

AMS Device View 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. This document is not to be redistributed without permission from Emerson.

Copyright and trademark information

© Emerson. 2018. All rights reserved.

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

AMS, DeltaV™, and Ovation™ are marks of one of the Emerson group of companies.

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

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

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

All other marks are property of their respective owners.

Document history

Part number	Date	Description
	May 2017	Initial release
	May 2018	Update, software version 2.0

Contents

- Introduction 1**
 - AMS Device View overview 1
 - Before you begin 1
 - Install AMS Device View 2
 - Configuration Assessment Tool 2
 - Reference documents 2
- System requirements 4**
 - Hardware requirements 4
 - Software requirements 5
 - Security requirements 6
- Install AMS Device View 8**
 - Install IIS 8
 - Install the AMS Device View web server 9
 - Configure AMS Device View client devices 10
- Index 14**

Introduction

This AMS Device View Installation Guide contains the following information:

- [Introduction](#), Introduction - provides an overview of AMS Device View and lists information you need to know before installing AMS Device View.
- [System requirements](#), System requirements - lists hardware, software, and security requirements for AMS Device View.
- [Install AMS Device View](#), Install AMS Device View - describes the procedures for installing AMS Device View and configuring your devices to trust the AMS Device View SSL Certificate.

AMS Device View overview

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

Projects allow you to view and track the status of devices being commissioned through Bulk Transfer operations in AMS Device Manager.

With intuitive dashboards and focused alerts, AMS Device View lets you quickly access the data you need.

For more information on how to use AMS Device View, see the *AMS Device View Help*.

Before you begin

To install AMS Device View effectively, you should be familiar with the basic functions and operations of:

- Microsoft Windows
- Microsoft Internet Information Services (IIS)
- Your Local Area Network (LAN) configuration and security
- Your AMS Device Manager system

You also need an activation code when installing AMS Device View. See [page 5](#) for more details.

Install AMS Device View

Ensure that the PC where you are installing the AMS Device View web server meets the minimum system requirements (see [page 4](#)).

Note

You do not need to uninstall a previous version of AMS Device View if you are upgrading to AMS Device View 2.0. You will need a new activation code. Follow the instructions in the installation to receive your code, and provide your AMS Device Manager System ID.

You can deploy AMS Device View in several places in your system, depending on your security requirements. If you are installing AMS Device View on an AMS Device Manager Server Plus or ClientSC, you cannot have PlantWeb Optics installed.

See the AMS Device Manager Planning and Installation Guide Appendix for details on deployment options for AMS Device View.

Configuration Assessment Tool

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

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



Reference documents

This *AMS Device View Installation Guide* is available in the AMS Device View\Install_Files\PDF Documentation folder on AMS Device Manager DVD 1.

After AMS Device View is installed, the *AMS Device View Help* is copied to your PC and can be accessed when you open AMS Device View (see [page 3](#)).

For more information on AMS Device Manager, see the AMS Device Manager *Planning and Installation Guide* and *Books Online*.

AMS Device View Help

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

System requirements

The PC where you are installing the AMS Device View web server must meet the minimum software and hardware requirements to ensure successful installation and operation of AMS Device View.

Hardware requirements

To install the AMS Device View web server, the PC must meet the following requirements:

- Intel® Core™ I5 quad processor, 2.4 GHz or greater
- 8 GB or more of memory
- 10 GB or more of free hard disk space

Software requirements

Operating systems

The AMS Device View web server requires the following Windows operating systems:

Operating System	Version	Service Pack
Windows 7	Professional or greater editions	1
Windows 10	Professional or greater editions	
Windows Server 2008 R2	Standard or greater editions	1
Windows Server 2012 R2	Standard or greater editions	
Windows Server 2016	Standard or greater editions	
Notes		
<ul style="list-style-type: none"> • Only 64-bit versions of the operating systems are supported. • Desktops, laptops, and tablets with touchscreens are supported on Windows 10. • The correct operating system service pack (SP) must be installed on your PC before installing AMS Device View. If your PC does not have the correct SP installed, or you are unsure, contact your network administrator. 		

License

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

.NET Framework

AMS Device View requires

- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 3.5 Service Pack 1.
- Microsoft .NET Core (32-bit) 1.0.1

AMS Device Manager compatibility

AMS Device View requires AMS Device Manager 14.0. You can install AMS Device View on a standalone PC without AMS Device Manager or co-deployed with AMS Device Manager. If you install AMS Device View on a standalone PC or on a Client SC Station, the installation will prompt you to enter the Server Plus Station name or IP address and the AMSDBUser password.

Note

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

DeltaV compatibility

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

Notes

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

Internet Information Services

The AMS Device View web server requires Internet Information Services (IIS) 7 or greater. Use the default settings when installing IIS. The following IIS modules are installed when default settings are selected:

- Anonymous Authentication Module
- ASP.NET Core Module

Contact your network administrator for more information.

Web browsers

AMS Device View supports the following web browsers:

- Microsoft Internet Explorer version 11
- Microsoft Edge
- Google Chrome version 66 or higher (Windows or Android OS only)
- Safari Mobile

Security requirements

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

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

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

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

- Device Read
- Device Write, to associate a device with a project, remove a device from a project, or mark a device as complete for a project
- Manage Alert Configurations, to disable alerts in AMS Device View
- System Settings Write, to rename, delete, or complete a project

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

Certificate Management

AMS Device View uses self-signed certificates as an out-of-the-box solution with a strong recommendation for the use of commercial CA issued public key certificates.

SSL Requirements

If you are connecting to AMS Device View using SSL (HTTPS protocol), you must use the name of the AMS Device View Web Server, not its IP address. If your local network prevents this, contact Emerson support for details.

Internet Information Services Recommendations

Run the CIS-CAT Pro tool before installing AMS Device View to ensure your IIS version is appropriately configured. See the Configuration Assessment Tool topic for details.

Install AMS Device View

Ensure that the PC where you are installing the AMS Device View web server meets the minimum system requirements (see [page 4](#)).

Note

You do not need to uninstall a previous version of AMS Device View if you are upgrading to AMS Device View 2.0. You will need a new activation code. Follow the instructions in the installation to receive your code, and provide your AMS Device Manager System ID.

You can deploy AMS Device View in several places in your system, depending on your security requirements. If you are installing AMS Device View on an AMS Device Manager Server Plus or ClientSC, you cannot have PlantWeb Optics installed.

See the AMS Device Manager Planning and Installation Guide Appendix for details on deployment options for AMS Device View.

Install IIS

- To install IIS in Windows 7 or Windows 10:
 1. Select Start > Control Panel.
 2. Click Programs.
 3. Click Turn Windows features on or off.
 4. Select the Internet Information Services checkbox and click OK.
 5. Restart your PC.
- To install IIS in Windows Server 2008 R2:
 1. Select Start > All Programs > Administrative Tools > Server Manager.
 2. Select Roles on the left and click Add Roles.
 3. Click Next.
 4. Select the Web Server (IIS) check box.
 5. Click Next.
 6. Click Next.
 7. Click Install.
 8. Click Close.
- To install IIS in Windows Server 2012 or Windows Server 2016:
 1. Select Start > Server Manager.
 2. Select Manage > Add Roles and Features.
 3. Click Next.

4. Select Role-based or feature-based installation.
5. Click Next.
6. Select a server and click Next.
7. Select the Web Server (IIS) check box.
8. Click Add Features.
9. Follow the prompts.
10. Click Install.
11. Click Close.

Install the AMS Device View web server

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

1. Install IIS (see [page 8](#)).
2. Exit/close all Windows programs, including any running in the background (including virus scan software).
3. Insert the AMS Device Manager DVD 1 in the DVD drive of the PC.
4. In the AMS Device View folder, double-click AMSDeviceView_Setup.exe.
5. If a message about third-party components is displayed, click OK.
6. (Optional) Restart your PC, if prompted.
7. Click Next.
8. Enter the activation code and click Next.

Note

For information on how to get your activation code, see [page 5](#).

9. Accept the License Agreement and click Next.
10. Do one of the following:
 - Click Next to install AMS Device View in the default location.
 - Click Browse to select a different location, and click OK.
11. The Enable Require SSL check box is selected by default. You will need to install the AMS Device Manager SSL certificate on any devices that will access the AMS Device View web server. See [Export the AMS Device View SSL Certificate](#) and install the certificate on the appropriate operating system. Emerson strongly recommends using secure communications.
12. Click Next.
13. (Optional) The AMS Device View Server Config dialog is displayed if you are installing on a PC without the Server Plus Station installed. Enter the Server Plus Station PC name or IP address and the AMSDbUser Password and click Configure.

Note

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

14. Click Finish.

Configure AMS Device View client devices

Note

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

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

Export the AMS Device View SSL Certificate

If you have selected secure communications at install time, and you are using the Emerson self-signed certificate, use this procedure to save the AMS Device View SSL certificate to install on any computer that will be communicating securely with the AMS Device View web server.

1. On the AMS Device View web server, enter `certmgr.msc` on the Start screen and press Enter.
2. Expand Trusted Root Certification Authorities and select Certificates.
3. Right-click the AMS Device View certificate and select All Tasks > Export.

Note

To quickly find the certificate, look for AMS Device View under the Friendly Name column.

4. Click Next.
5. Select No, do not export the private key.
6. Click Next.
7. Select DER encoded binary X.509 (.CER).
8. Browse to a location where you want to save the certificate and enter a file name.
9. Click Save.
10. Click Next.
11. Click Finish.

Install the AMS Device View SSL Certificate on Windows PCs

1. Copy the certificate file you exported in the AMS Device View web server (see [page 10](#)) to your AMS Device View client PC.
2. Double-click the certificate file.
3. Click Install Certificate.
4. Do one of the following:
 - On Windows 10, Server 2012 R2, or Server 2016, select Local Machine and click Next.
 - On Windows 7 or Server 2008 R2, click Next.
5. Click Next.
6. Select Place all certificates in the following store.
7. Click Browse and select Trusted Root Certification Authorities.
8. Click OK.
9. Click Next.
10. Click Finish.
11. If you see the Security Warning dialog, click Yes.
12. Click OK.
13. Restart your browser and open AMS Device View.

Note

When you open AMS Device View, ensure that you use the fully qualified domain name (for example, <https://myserver.mydomain.com/AmsDeviceView>) of the AMS Device View web server. See [page 12](#) for more information.

Install the AMS Device View SSL Certificate on iOS devices

1. Email the certificate file you exported in the AMS Device View server (see [page 10](#)) to an account accessible on your iOS device.
2. Open the email and tap the attached certificate file.
3. Tap Install.
4. Tap Install Now.
5. Tap Done.
6. Go to Settings > General > About > Certificate Trust Settings.
7. Turn on the toggle button for the AMS Device View certificate.
8. Tap Continue.

Install the AMS Device View SSL Certificate on Android devices

1. Copy the certificate file you exported in the AMS Device View web server (see [page 10](#)) to a specific location on your Android device.
2. Open Settings > Security.
3. Scroll down to Credential Storage and tap Install from device Storage.
4. Browse to the location of the certificate file and select the certificate.
5. Enter a Certificate name.
6. Select VPN and apps under Credential use.
7. Tap OK.
8. Open Trusted Credentials > USER.

The certificate is displayed under the USER tab.
9. Open AMS Device View on Google Chrome.

Note

When you open AMS Device View, ensure that you use the fully qualified domain name (for example, <https://myserver.mydomain.com/AmsDeviceView>) of the AMS Device View web server. See [page 12](#) for more information.

10. (Optional) Re-install the certificate from Google Chrome, if prompted.
11. (Optional) If Google Chrome asks you to install the certificate again, tap Cancel.

AMS Device View should now open without any security warnings.

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

1. On the AMS Device View server PC, click Start.
2. Right-click on Computer.
3. Select Properties.

The fully qualified domain name is listed in the Full computer name field.

Log in to AMS Device View

Ensure your Windows username is enabled in AMS Device Manager User Manager utility.

1. Open AMS Device View (<https://<yourservername>/AmsDeviceView>) with a supported browser. See the *AMS Device View Installation Guide* for the list of supported browsers.

Note

Ensure that you use the fully qualified domain name of the AMS Device View server. You can not use an IP address in the URL if you are accessing by SSL (HTTPS://)

2. Enter your Windows username and password.
3. Select Login.

Index

A

- AMS Device View Help 3
- AMS Device View web server
 - install 9
 - view fully qualified domain name 12

B

- before you begin 1

C

- configure AMS Device View clients 10

H

- hardware requirements 4

I

- IIS
 - install 8
- installation 2, 8
- introduction 1

L

- license 5
- log in 12

O

- operating systems 5
- overview 1

R

- reference publications 2

S

- security requirements 6, 7
- software requirements
 - .NET framework 5
 - AMS Device Manager 5
 - DeltaV 6
 - IIS 6
 - operating systems 5
 - web browser 6
- SSL Certificate
 - Android install 12
 - export 10
 - iOS devices install 11
 - Windows PC install 11
- system requirements 4

Emerson

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

©2018, Emerson.

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. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.

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

