS Device Manager for
8000 BIM System Interface 111
DeltaV 98

documenting calibrator 88
FF HSE System Interface 102
HART Communicator 86
HART modem 80
HART Over PROFIBUS 113
modems 79
multiplexer network 90
Ovation System Interface 100
PROVOX System Interface 106
ROC System Interface 104
RS3 System Interface 109
STAHL network 109
Wireless Network 94
consolidating databases 48

D

database
backup 15
consolidating 48
conversion utility 128
export 48
import 48
migrating 48
moving 48
restore 16
sharing 56
DeltaV System Interface 96
configuring 97
configuring AMS Device Manager for 98
requirements 30
verifying node response 97
Device manual installation 124
Device manuals 124
devices, adding 125
disk space requirements 19
distributed AMS Device Manager system
configuring 56
installing 9, 45
licensing 55
modifying 57–63
requirements/constraints 46
upgrading 47
distributed control systems 93
DNS name 49
documentation, AMS Device Manager 123
documentation, electronic 123
documenting calibrator 88
domain 27
domain controller
security requirements 64
domain controllers

installing AMS Device Manager on 63

Drawings/Notes 46

duplicate device icon 92

E

electronic documentation 123

Ethernet 21, 30, 34, 41, 111

export database 48

F

FF HSE interface

requirements 38

FF HSE System Interface 102–103

Field Communicator 83–85

connecting to AMS Device Manager 84

Listen for PC setting 85

field devices, installation 125

firewall settings, changing 119

G

gateway

adding 95

H

hardware requirements 19–20

serial interfaces 20

USB interfaces 20

HART Communicator 85–87

connecting to AMS Device Manager PC 86

Listen for PC setting 87

HART Instrument Locator Tool (HILT) 105

HART modem 20, 32

Bluetooth 79

serial 79

USB 79

HART multiplexer 32

network interface 89

requirements 41

HART Over PROFIBUS System Interface 112–113

requirements 42

Help, AMS Device Manager

Books Online 123

What's This? Help 123

HILT 105

host system interfaces, *see* system interfaces

HSE System Interface, *see* FF HSE System Interface

I

I/O subsystems 93

import database 48

installation

AMS Device Manager Client SC Station 52

AMS Device Manager on DeltaV station, Client SC

69, 76

AMS Device Manager on DeltaV station, Server Plus

66, 74

AMS Device Manager Server Plus Station 50

AMS Device Manager Web Services 118

distributed AMS Device Manager system 45

HART Over PROFIBUS 112

Kongsberg 42, 114

Siemens 43, 115

troubleshooting 127

Web Services 117

on an AMS Device Manager station 117

installing devices

manually 125

Internet Explorer 24

ISA bus 20

K

Kongsberg System Interface 42, 114

L

laptop computer 79, 125

licensing AMS Device Manager

distributed system 55, 67, 74

login, User Manager 120

M

memory requirements 19

Microsoft SQL Server, *see* SQL Server

migrating databases 48

mobile workstation 64

modem, *see* HART modem

moving databases 48

multidrop installation, multiplexer 80

multiplexer network 89

multiplexer, *see* HART multiplexer

N

network structure 115

nonresponding device 93, 116

O

Online Help, *see* Books Online
operating system, AMS Device Manager 22
Ovation System Interface 99–101
 requirements 34

P

passwords 46, 107, 119
PC requirements 19
PDF Installer utility 124
permissions 120, 122
polling address 80
PROVOX System Interface 104
 HLT file 105
 requirements 38

R

Rebuild Hierarchy 92, 115, 116
Release Notes 124
Remote Desktop 23
Renaming an AMS Device Manager PC 61
requirements 19–43
 8000 BIM System Interface 41
 AMS Device Manager system 19
 DeltaV System Interface 30
 FF HSE System Interface 38
 HART multiplexer 41
 HART Over PROFIBUS System Interface 42
 network 21
 Ovation System Interface 34
 PROVOX System Interface 38
 ROC System Interface 39
 RS3 System Interface 40
 security 27
 software 22
 SQL Server 25
 STAHL HART System Interface 40
 system interfaces 29
 Web browser 24
 Wireless Network 29
ROC System Interface 103–104
 requirements 39
Roving Station
 attaching 125
RS-232 to RS-485 converter 90
RS3 System Interface 107
 communication with RNI 108
 configuring 107
 requirements 40

RS-485 converter 41, 111

S

scan new devices 116
security requirements 47, 52, 68, 76, 119
serial HART modem 79
serial interfaces 20
serial link 41, 111
Server Plus Station
 requirements 19
service notes, *see* Drawings/Notes
Siemens System Interface 43, 115
simple file sharing 27
Simulate ID key (VX dongle) 65
SNAP-ON applications, installing 56
 on AMS Device Manager Client SC Station 54
 on AMS Device Manager Server Plus Station 54
software requirements 22–27
 operating systems 22
 SQL Server 25
 Web browser 24
SQL Server 25
 account password 26, 27
STAHL HART System Interface 109
 requirements 40
standalone station
 installing 9, 10
Standard User, add 121
Station Configuration dialog box 56, 60
support, AMS Device Manager 127
synchronization, clock 46
system administration 120
system interfaces 93–118
 additional requirements 29–43
 AMS Device Manager Web Services 118
 DeltaV 96
 determining structure of 115
 FF HSE 102
 HART Over PROFIBUS 112
 Kongsberg 42, 114
 multiplexer network 89
 Ovation 99
 reading parameter data 116
 ROC 103
 RS3 104, 107, 109
 Siemens 43, 115
 STAHL HART 109
system requirements, *see* requirements, AMS Device
 Manager system

T

TCP/IP 105

requirements 21

Terminal Services 23

troubleshooting 127–129

error messages 127

modem connections 82

using database conversion utility 128

U

uninstalling

AMS Device Manager 16

upgrading

an AMS Device Manager system 11

distributed AMS Device Manager system 47

from AMS Device Manager 9.0 or later 12

from AMS Wireless Configurator 12

USB HART modem 79

USB interfaces 20

Use simple file sharing 27

User Manager 120–122

username 46

username, add 121

V

virtual memory size 19

virus scan software 50, 66

VX Dongle, see Simulate ID key

W

Web browser 24

Web Services, see AMS Device Manager Web Services

Windows 7 Professional 22

Windows Firewall 119

Windows operating systems 22

Windows security requirements 27

Windows Server 2003/2008/2008 R2 22

Windows User, add 121

Windows XP 22

Wireless Network

requirements 29

WirelessHART adapter 80

Comment Form

AMS Suite: Intelligent Device Manager Installation Guide

The *AMS Suite: Intelligent Device Manager Installation Guide* is intended to provide the basic information you need to install AMS Device Manager software and configure your system. Detailed information about AMS Device Manager is provided in AMS Device Manager Books Online.

Please give us your feedback to help us improve this manual.

Did you use this manual to:	Yes	No
Help you install AMS Device Manager?	_____	_____
Help you configure AMS Device Manager?	_____	_____
Troubleshoot your AMS Device Manager installation?	_____	_____
Can you easily find answers to your questions about AMS Device Manager installation in this manual?	_____	_____
If "No," can you easily find the answers to your questions in AMS Device Manager Books Online?	_____	_____
How could we make this manual more useful to you? _____		

Identify any errors you found in this manual:

Identify any areas that you found difficult to understand:

Other comments:

May we contact you about your comments?	Yes _____	No _____
Name	_____	
Company	_____	
Phone	_____	
Date	_____	

Thank you for your comments.
Fold and mail this form to Emerson Process Management or fax it to 1-952-828-3299.

Name _____
Company _____
Address _____

Place
Stamp
Here

Emerson Process Management
AMS Device Manager User Documentation
Mail Station AO01
12001 Technology Drive
Eden Prairie, MN 55344
USA

(Seal with tape)
