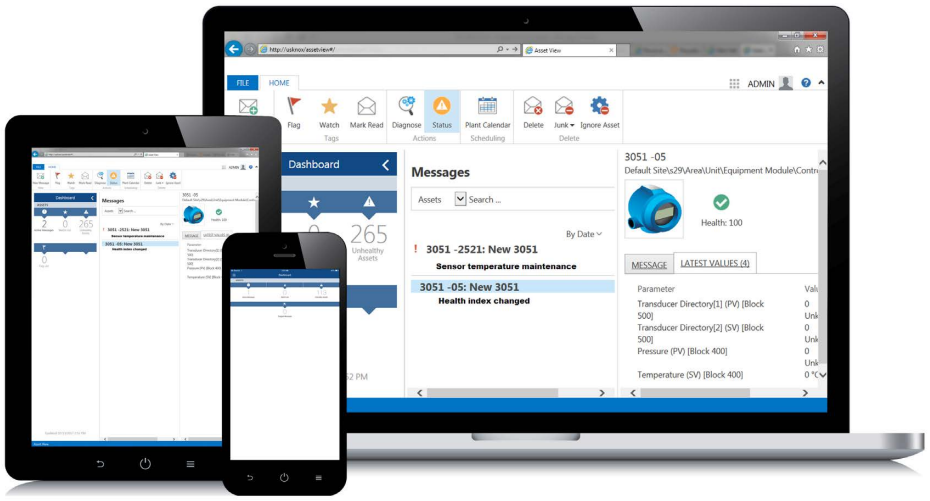
System Guide
MHM-97911, Rev 1
September 2017

AMS ARES™ Platform v1.4

System Guide



EMERSON™

Where to get help

Emerson provides a variety of ways to reach your Product Support team to get the answers you need when you need them:

Phone Toll free 800.833.8314 (U.S. and Canada)
+65.6770.8711 (Europe and Middle East)
+63.2.702.1111 (Asia Pacific)

Email *ap-sms@emerson.com*

Web *http://www.emerson.com/en-us/contact-us* and select AMS or CSI TECHNOLOGIES from the Automation Solutions drop-down menu.

To search for documentation, visit *http://www.emerson.com* and select **Documents & Drawings**.

To view toll free numbers for specific countries, visit *http://www.emersonprocess.com/technicalsupport*.

Contents

Appendices and reference

1 Overview

AMS ARES™ Platform

The AMS ARES™ Platform lets you monitor the health of your assets in relevant time and from any location. It is an extensible platform that aggregates process and predictive diagnostic data for a holistic view of the health of your assets. The AMS ARES Platform supports Wireless HART gateways, AMS Device Manager, AMS Machine Works, and OPC UA.

The AMS ARES Platform employs an asset-centric approach so you can prioritize and monitor the health of your assets either onsite or offsite. Persona-specific user accounts ensure that the right information is going to the right person, allowing each user to get exactly what they want to see, and nothing more.

The AMS ARES Platform has these applications that enable you to perform plant management functions:

- Asset Explorer—access and manage assets in your plant.
- Asset View—send, receive, and view messages generated in the AMS ARES Platform.

  You can view these messages from a computer or from a mobile device.
- User Manager—control and monitor access to the various components of the AMS ARES Platform.
- Event Viewer—view events generated in the AMS ARES Platform.

About this manual

The AMS ARES Platform System Guide is intended for system administrators to help plan, install, and set up the AMS ARES Platform. Emerson recommends that system administrators reference this document when setting up the AMS ARES Platform system.

Other relevant documents

- *AMS ARES Platform Online Help*—provides instructions and reference information for using the software. This is built into the application and accessed by clicking in the user toolbar.
- Release Notes—contains what's new and notes pertaining to the release.
- Knowledge Base Articles—documents released to address known issues and bugs.

2 Planning considerations

2.1 .NET Framework 3.5

- Microsoft .NET Framework 3.5 is required to install the AMS ARES Platform.
- Use “Turn Windows features on or off” to enable .NET Framework 3.5. See KBA NK-1600-0300 for instructions.
- You need an Internet connection to enable .NET Framework 3.5.

2.2 Internet Information Services (IIS)

- During default installation, IIS is automatically installed and configured to use the Default Site (port 80).
- Check Windows’ Programs and Features to verify IIS is not listed. If IIS is installed, you can delete the Default Site (if unused) or configure it to use another port, before installing the AMS ARES Platform. See *page 79* for instructions.

2.3 Microsoft SQL Server

There are two database configuration options available. The database can either reside on the AMS ARES Platform server (Tier-1 installation) or on a separate server from where the AMS ARES Platform is installed (Tier-2 installation). If you already have an existing separate SQL Server setup and would like to use it, select a Tier-2 installation.

Tier-1 installation

Tier-1 is the default configuration and represents the typical single or network server system.

- Check Windows’ Programs and Features to verify that Microsoft SQL Server is not currently installed. During default installation, Microsoft SQL Server 2014 Express is automatically installed and configured for the AMS ARES Platform.
- The EmersonCSI named instance is automatically created with the AMS ARES Platform installation when there is no existing Microsoft SQL Server installation.
- If Microsoft SQL Server is currently installed, create the EmersonCSI named instance before beginning the AMS ARES Platform installation. The user installing the AMS ARES Platform should be a system administrator for the EmersonCSI named instance.
- The EmersonCSI named instance needs to be set up for mixed authentication—Windows and SQL accounts.

- If you are manually installing SQL Server 2014, make sure the account running the SQL Server setup has rights to back up files and directories, rights to manage auditing and the security log, and rights to debug programs. See *page 81* for instructions.

Tier-2 installation

A Tier-2 installation requires configuration and management by a database administrator.

- For Tier-2 installations, the database can be Microsoft SQL Server 2014 or later.
- The SQL server must be configured to requirements before installing the AMS ARES Platform. See *page 89* for instructions.
- Create the EmersonCSI named instance before beginning the AMS ARES Platform installation. The user installing the AMS ARES Platform should be a system administrator for the EmersonCSI named instance.
- The EmersonCSI named instance needs to be set up for mixed authentication—Windows and SQL accounts.
- Enable TCP/IP protocol for EmersonCSI SQL Server Network Configuration.
- Ensure SQL Browser is running, and set it to auto-start.

2.4 Planning your AMS ARES Platform installation

Installable components

The AMS ARES Platform, being an extensible system, consists of components with its own installations.

Installable component	Description
AMS ARES Platform	The main component of the software. **Note** You have to install the platform first before all other applications can be installed and integrated with it.
AMS Machine Works—ARES Asset Extension	Enables you to use the AMS Machine Works Vibration Analyzer and create machines in Asset Explorer.
Emerson Wireless Gateway ASI	Enables you to connect and display information from an Emerson Wireless Gateway and from devices on the gateway.
AMS Device Manager ASI	Enables you to bring AMS Device Manager alerts, data, and hierarchy into the AMS ARES Platform. The AMS Device Manager ASI installation consists of two parts: the Service and the Web Application (Web App).
OPC UA platform extension	Enables you to connect to OPC UA clients.

Installable component	Description
AMS Machine Works Vibration Analyzer	Enables you to analyze periodic and online vibration data. You should have the AMS Machine Works—ARES Asset Extension installed for this to work.
AMS Device Manager Launcher	Enables you to launch AMS Device Manager in context from Asset Explorer when AMS Device Manager is installed on the computer. It is different from the AMS Device Manager ASI.
Asset View Mobile	A mobile version of Asset View that allows you to display, send, and receive AMS ARES Platform messages and notifications from your mobile device.

Important

Emerson recommends installing only the components you plan to use.

If you install components you do not need, it will unnecessarily use system resources. For example, only install OPC UA if you plan on using it. You can install OPC UA later if needed.

Installation on a single system or client-server system

The AMS ARES Platform can be installed as either a single system or as a server with one or multiple connected clients. The following table shows where the AMS ARES Platform components can be installed:

Component	Single system	Client-server system		
		Server	Second server	Client
AMS ARES Platform	x	x		
AMS Machine Works—ARES Asset Extension	x	x		
Emerson Wireless Gateway ASI	x	x	x (install one instance on one server)	
AMS Device Manager ASI Service	x		x (install one instance on one server)	
AMS Device Manager ASI Web Application	x	x		
OPC UA platform extension	x	x		
AMS Machine Works Vibration Analyzer	x			x

Component	Single system	Client-server system		
		Server	Second server	Client
AMS Device Manager Launcher(1)				x

(1) Do not install the AMS Device Manager Launcher on a single system or on the platform server. It is intended as a client application and should only be installed on client stations.

⚠ CAUTION!

If you install both the AMS Device Manager ASI and Emerson Wireless Gateway ASI on your AMS ARES Platform system, do not add the same Emerson Wireless Gateway to both AMS Device Manager and Emerson Wireless Gateway ASI. Duplicate devices, events, and process variables will display in the AMS ARES Platform.

If your system gets into this state, contact Emerson Product Support for help in cleaning up the underlying database components. There is no automated or user-facing methodology available to recover from this condition.

See *page 6* for diagrams showing recommended deployments.

Databases

There are two database configuration options available, Tier-1 and Tier-2.

Tier-1 is the default configuration and represents the typical single or network server system. Tier-1 installations have databases on the server where the AMS ARES Platform is installed.

- Database resides on the AMS ARES Platform server
- Uses Microsoft SQL Server 2014 Express (automatically installed by default)
- Automatic backup processing available. See *page 86* for more information.

Tier-2 installations have databases on a separate SQL Server from the AMS ARES Platform server and require configuration and management by a database administrator.

- Database resides on an existing Microsoft SQL database server.
- Database server must be configured to requirements before installing the AMS ARES Platform. See *page 89* for more information.
- Automatic backup processing is not available; backups should be managed by your database administrator.

Custom installations

You can specify non-default installation/database locations and database passwords. The list shows installations that can be customized for some components of the AMS ARES Platform:

- AMS ARES Platform – you can change the location where data is stored and change database user passwords.

- AMS Machine Works—ARES Asset Extension – you can change the database user passwords.
- Emerson Wireless Gateway ASI – you can specify a non-default install location.

Mobile

Download the Emerson Asset View mobile application from the Google Play™ Store or the Apple® AppStore™ and install it to display, send, and receive AMS ARES Platform messages and notifications on your mobile device.

2.5 Deployment best practices

2.5.1 Deployment diagrams

These diagrams show recommended deployments of the AMS ARES Platform and its components and ASIs.

Figure 2-1: One- or two-level deployment

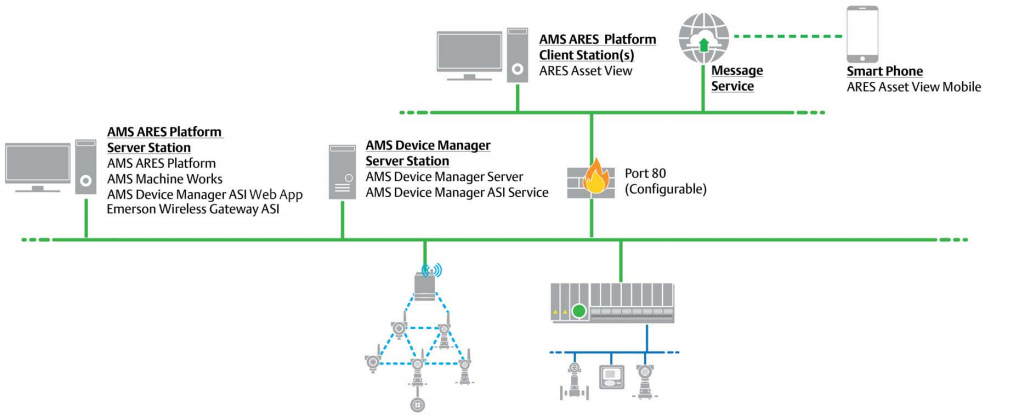


Figure 2-2: Three-level deployment

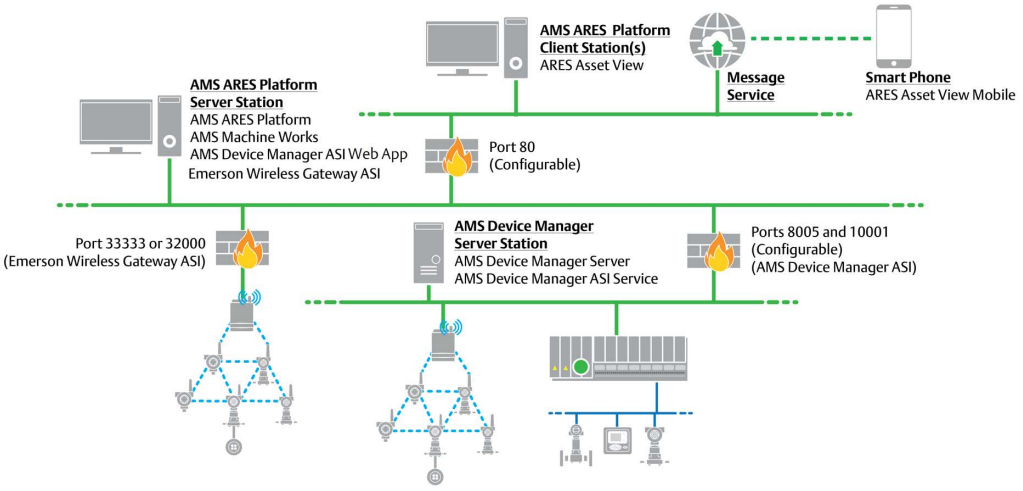


Figure 2-3: Four-level deployment

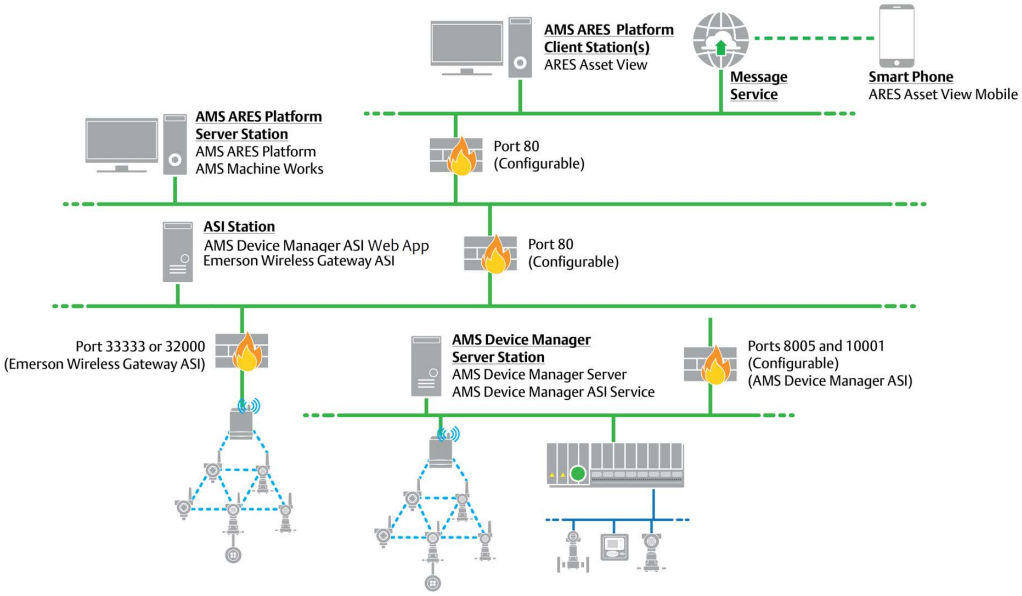
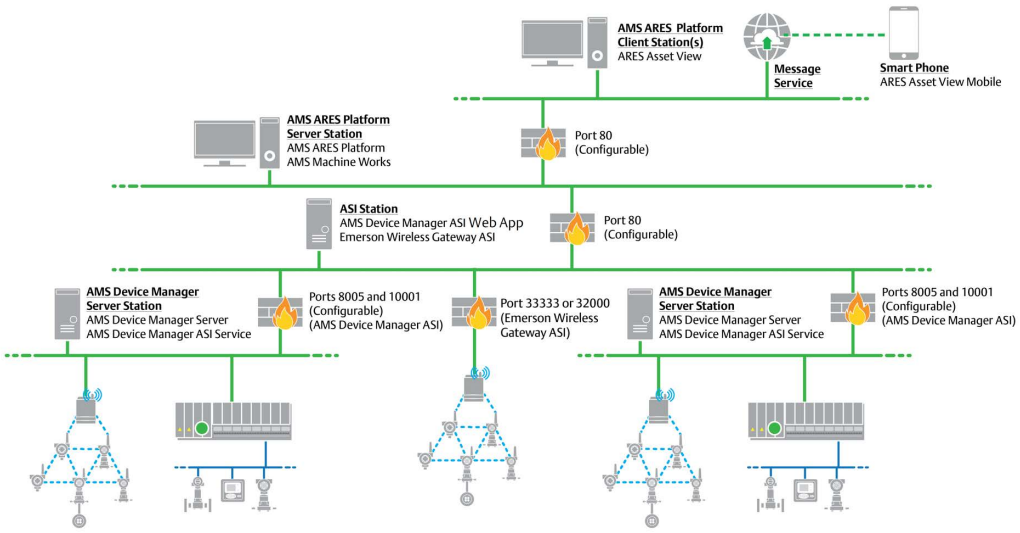


Figure 2-4: Four-level deployment with multiple AMS Device Manager systems



2.5.2 AMS ARES Platform setup

The AMS ARES Platform can be set up as a single system or as a server with multiple clients.

The AMS ARES Platform database can be hosted in the platform server or on a separate server. Tier-1 means the platform database is on the same computer as the AMS ARES Platform installation. Tier-2 means the AMS ARES Platform database is on a separate SQL Server.

Tier-1, non-server OS

AMS ARES Platform Server
& AMS ARES Platform Client

Tier-1, server OS

AMS ARES Platform Client

AMS ARES Platform Server

Tier-2, server OS

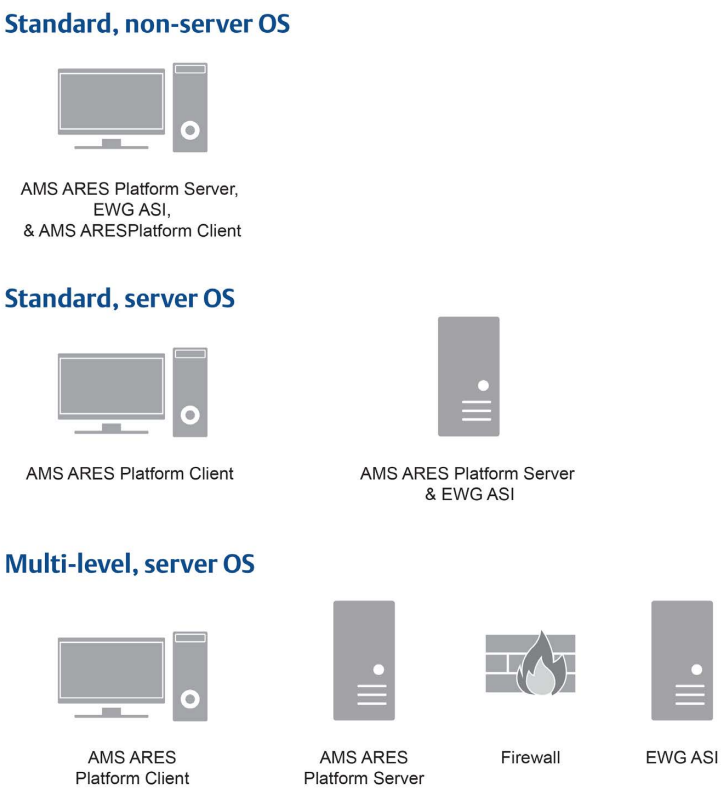
AMS ARES
Platform Client

AMS ARES
Platform Server

SQL
Server

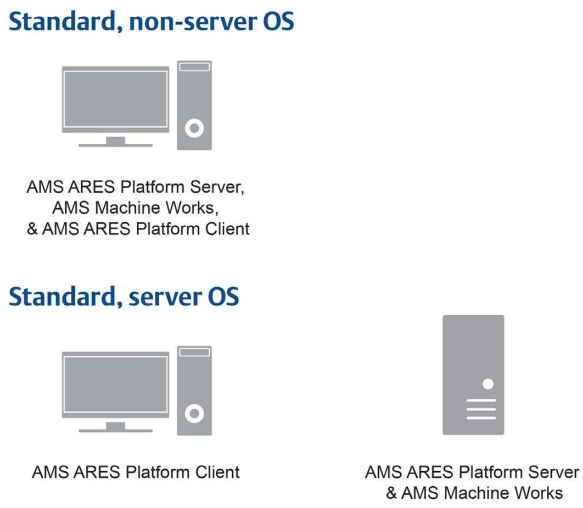
2.5.3 Emerson Wireless Gateway ASI deployment

The Emerson Wireless Gateway ASI can be installed on an AMS ARES Platform single system, on the server in a client-server setup, or it can be installed separately from the AMS ARES Platform system, divided by a firewall.



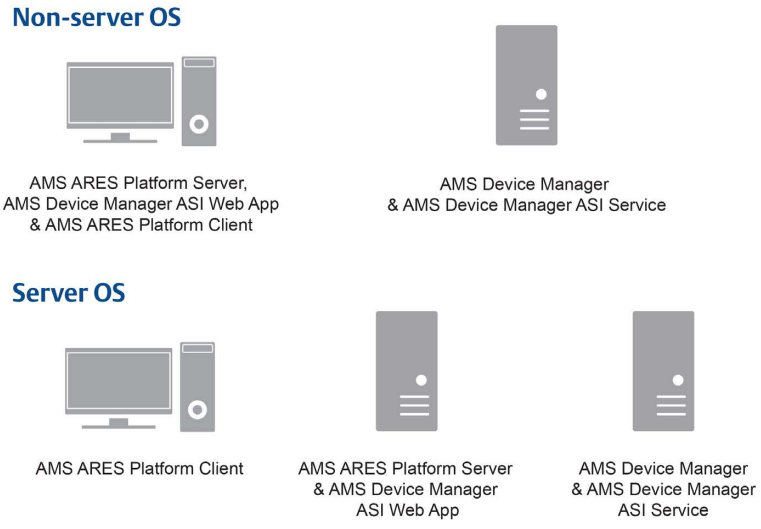
2.5.4 AMS ARES Machine Works deployment

The AMS ARES Machine Works can be installed on an AMS ARES Platform single non-server system, or on the server in a client-server system.



2.5.5 AMS Device Manager ASI deployment

The AMS Device Manager ASI Web Application can be installed on an AMS ARES Platform single non-server system, or on the server in a client-server setup. The AMS Device Manager ASI Service can be installed on a server separate from the AMS ARES Platform.



2.6 AMS Device Manager ASI in your network

There are two components that allow the AMS Device Manager ASI to provide data to the AMS ARES Platform: the Service and the Web Application.

The Service gathers AMS Device Manager data from the AMS Device Manager database and must be installed on an AMS Device Manager station. Emerson recommends a Client SC station.

The Web Application passes the information from the Service, using Microsoft Internet Information Services, through HTTP (or secure HTTPS), to the AMS ARES Platform. The components are distributed in a single installation package, but they can be installed on one or two PCs, depending on your network requirements. Each AMS Device Manager ASI must communicate to one and only one AMS ARES Platform.

AMS Device Manager systems/devices requirements

- Up to four (4) AMS Device Manager systems supporting up to 4,000 devices total.
- Audit Trail license (to display device health).

Deployments on other Emerson systems

The AMS Device Manager ASI can be deployed on DeltaV and Ovation systems on these station types:

System	Station Type
DeltaV	Local Application Station
Ovation	Standalone Station Operator/Engineer Station Engineer/System Database Server

See the AMS Device Manager documentation for a list of supported Ovation and DeltaV versions.

2.6.1 Installing both AMS Device Manager ASI Components on a single PC

You can install the AMS Device Manager ASI (Service and Web Application) on a single PC. The PC must be an AMS Device Manager station. In addition, you must install the AMS ARES Platform on another PC prior to the AMS Device Manager ASI installation.

If the AMS ARES Platform is separated from the AMS Device Manager ASI components with a firewall, you will need to ensure default Windows port 80 is configured to allow traffic. Port 80 is the default port used by AMS ARES Platform, but it is configurable.

The AMS Device Manager ASI can also communicate with the AMS ARES Platform from a different network. See *page 6* for more information.

2.6.2 Installing AMS Device Manager ASI Components on separate PCs

If your AMS ARES Platform PC and AMS Device Manager PCs are on different networks, or are separated by a firewall, you can deploy the AMS Device Manager ASI Windows Service with the AMS Device Manager station, and the AMS Device Manager ASI Web Application, along with Microsoft Internet Information Services (IIS) or IIS Express, on different PCs. See *page 6* for more information.

2.6.3 Firewall considerations for AMS Device Manager ASI deployment

If the AMS Device Manager ASI Service and Web Application are separated by a firewall, you must configure the firewall to allow communication on port 8005 and port 10001.

If the AMS Device Manager ASI Web Application and the AMS ARES Platform are separated by a firewall, you must configure the firewall to allow communication on port 80 (default, but configurable).

Note

Before the AMS Device Manager ASI installation, you need to have TCP/IP ports open between the servers. See *page 87* for instructions.

2.7 Security considerations

Network security

Emerson recommends installing the AMS ARES Platform server in a demilitarized zone (DMZ), between Levels 2 and 3 and separated by firewalls. The AMS ARES Platform clients can be installed on Levels 2 and 5.

Responsibilities and permissions

Assign responsibilities and permissions according to job functions. This strategy ensures that appropriate persons in the plant see relevant alarms and health changes.

Responsibilities restrict the user's view in Asset Explorer according to the locations assigned to him. Permissions assigned to the user would either enable or prevent him from performing tasks related to assets, messages, and plant management.

User accounts

User Manager controls user account security. Consider setting account lockouts, password complexity requirements, and session length, before adding users in the AMS ARES Platform.

2.8 System capacity

System/device	Supported maximum	Remarks
AMS Device Manager	4 systems	—
Devices connected to AMS Device Manager	4000 devices total	If there is only 1 AMS Device Manager connection, it can support up to 4000 devices in that single connection.
Emerson Wireless Gateway	2	—
CSI 9420 Wireless Vibration Transmitters connected to an Emerson Smart Wireless Gateway	40	Maximum of 25 CSI 9420 devices per gateway

⚠ CAUTION!

If you install both the AMS Device Manager ASI and Emerson Wireless Gateway ASI on your AMS ARES Platform system, do not add the same Emerson Wireless Gateway to both AMS Device Manager and Emerson Wireless Gateway ASI. Duplicate devices, events, and process variables will display in the AMS ARES Platform.

If your system gets into this state, contact Emerson Product Support for help in cleaning up the underlying database components. There is no automated or user-facing methodology available to recover from this condition.

3 System requirements

AMS ARES Platform server- minimum requirements

System requirements	
Operating system	Windows Server 2012 R2 Standard
CPU architecture	x64
Processor	2.4 GHz quad processor or faster
RAM	8 GB minimum 16 GB recommended
Available disk space	50 GB
Browsers	Internet Explorer 11 *(required, even if not used as the primary browser)* Chrome v60
Ports used by the AMS ARES Platform(1)	
HTTP	TCP 80 (default), configurable
HTTPS	TCP 443 **Note** TCP 443 outbound to *.azurewebsites.net should be open to the Internet for the Asset View Mobile application to work.
SQL Server	TCP 139 TCP 445 FILESTREAM **Note** There are other ports that need to be open for SQL communication. These ports vary depending on the AMS ARES Platform database setup. See *page 87* and *page 89* for more information.
RPC (Remote Procedure Call)	TCP 135
MSDTC (Microsoft Distributed Transaction Coordinator)	TCP 135
MSMQ (Microsoft Message Queue)	TCP 135 TCP 1801
OPC	TCP 4840

(1) These ports should be available for the AMS ARES Platform and need to be open through firewalls.

AMS ARES Platform client - minimum requirements

Operating system	Windows 10 Enterprise, 64-bit Windows 10 Professional Windows 7 Professional
CPU architecture	x86 x64
Processor	2.2 GHz dual processor or faster
RAM	4.0 GB
Browsers	Internet Explorer 11 *(required, even if not used as the primary browser)* Chrome v60

AMS ARES Platform single non-server installation - minimum requirements

Operating system	Windows 10 Enterprise, 64-bit Windows 10 Professional Windows 7 Professional
CPU architecture	x64
Processor	2.4 GHz quad processor or faster
RAM	16.0 GB
Available disk space	50 GB
Browsers	Internet Explorer 11 *(required, even if not used as the primary browser)* Chrome v60

Additional specifications

Ethernet	One or more Ethernet ports
Internet connectivity	An Internet connection is required to download installations and patches, register software, and receive alerts and messages on the mobile application
Supported virtualization	• VMware 6 • Hyper-V 2012
Software	Microsoft .NET 3.5, SP1
Supported antivirus software	• Symantec™ Endpoint Protection • McAfee™ Endpoint • Norton Security with Backup

Note

Computers with AMS ARES components installed must have their system clocks synchronized. Communication can be blocked if the system clock changes. (Many third-party tools are available to synchronize system clocks). System clocks do not need to be synchronized for Mobile applications or PCs with browser-only access.

AMS ARES Machine Works - minimum requirements

AMS ARES Machine Works is always installed on the AMS ARES Platform server and the computer should meet the requirements for a server installation.

Ports used by AMS ARES Machine Works*	Direction
TCP 80 (default), configurable	Inbound
TCP 443	Inbound
* *These ports should be available and need to be open through firewalls.*	

AMS Device Manager ASI - minimum requirements

The AMS Device Manager ASI Web App should be installed on a computer that meets the requirements for a single system or server installation.

The AMS Device Manager ASI Service is always installed on an AMS Device Manager station. For a list of AMS Device Manager system requirements, see the *AMS Device Manager Planning and Installation Guide*.

Ports used by AMS Device Manager ASI*	Direction
TCP 80 (default), configurable	Inbound
TCP 443	Inbound
TCP 8005	Bidirectional
TCP 10001	Bidirectional
* *These ports should be available and need to be open through firewalls.*	

Note

There are other ports that need to be open for SQL communication. These ports vary depending on the AMS ARES Platform database setup. See *page 87* and *page 89* for more information.

Emerson Wireless Gateway ASI - minimum requirements

The Emerson Wireless Gateway ASI should be installed on a computer that meets the requirements for a server installation.

Ports used by Emerson Wireless Gateway ASI*	Direction
TCP 80 (default), configurable	Inbound

Ports used by Emerson Wireless Gateway ASI*	Direction
TCP 443	Inbound
TCP 33333	Bidirectional
TCP 32000	Bidirectional
* *These ports should be available and need to be open through firewalls.*	

Note

There are other ports that need to be open for SQL communication. These ports vary depending on the AMS ARES Platform database setup. See *page 87* and *page 89* for more information.

AMS Machine Works Vibration Analyzer - minimum requirements

AMS Machine Works Vibration Analyzer can be installed on a computer that meets the requirements for client installation.

Ports used by AMS Machine Works Vibration Analyzer*	Direction
TCP 80 (default), configurable	Inbound
TCP 443	Inbound
* *These ports should be available and need to be open through firewalls.*	

4 Mobile requirements

Mobile client - minimum requirements	
iOS	iOS 9.3.1 or later with Safari iOS 9.0 with Safari iPhone 6, iPhone 6 Plus, or later versions
Android	5.1.1 (Lollipop) or later versions 4.4.2 (KitKat)
Internet	Internet connectivity is required to send and receive messages in Asset View.
Port	TCP 443 outbound to *.azurewebsites.net should be open to the Internet for the Asset View Mobile application to work.

5 Server installation

Server installation

On the server, you can install the following:

- AMS ARES Platform
- AMS ARES Machine Works
- Emerson Wireless Gateway ASI
- AMS Device Manager ASI Web Application

  The AMS Device Manager ASI Service is recommended to be installed on an AMS Device Manager station, separate from the AMS ARES Platform server.
- OPC UA platform extension

These can be installed on servers in different combinations. See *page 3* for more information.

Optionally, you can install the AMS Machine Works Vibration Analyzer on the server.

5.1 Install the AMS ARES Platform

The AMS ARES Platform is the main installable component of the software. It serves as the framework for the system and all the other components can be installed into it.

Important

You need to install the AMS ARES Platform on the computer you designate as the AMS ARES Platform server first before installing its components.

Prerequisites

- You need the AMSARESPlatformInstall.zip.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.
- You may need to change your computer name before installing the AMS ARES Platform. Special characters (< > ; : " * + = \ | ? , _ !), accented characters, and other multibyte characters in a computer name can cause problems and interfere with a successful installation of the AMS ARES Platform. A valid computer name can have numbers 0-9, uppercase and lowercase letters A-Z, and the hyphen (-). Computer names cannot have only numbers, nor can they contain spaces.
- Determine if you will use the server name or IP address to launch the AMS ARES Platform applications. Emerson recommends using the server name instead of the IP address.

- If you use an IP address, use a static address.
- If you use the server name, ensure the computer name is valid with no special, accented, or multibyte characters.
- Only make changes to the IP address or server name before installing the AMS ARES Platform.

Procedure

1. Extract the AMSARESPlatformInstall zip file.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.

3. Select Install AMS ARES Platform and click Next.

   You must install the platform before you can install any asset or platform extensions and ASIs.

4. Read and accept the license agreement, and click Next.
5. Select the database setup and click Next:

   - Choose AMS ARES Platform and DB on the same server (Tier-1) to install the AMS ARES Platform and SQL database on the same server.

     When you choose Tier-1, you have the option to include an automated SQL maintenance task that will back up the AMS ARES Platform and AMS ARES Machine Works database daily. The backup is set to simple recovery. See *page 86* for more information.

     Uncheck the Include Automated SQL Maintenance if you do not want to schedule the daily backup of the AMS ARES Platform and AMS ARES Machine Works database.

   - Choose AMS ARES Platform and a separate DB server (Tier-2) to install the AMS ARES Platform with the AMS ARES database on a separate SQL Server.

     Important
     In a Tier-2 installation, you need to connect to a separate SQL Server that needs preliminary setup prior to installation. See *page 89* for instructions.

6. If you chose Tier-2 in the previous step, enter the following to point to the database server:

Server name	The computer name of the database server. **Note** All connected computers with SQL databases will show up in the list. If your database server has been set up to requirements, it will show as a computer name with \EMERSONCSI appended to it.
Authentication	Choose Windows Authentication or SQL Server Authentication. Select Windows Authentication to use the current Windows logged in user account for database authentication. Select SQL Server Authentication to use the user specifically created by the database administrator when creating the EmersonCSI named instance. If you select Windows Authentication, you will still need to use the SQL Server Authentication user name and password when accessing the database server.
User name	The username used for database authentication.
Password	The password associated with the user name used for authentication.

7. If necessary, edit fields in the Server and Port Binding Configuration screen, and click Next:

Server Configuration	
Use Server Name	Choose Use Server Name if you want to access or launch the AMS ARES Platform using the server name. This is the default and recommended option.
Use IP Address	Choose Use IP Address if you want to access or launch the AMS ARES Platform using the server IP address.
Note Your choice becomes the only allowed setting when launching the AMS ARES Platform and when installing ASIs and platform extensions. Failure to use the same configuration when installing ASIs and platform extensions may cause the installation to fail and you will need to uninstall and reinstall the AMS ARES Platform or any associated ASIs to use the same server setting.	
Site Binding Information	
Port	The port number when accessing the AMS ARES Platform. Port 80 is the default port. If a port is already in use, there is a red square around the port number. You must change any port binding that is being used by another website. See *page 79* to free up port 80, if it is being used by another application.

8. Select Install Now to install with all the default options or Customize to change the database location and database user passwords.

   If you chose Customize, follow these steps:

   a. Modify the password for FWK_Admin SQL Server user account and click Next.

   ⚠ CAUTION!

   When you modify passwords, make a note of the new passwords for each user account.

   b. Modify the password for FWK_Reader SQL Server user account and click Next.
   c. Modify the password for FWK_Writer SQL Server user account and click Next.
   d. Click Browse and select where you want to place the database and click Next.

      By default, the database is stored in C:\EMERSONCSI\DATA.

9. (Optional) On the finish page, when prompted on what you want to do now, click the link to install the AMS Device Manager Launcher on the client machine.

   The AMS Device Manager Launcher lets you use AMS Device Manager if it is already installed. The AMS Device Manager Launcher is a client application that is recommended to be installed only on client machines. See *page 31* for more information.

10. Click Done.

5.2 Install the AMS ARES Machine Works asset extension

The AMS ARES Machine Works asset extension has components that allow you to create machines in Asset Explorer. The AMS ARES Machine Works asset extension also enables you to use the AMS Machine Works Vibration Analyzer.

The AMS ARES Machine Works asset extension is always installed on the AMS ARES Platform server.

Prerequisites

- Ensure the AMS ARES Platform is already installed on the computer you designate as the AMS ARES Platform server.
- You need the AMSMachineWorksInstall.zip.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.

Procedure

1. Extract the AMSMachineWorksInstall zip file on the server.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.

3. Read and accept the license agreement, and click Next.
4. Select Install Now to install with all the default options or Customize to change the default AMS ARES Machine Works asset extension database passwords.

   If you chose Customize, follow these steps:

   a. Modify the password for Mhm_Admin SQL user account and click Next.

   ⚠ CAUTION!
   When you modify passwords, make a note of the new passwords for each user account.

   b. Modify the password for Mhm_Reader SQL user account and click Next.

      AMS ARES Platform services uses the user name Mhm_Reader for reading data from the SQL database.

   c. Modify the password for Mhm_Writer SQL user account and click Next.

      AMS ARES Platform services uses the user name Mhm_Writer to write data to the SQL database.

5. (Optional) At the finish page, when prompted on what you want to do now, click the link to install the AMS Machine Works Vibration Analyzer on the server.

   The AMS Machine Works Vibration Analyzer lets you diagnose your machines by viewing Spectrum, Trend, and Waveform plots to analyze periodic vibration data collected from CSI 9420s that are monitoring machines in your site.

6. Click Done.

5.3 Install the Emerson Wireless Gateway ASI

The Emerson Wireless Gateway ASI enables you to connect and display information from an Emerson Wireless Gateway and connected CSI 9420 transmitters.

You can install the Emerson Wireless Gateway ASI on the AMS ARES Platform server. If you want a more secure implementation, you can install it on a separate server, preferably on a server located on Level 2 of your network.

⚠ CAUTION!

If you install both the AMS Device Manager ASI and Emerson Wireless Gateway ASI on your AMS ARES Platform system, do not add the same Emerson Wireless Gateway to both AMS Device Manager and Emerson Wireless Gateway ASI. Duplicate devices, events, and process variables will display in the AMS ARES Platform.

If your system gets into this state, contact Emerson Product Support for help in cleaning up the underlying database components. There is no automated or user-facing methodology available to recover from this condition.

Prerequisites

- Ensure the AMS ARES Platform is already installed on the computer you designate as the AMS ARES Platform server.
- You need the EWGPluginInstall.zip.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.
- If you will install the ASI on a separate server, the ASI server must be configured to requirements before installation. The requirements vary depending on the database setup of the AMS ARES Platform server. See *page 87* and *page 95* for instructions.

Procedure

1. Extract the EWGPluginInstall zip file on the server.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.
3. Read and accept the license agreement, and click Next.
4. Enter the server name or IP address of the AMS ARES Platform server and the port number.

Important

Use the same setting as with the AMS ARES Platform installation.

For example, if you chose Use Server Name during the AMS ARES Platform installation, enter the server name here.

5. Configure the database server settings and click Next:

Server name	The computer name of the AMS ARES Platform database server. **Note** All connected computers with SQL databases will show up in the list. If your database server has been set up to requirements, it will show as a computer name with \EMERSONCSI appended to it.
Authentication	Choose Windows Authentication or SQL Authentication. Select Windows Authentication to use the current Windows logged in user account for database authentication. Select SQL Authentication to use the user specifically created by the database administrator when creating the EmersonCSI named instance for database authentication. If you select Windows Authentication, you will still need to use the SQL user name and password when accessing the database server.
User name	The username used for database authentication.
Password	The password associated with the user name used for authentication.

6. Select Install Now to install with all the default options or Customize to change the installation location.

   a. If you chose Customize, select an installation location and click Next.

7. Click Done.

5.4 Install the AMS Device Manager ASI

There are two components that allow the AMS Device Manager ASI to provide data to the AMS ARES Platform: the AMS Device Manager ASI Service and the Web Application. Both components must be installed as part of the whole AMS Device Manager ASI. Deployment of these two components would depend on your network setup.

The AMS Device Manager ASI Web Application communicates with the AMS Device Manager ASI Service and passes data to the AMS ARES Platform when an asset source is configured. This component requires the installation of the AMS Device Manager ASI Service. The Web Application can be installed anywhere on the network or on the AMS ARES Platform server.

The AMS Device Manager ASI Service communicates with the AMS Device Manager database, requires Microsoft Internet Information Services, and must be installed on an AMS Device Manager station. This component requires the installation of the AMS Device Manager ASI Web Application.

See *page 11* for deployment scenarios.

⚠ CAUTION!

If you install both the AMS Device Manager ASI and Emerson Wireless Gateway ASI on your AMS ARES Platform system, do not add the same Emerson Wireless Gateway to both AMS Device Manager and Emerson Wireless Gateway ASI. Duplicate devices, events, and process variables will display in the AMS ARES Platform.

If your system gets into this state, contact Emerson Product Support for help in cleaning up the underlying database components. There is no automated or user-facing methodology available to recover from this condition.

Prerequisites

- Ensure the AMS ARES Platform is already installed on the computer you designate as the AMS ARES Platform server.
- You need the AMSDeviceManagerASIInstall.zip file.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.
- If you install the AMS Device Manager ASI Web App on a separate server, the ASI server must be configured to requirements before installation. The requirements vary depending on the database setup of the AMS ARES Platform server. See *page 87* and *page 95* for instructions.

Procedure

1. Extract the AMSDeviceManagerASIInstall.zip.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.
3. Read and accept the license agreement, and click Next.
4. Select to install the AMS Device Manager ASI Web Application, AMS Device Manager ASI Service, or both and click Next.

   Your choice must depend on your network setup and requirements. See *page 12* and *page 6* for more information.

5. Enter the server name or IP address of the AMS ARES Platform server, and the port that is configured to accept messages, and click Next.

   The default port is 80.

6. Configure the database server settings and click Next:

Server name	The computer name of the AMS ARES Platform database server. **Note** All connected computers with SQL databases will show up in the list. If your database server has been set up to requirements, it will show as a computer name with \EMERSONCSI appended to it.
Authentication	Choose Windows Authentication or SQL Authentication. Select Windows Authentication to use the current Windows logged in user account for database authentication. Select SQL Authentication to use the user specifically created by the database administrator when creating the EmersonCSI named instance for database authentication. If you select Windows Authentication, you will still need to use the SQL user name and password when accessing the database server.
User name	The username used for database authentication.
Password	The password associated with the user name used for authentication.

7. Select Install Now to install with all the default options or Customize to change the installation location.

   a. If you chose Customize, select an installation location and click Next.

8. Click Done.

5.5 Install the OPC UA AMS ARES Platform extension

Install the OPC UA AMS ARES Platform extension to connect to OPC UA clients.

The OPC UA platform extension is always installed on the AMS ARES Platform server.

Note

Emerson recommends installing only the components you plan to use.

If you install components you do not need, it will unnecessarily use system resources. For example, only install OPC UA if you plan on using it. You can install OPC UA later if needed.

Prerequisites

- Ensure the AMS ARES Platform is already installed on the computer you designate as the AMS ARES Platform server.
- You need the AMSARESPlatformInstall.zip file.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.

Procedure

1. Extract the AMSARESPlatformInstall zip file.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.
3. Select Install ARES OPCUA Plugin and click Next.
4. Read and accept the license agreement, and click Next.
5. Select Install Now.
6. Click Restart Now.

   Note
   Building the plant hierarchy can take several minutes after installation or reboot of the AMS ARES Platform. Allow several minutes after installation or reboot before attempting to connect OPC UA clients.

6 Client installation

On the AMS ARES Platform client, you can install the following:

- AMS Machine Works Vibration Analyzer
- AMS Device Manager Launcher

6.1 Install the AMS Machine Works Vibration Analyzer

The AMS Machine Works Vibration Analyzer enables you to analyze periodic and online vibration data collected from connected CSI 9420 devices. This is a client application that can also be installed on the server.

Prerequisites

- Ensure the AMS ARES Platform and AMS Machine Works—ARES Asset Extension are already installed on the computer you designate as the AMS ARES Platform server.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.

Procedure

1. Open a browser, type http://[server]:[port number]/VibApp.

   Where [server] is the computer name or IP address of the server where the AMS ARES Platform and AMS Machine Works—ARES Asset Extension are installed and [port number], if required, is the port number assigned for the AMS ARES Platform.

   Note
   You can either enter the server name or IP address, depending on the configuration you set during installation of the AMS ARES Platform.

2. On the AMS Machine Works Vibration Analyzer installation page, click Install.
3. Run the application.
4. Click Next.
5. When prompted, enter the name or IP address of the AMS ARES Platform server and click Next.

Note

Use the same server setting, either IP address or server name as the ARES Platform configuration, when installing or upgrading, components, ASIs, asset extensions, or platform extensions. For example, when you choose the Use Server Name option in the Server and Port Binding Configuration screen during the ARES Platform installation, you must enter the server name of the ARES Platform.

Failure to use the same configuration as the AMS ARES Platform when installing or upgrading components, ASIs, and platform extensions may cause the installation to fail and you will need to uninstall and reinstall the AMS ARES Platform or any ASIs, asset extensions, and platform extensions to configure the same server setting.

6. Click Install.
7. Click Finish when done.

6.2 Install the AMS Device Manager Launcher

The AMS Device Manager Launcher enables you to use AMS Device Manager with the AMS ARES Platform, if AMS Device Manager is installed on the client PC. The AMS Device Manager Launcher is a client application that is recommended to be installed only on client machines.

The AMS Device Manager Launcher is different from the AMS Device Manager ASI. The AMS Device Manager Launcher lets you launch AMS Device Manager in context when using Asset Explorer. The AMS Device Manager ASI extends that functionality by letting you bring AMS Device Manager alerts, data, and hierarchy into the AMS ARES Platform.

Prerequisites

- Ensure the AMS ARES Platform and AMS Machine Works—ARES Asset Extension are already installed on the computer you designate as the AMS ARES Platform server.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

  Failure to turn off automatic updates can result in multiple reboots and possible installation failure.

Procedure

1. Open a browser, type http://[server]:[port number]/DM.

   Where [server] is the computer name or IP address of the AMS ARES Platform server and [port number], if required, is the port number assigned for the AMS ARES Platform.

   Note

   You can either enter the server name or IP address, depending on the configuration you set during installation of the AMS ARES Platform.

2. On the AMS Device Manager Launcher installation page, click Install.

3. Run the application.
4. Click Next.
5. When prompted, enter the name or IP address of the AMS ARES Platform server, and click Next.

Note

Use the same server setting, either IP address or server name as the ARES Platform configuration, when installing or upgrading, components, ASIs, asset extensions, or platform extensions. For example, when you choose the Use Server Name option in the Server and Port Binding Configuration screen during the ARES Platform installation, you must enter the server name of the ARES Platform.

Failure to use the same configuration as the AMS ARES Platform when installing or upgrading components, ASIs, and platform extensions may cause the installation to fail and you will need to uninstall and reinstall the AMS ARES Platform or any ASIs, asset extensions, and platform extensions to configure the same server setting.

6. Click Install.
7. Click Finish when done.

7 Single installation

On a single, non-server system, you can install the following:

- AMS ARES Platform
- AMS ARES Machine Works
- Emerson Wireless Gateway ASI
- AMS Device Manager ASI Service
- AMS Device Manager ASI Web Application
- OPC UA platform extension
- AMS Machine Works Vibration Analyzer

Note

Do not install the AMS Device Manager Launcher on a single system. It is a client application that is recommended to be installed only on client machines.

8 Mobile installation

8.1 Download Asset View on a mobile device

Emerson Asset View mobile is available for download from the Google Play™ Store or the Apple® AppStore™. It is a mobile version of Asset View that enables you to display, send, and receive AMS ARES Platform messages and notifications from your mobile device.

1. On the mobile device, open the Google Play™ Store or the Apple® AppStore™.
2. In the search bar, type `Emerson Asset View`.
3. Choose to install, and accept permissions.

9 Uninstall the AMS ARES Platform

Note
Steps for uninstalling the software can differ depending on your operating system.

Prerequisites

Uninstall the AMS ARES Platform components in the following order:

- AMS Machine Works Vibration Analyzer
- AMS Device Manager Launcher
- OPC UA platform extension
- Emerson Wireless Gateway ASI
- AMS Device Manager ASI
- AMS Machine Works—ARES Asset Extension
- AMS ARES Platform

Procedure

1. Open the Control Panel.
2. Click Uninstall a program.
3. Select to uninstall a component of the AMS ARES Platform or uninstall the AMS ARES Platform.
4. On the wizard, click Uninstall.
5. Follow the prompts and click Next.
6. Restart your computer.

10 Upgrade from a previous version

Important
Back up your databases first before starting the upgrade. See *page 71* for instructions.

Emerson recommends you upgrade all components before using the software and that you upgrade in this order:

- AMS ARES Platform

  Note
  You need to upgrade the AMS ARES Platform first before upgrading all other components.

- Emerson Wireless Gateway ASI
- AMS ARES Machine Works
- OPC UA platform extension
- AMS Machine Works Vibration Analyzer(1)
- AMS Device Manager Launcher(1)

AMS Device Manager ASI is not part of the upgrade procedure. It is new in this release.

10.1 Upgrade the AMS ARES Platform

Prerequisites

Important
Back up your databases first before starting the upgrade. See *page 71* for instructions.

- You need the AMSARESPlatformInstall.zip
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.

Procedure

1. Extract the AMSARESPlatformInstall zip file.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

(1) You need to uninstall the previous version of this client application and install a new version from the upgraded AMS ARES Platform server.

Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.

3. Select Install AMS ARES Platform and click Next.
4. Click Upgrade.
5. Click Restart Now.

10.2 Upgrade the Emerson Wireless Gateway ASI

Prerequisites

- You need the EWGPluginInstall.zip.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.
- Ensure the AMS ARES Platform is upgraded first.

Procedure

1. Extract the EWGPluginInstall zip file on the server.

Note
Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.
3. Click Upgrade.
4. Click Done.
5. Restart your computer.

10.3 Upgrade the AMS ARES Machine Works asset extension

Prerequisites

- You need the AMSMachineWorksInstall.zip.
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.
- Ensure the AMS ARES Platform is upgraded first.

Procedure

1. Extract the AMSMachineWorksInstall zip file on the server.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.
3. Click Upgrade.
4. Click Done.
5. Restart your computer.

10.4 Upgrade the OPC UA AMS ARES Platform extension

Prerequisites

- You need the AMSARESPlatformInstall.zip
- On a Windows 7 operating system, turn off automatic Windows updates before starting installation or upgrade.
- Ensure the AMS ARES Platform is upgraded first.

Procedure

1. Extract the AMSARESPlatformInstall zip file.

   Note
   Extract the zip file on a root directory. For example, drive C.

2. Double-click install.exe.

   Running install.exe checks the .NET Framework 3.5 requirement for proper installation to continue. Installation will fail if you instead run setup.exe and .NET Framework 3.5 is not yet installed on the system.
3. Select Install ARES OPCUA Plugin and click Next.
4. Click Upgrade.
5. Click Done.
6. Restart your computer.

10.5 Upgrade the AMS Machine Works Vibration Analyzer

To upgrade, you need to uninstall the previous version of the AMS Machine Works Vibration Analyzer and install a new version from the upgraded AMS ARES Platform server.

Prerequisites

Ensure the AMS ARES Platform and AMS Machine Works—ARES Asset Extension are upgraded first.

Procedure

1. Uninstall the previous version of the AMS Machine Works Vibration Analyzer.

   See *page 35* for uninstall instructions.
2. Open a browser, type http://[server]:[port number]/VibApp.

   Where [server] is the computer name or IP address of the server where the AMS ARES Platform and AMS Machine Works—ARES Asset Extension are installed and [port number], if required, is the port number assigned for the AMS ARES Platform.

   Note
   You can either enter the server name or IP address, depending on the configuration you set during installation of the AMS ARES Platform.
3. On the AMS Machine Works Vibration Analyzer installation page, click Install.
4. Run the application.
5. Click Yes on the dialog to continue with the upgrade.
6. Click Next.
7. Click Finish when done.

10.6 Upgrade the AMS Device Manager Launcher

To upgrade, you need to uninstall the previous version of the AMS Device Manager Launcher and install a new version from the upgraded AMS ARES Platform server.

Prerequisites

Ensure the AMS ARES Platform is upgraded first.

Procedure

1. Uninstall the previous version of the AMS Device Manager Launcher.

   See *page 35* for uninstall instructions.
2. Open a browser, type http://[server]:[port number]/DM.

Where [server] is the computer name or IP address of the AMS ARES Platform server and [port number], if required, is the port number assigned for the AMS ARES Platform.

Note

You can either enter the server name or IP address, depending on the configuration you set during installation of the AMS ARES Platform.

3. On the AMS Device Manager Launcher installation page, click Install.
4. Run the application.
5. Click Yes on the dialog to continue with the upgrade.
6. Click Next.
7. Click Finish when done.

11 Launch the AMS ARES Platform

Prerequisites

- If Enhanced Security Configuration is enabled in Internet Explorer, add the AMS ARES Platform server URL to the list of trusted sites. See *page 79* for instructions.
- You need to know if the AMS ARES Platform server is set up to launch by IP address or server name.
- You need to know if the AMS ARES Platform server is set up to use the default port.

Procedure

1. Open a web browser.
2. In the web browser address field, enter the URL for the application you want to launch. Refer to the following table.

Launch this application	From this URL	To perform the following
User Manager	http://[server]:[port number]/UserManager	• Set up users • Control and monitor access to the AMS ARES Platform
Asset Explorer	http://[server]:[port number]/AssetExplorer	• Set up your site • Access and manage assets in your plant
Asset View	http://[server]:[port number]/AssetView	• Send, receive, and view messages related to assets and health changes
Event Viewer	http://[server]:[port number]/EventViewer	• View events generated in the AMS ARES Platform

Where [server] is the computer name or IP address of the AMS ARES Platform server and [port number], if required, is the port number assigned to the AMS ARES Platform.

For example, to launch Asset Explorer from the AMS ARES Platform server named USKnoxx with an IP address of 10.164.252.89 and a port number of 8080, enter http://USKnoxx:8080/AssetExplorer or http://10.164.252.89:8080/AssetExplorer.

Note

You can only use either the server name or IP address when launching the AMS ARES Platform, depending on the configuration you set during installation. If you chose the Use Server Name option in the Server and Port Binding Configuration screen, you can only launch the ARES

Platform using the server name. If you chose the Use IP Address option, you can only launch the AMS ARES Platform using the server IP address.

3. Enter your credentials and log in.

   On first login, use the following defaults:

   - Username: admin
   - Password: Emerson#1

   Note

   After initial login, you are required to change this password. Your new password must have at least one special character, have an uppercase letter, and should be a combination of alphanumeric characters. As an AMS ARES Platform administrator, you have the option to change the password complexity requirement in User Manager.

12 Activate the AMS ARES Platform

The AMS ARES Platform software comes with a demo license. The demo license allows you to use the software for two hours, followed by a cool down period of four hours when you cannot access the software. The countdown to the cool down period is triggered by any first successful login to the AMS ARES Platform when it is in demo mode.

To access the software without the cool down period, you need to purchase a license and activate the software.

Procedure

1. Contact your local Emerson sales representative to purchase a license.

   Emerson will issue a zip file containing an enable table. Save this file.

2. In Asset Explorer or Asset View, click File > System Settings > License Management.

   If you are in the cool down page, scroll to the bottom of the page, click on the link that prompts you to upgrade the software.

3. Click Upgrade License.
4. Browse to the EnableTable.zip file and click OK.
5. If necessary, in the License Management dialog, click Activate License.

   Take note of the serial number and request number.

6. Call or email World Wide Customer Service (WWCS) and provide the serial number and request number. WWCS will, in turn, give you a response code.

Phone:	Toll free 888.367.3774, option 2 (U.S. and Canada) +63.2.702.1111 (Rest of world)
Email:	*wwcs.custserv@AP.EmersonProcess.com*
Web:	*http://www.emersonprocess.com/machineryhealthreg*

   Note
   If you have an email client set up on your machine, turn off the pop-up blocker.

7. Enter the response code and click OK. Click OK on the subsequent dialogs.

   Your AMS ARES Platform software is now licensed and activated.
   In the License Management dialog, the value in the Status field should be Licensed.

   Note
   If you licensed the software from the cool down page, it may be necessary to launch the AMS ARES Platform again.

13 Set up users in User Manager

User Manager function varies for administrators and users. For administrators, it is where access control to various components of the AMS ARES Platform is specified. From User Manager, administrators can add users to the system, edit properties, responsibilities, and settings for all currently registered users. It is also where mobile tokens can be conveniently issued and tracked. For users, User Manager displays read-only information about user properties, responsibilities, and mobile tokens.

13.1 Add a user

1. In User Manager, select the Users list.
2. In the Actions pane, select Add User.
3. Enter the user account details:

Field	Description
Username	The username to access the AMS ARES Platform. The username must be unique to the system. Spaces are not allowed.
Email address	A valid email address to contact the user. The user receives notification emails and messages at this address, based on the user's subscription settings.
First Name and Last Name	The user's first name and last name. This is the Display Name.
Password and Confirm Password	Password for the user when logging in to the AMS ARES Platform for the first time. **Note** The password must meet the complexity set in File > Settings > Password Settings.

   a. Check User must change password on next logon to allow the user to create his own password.
   b. Check Account is disabled to create the user account but not allow the user to log in.

4. Click Create.

   The new user is added to the Users list. You can then assign responsibilities and permissions, and issue mobile tokens for the user.

13.2 Delete a user

1. In User Manager, click the Users list, and select the user account you want to delete.
2. In the Actions pane, select Delete.
3. Click Ok to confirm.

13.3 Disable or enable a user account

A disabled user account cannot login and cannot receive notifications or messages.

1. In User Manager, click the Users list, and select the user account you want to disable/enable.
2. In the Actions pane, select Disable or Enable.

   When an account is disabled, a check mark appears in the Disabled column for the user account.

13.4 Lock or unlock a user account

A locked-out user receives notifications and email messages but is unable to log in. If Lockout Settings are enabled, an account can also become locked after a specified number of failed login attempts.

1. In User Manager, click the Users list, and select the user account that you want to lock/unlock.
2. In the Actions pane, select Lock or Unlock.

   When an account is locked, a check mark appears in the Locked column for the user account.

13.5 Assign responsibilities and permissions to a user

Permissions and responsibilities ensure the user has the proper access to locations and assets to which he is assigned.

Procedure

1. In User Manager, click the Users list, and select the user account you want to edit.
2. In the Actions pane, click Properties and select the Responsibilities tab.
3. Associate the user with locations, assets, and asset sources:

   a. Next to the Locations Associated with User [username], click Add.

   b. In the Select Plant Entities dialog, check the box next to each location and asset you want to assign to the user.

The entities in the Select Plant Entities dialog are identical to your Location and Network navigators. When you check a box, all children of that entity are automatically checked.

In Asset Explorer, the user can only view the locations to which he is assigned.

c. Click Submit.

4. Set permissions for the user:

a. Highlight the location associated with the user and next to the Permissions for User [username] at Location [location], click Add.

b. In the Add Permissions dialog, select the permissions to assign to the user.

Permission	Meaning for the assigned location
Can read data for a location	Can read data for the location. Cannot edit the data displayed.
Can edit data for a location	Can read and edit data.
Can bind asset	Can bind assets in Asset Explorer.
Can subscribe to messages	Can subscribe to messages in Asset View.
Can view flagged assets	Can view flagged assets in Asset View.
Can flag/unflag an asset	Can flag or unflag assets in Asset View.
Can ignore/unignore an asset	Can ignore assets or remove assets from the ignore list.
Can watch/unwatch an asset	Can watch assets or remove assets from the watch list in Asset View.
Can create user message	Can create messages in Asset View.
Can manage plant calendar	Can manage the plant calendar.

5. Select the Can Manage User check box to allow the user to edit settings of other accounts in User Manager.

When checked, this gives the user account administrator privileges.

6. Click Ok.

13.6 Export the users list to a CSV file

1. In User Manager, click Actions > Export List.
2. Save the CSV file.

13.7 Change the password complexity requirements

1. In User Manager, click File > Settings.

2. Expand Password Settings and specify requirements for user passwords:
   a. In the Required Minimum Length text box, specify a minimum length for user passwords.
   b. Check the Require Special Character box to require users to include at least one allowed special character in their passwords.

      Spaces and these special characters are *not* allowed \ / | " * : < > ? , . ; ' " [ ] { } - _ = + ~ `
   c. Check the Require Digit box to require users to include a number in their passwords.
   d. Check the Require Lowercase box to require users to include a lowercase letter in their passwords.
   e. Check the Require Uppercase box to require users to include an uppercase letter in their passwords.
3. Click Ok.

13.8 Specify requirements for user accounts

1. In User Manager, click File > Settings.
2. Expand User Settings and specify user account requirements:
   a. Check the Require Unique Email box to prevent a single email address from having multiple accounts.
   b. Check the Allow Only Alphanumeric User Names box to prevent users from adding special characters to their usernames.
3. Click Ok.

13.9 Set user lockout settings

A locked-out user receives notifications and email messages but is unable to log in. Users can be locked out manually or you can set parameters to automatically lock out users from the system after a specified number of failed login attempts.

1. In User Manager, click File > Settings.
2. Expand Lockout Settings and specify requirements for locking accounts:
   a. Check the Enabled box to enable lockout settings.
   b. In the Lockout Time text box, specify the amount of time, in minutes, that a user is prevented from attempting to log in after the account is locked.
   c. In the Max Failed Access Attempts text box, specify the number of times a user can incorrectly enter his login credentials before the account is locked.
3. Click Ok.

13.10 Specify the session length for user accounts

1. In User Manager, click File > Settings.
2. Expand Cookie Settings and specify session length and validation settings:
   a. Check the Allow Refresh box to allow the user's session to be periodically and automatically verified.
   b. In the Validate Interval text box, specify the amount of time, in minutes, before a session is refreshed and verified.
   c. In the Session Expires text box, specify the amount of idle time, in minutes, before a session expires.
3. Click Ok.

13.11 Issue a mobile token

You need to issue a mobile token for each user who will access the Asset View mobile application.

Procedure

1. In User Manager, click the Users list, and select the user account to whom you want to issue the mobile token.
2. In the Actions pane, select Issue Mobile Token.
3. Click the Application drop-down menu to select the application for which you want to issue a mobile token.

   Note
   At the time of this release, Asset View is the only supported mobile application.

4. Check the Send issued token to user box to send an email to the user with instructions how to claim the mobile token.
5. Click Issue.

   The mobile token appears in the Mobile list.

Postrequisites

The user can claim the token in the mobile application for which it was issued.

Note
When a mobile token is issued to a user, that user must claim the token within 24 hours, or the token expires.

13.12 View properties of a mobile token assigned to a user

A token is associated with the user who claimed it. The token is read-only and you cannot reconfigure settings for a mobile token once it has been issued.

Procedure

In User Manager, click  Mobile.

The following read-only information is displayed:

- Token number
- User for which the mobile token was issued
- Application for which the mobile token was issued

Note
At the time of this release, Asset View is the only supported mobile application.

- Date and time the mobile token was issued
- Date and time when the token expires
- Date and time the mobile token was claimed
- The device where the mobile token was claimed

14 Set up your site in Asset Explorer

Asset Explorer is where you can set up your site; create locations, add machines and devices, and arrange them according to how your plant is set up. Asset Explorer lets you centrally manage and view the health status of your plant assets.

You can set persona-specific functions for user accounts by setting responsibilities and permissions in User Manager. Permissions and responsibilities ensure the user has the proper access to locations and assets to which he is assigned.

14.1 Join an Emerson Wireless Gateway to the AMS ARES Platform

When you set up a connection to a gateway, the AMS ARES Platform lets you set up your system quickly by enabling quick mapping and binding. If you do not have a gateway connected, you can set up your site with locations, assets, machines, and devices prepared for mapping and binding later.

Prerequisites

- In AMS Device Manager or from a Field Communicator, enable MHM Access Control for each CSI 9420 device before adding the gateway. This is to make sure you can configure device settings and alert limit settings from the AMS ARES Platform.

  To enable this setting in AMS Device Manager for rev 4 or later devices, right-click the CSI 9420 device, and select Configure > Manual Setup > General Settings tab > MHM Access Control. To enable this setting in AMS Device Manager for rev 3 or earlier devices, right-click the CSI 9420 device, and select Configure > Manual Setup > Device Setup tab > MHM Access Control.
- Port 33333 or 32000 must be open on the network and enabled in the Emerson Smart Wireless Gateway.
- The Emerson Wireless Gateway ASI should be installed and reachable on the network.

Procedure

1. In Asset Explorer, select the Network tab, and click Emerson Wireless ASI.
2. In the Home ribbon, select Add Asset Source.
3. Enter the following:

Field	Description
Site	Select the site where the Gateway is housed.
Name	Specify a name for the Gateway.
Description	Enter a description for the Gateway.

Field	Description
IP Address	Enter the Gateway IP address. **⚠ CAUTION!** **If you install both the AMS Device Manager ASI and Emerson Wireless Gateway ASI on your AMS ARES Platform system, do not add the same Emerson Wireless Gateway to both AMS Device Manager and Emerson Wireless Gateway ASI. Duplicate devices, events, and process variables will display in the AMS ARES Platform.** **If your system gets into this state, contact Emerson Product Support for help in cleaning up the underlying database components. There is no automated or user-facing methodology available to recover from this condition.**
Port Number	Enter 33333 for an unsecured HART connection. Enter 32000 for a secure connection. **Note** The above values are default port numbers. Check the Gateway web interface to ensure you enter the correct port number.
Enable Secure Protocol	Check the box to enable the username and password security protocols. **Note** You must also enable secure communication for the Gateway and have the 1420 Security Setup Utility installed.
User Name	Specify the Emerson Wireless Gateway ASI server user name. This field is only available when you select the Enable Secure Protocol check box.
Password	Specify the Emerson Wireless Gateway ASI server password. This field is only available when you select the Enable Secure Protocol check box.

4. Click Create.

The Emerson Wireless Gateway appears in the Network navigator.

14.2 Enable secure communication with an Emerson Wireless Gateway

You must perform these steps on the Emerson Wireless Gateway ASI server only after installing the 1420 Security Setup Utility.

Prerequisites

Install the latest version of 1420 Security Setup Utility (v1.5.7 or latest) on the server where the Emerson Wireless Gateway ASI is installed.

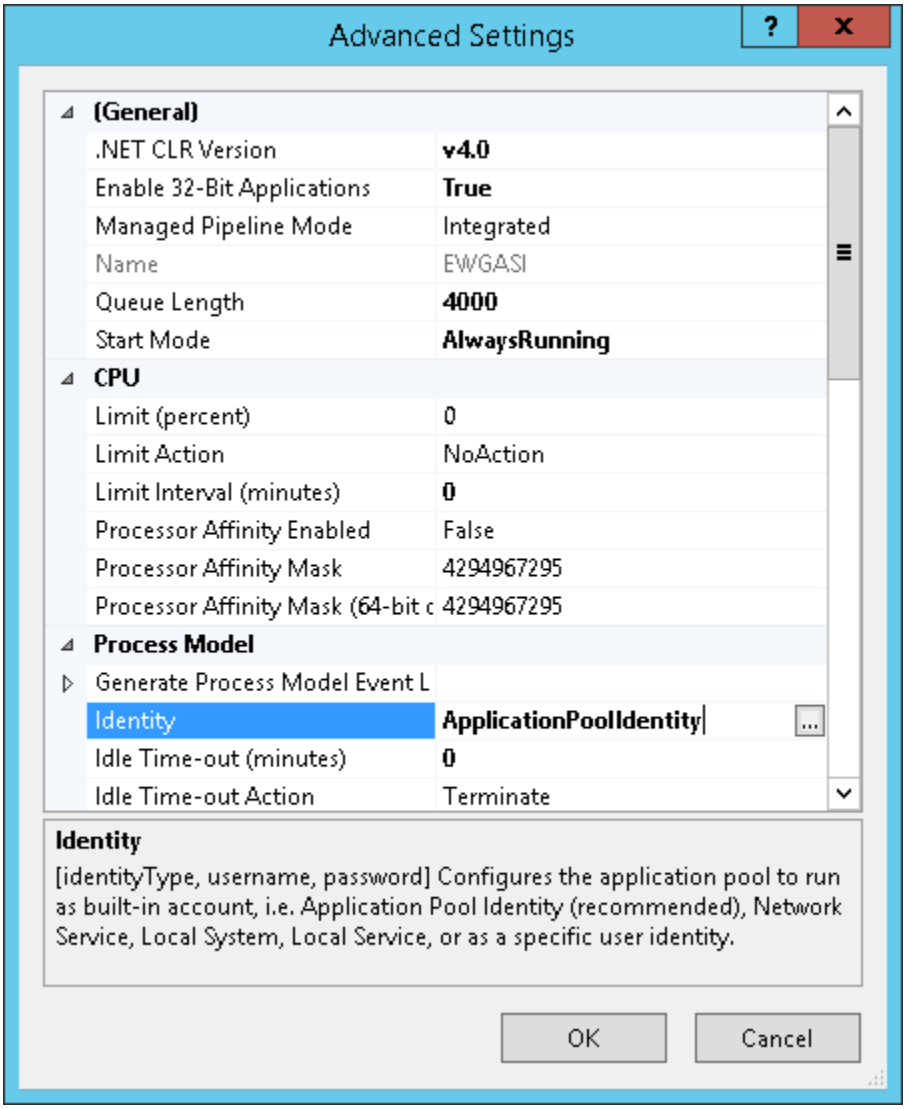
For more information on the 1420 Security Setup Utility, see the Emerson Wireless Gateway *Reference Manual*.

Procedure

1. Launch IIS Manager and expand the server name.
2. Click Application Pools and right-click on EWGASI.
3. Select Advanced Settings.

   The Advanced Settings dialog is displayed.
4. Under the Process Model tree, select Identity, and click  .

Figure 14-1: Advanced Settings—Identity



5. From the Application Pool Identity dialog, select Custom account and click Set.
6. Enter the administrator username and password and click OK.

   The Emerson Wireless Gateway ASI is now set up to run as an administrator.

7. Click OK to close the dialogs.
8. From the list of Application Pools, right-click on EWGASI, and select Recycle.
9. Launch the Security Setup Utility and create a new proxy:

   a. Select Edit > New > Add AMS Access Proxy.
   b. Right click the new proxy and select Properties.
   c. Enter the IP address of your Emerson Wireless Gateway.

d. Click OK.

e. Select File > Save.

f. If you are prompted for authentication, enter the admin password for the target Gateway.

g. Click OK.

14.3 Add locations to your site

Use locations to represent functional areas, floors, or sections of your site. You can nest locations within locations. You can add asset locations and asset source locations to locations. However, you cannot add locations to assets or asset source locations.

Procedure

1. In the Asset Explorer navigator pane, select the Location tab, and highlight the site or a location.
2. In the Home ribbon, click New Location.

   A new location appears at the bottom of the navigator. It has a folder icon and is named New Area. To rename, highlight New Area and, in the Home ribbon, click Rename.

3. Create and name additional locations at the site level, and structure locations within the locations to represent different places in your facility.

   You can create an unlimited number of locations.

Postrequisites

Add assets and asset sources to your site.

14.4 Add assets to your site

You can add assets at the site level, in locations, or in other assets. Organize the assets in logical groups similar to how the assets are physically organized in your facility.

1. In the Asset Explorer navigator pane, click the Location tab.
2. Highlight the location where you want to add assets, or create a new location.
3. In the Home ribbon, select New Asset:

   a. Select Asset (Generic) to create a new generic asset.

   b. Select Device to create a new device.

   c. Select Machine and select from the available machine components to create a machine train.

   An asset or device labeled "New" appears below the location. If you added a machine train, the name you assigned in the Machine Configurator dialog is displayed.

4. Rename the asset or device to something relevant or appropriate to your plant setup.

14.5 Create a new machine

You can add a machine, including the driver and driven components, to a location or asset. The following are general guidelines for setting up your monitoring scenario:

- When the machine you are adding is one complete machine to be monitored as a single asset, add the machine to a location.
- When you have an asset that is made up of several machines being monitored individually, and as a system, add machines to an asset.
- When you have an asset made up of multiple assets or machines, you can monitor the health of the asset as a whole, in addition to each machine and its associated monitoring devices.

Prerequisites

The AMS Machine Works—ARES Asset Extension is installed.

Procedure

1. In the Asset Explorer navigator pane, select the Location tab, and highlight a location or generic asset.
2. In the Home ribbon, click New Asset > Machine, and select a specific machine type.

   The machine types in the dropdown menu have pre-configured driver and/or driven values.
3. In the Machine Configurator dialog, enter a name and description.
4. Click the Driver checkbox and specify values in the field below:

   a. Select a machine type from the Machine Type drop-down menu.

      The Name and Speed (RPM) fields auto-populate with standard values from the catalog.

   b. Edit the values in the Name and Speed fields, if necessary.
   c. Select a bearing type from the drop-down menu.
   d. Select a lubrication type from the drop-down menu.
   e. In the Bearing Location table, click the magnifying glass in either the inboard or outboard row to open the Bearing Manager dialog and specify the brand and model number of bearings at those locations:

      a. In the Available Bearings text box, type the name of the bearing manufacturer and select a result from the predictive list.

         Values in the Precalculated Data and Physical Data fields automatically fill.

      b. Click Assign or you can use your mouse to drag and drop bearings from the Available Bearings box to the Assigned Bearings box.

You can specify multiple bearings for both the inboard and outboard locations.

c. Click OK.

Measurement locations are automatically created on your machines.

5. Place a checkmark in the Driven box and repeat steps 4a through 4e to specify values.
6. In the Machine Configurator dialog, click Save and Close.

The new machine appears in the Location navigator.

Postrequisites

Add an asset location to represent the device monitoring this machine. For example, add a device for each CSI 9420 that has sensors attached to this machine.

14.6 Add asset source locations

It is easier to add a monitoring device after it has been added to the AMS ARES Platform network. However, you might need to define the network devices in your site before that device is available on your network. You can add asset source locations for your devices to the Location navigator. Asset source locations are placeholders and are not yet bound to a physical device on the network.

Note

When you select the Add Logical Hierarchy in addition to Physical Hierarchy when adding an AMS Device Manager system to the AMS ARES Platform, the asset source locations created in the Location navigator are already bound to the corresponding devices in Network navigator.

1. In the Asset Explorer navigator pane, select the Location tab.
2. Select a location where to add the device, and in the Home ribbon, click New Asset > Device.
3. In the Add Device dialog, locate your device by manufacturer and select from a list of available models.

   For example: To add a CSI 9420, navigate to Device > Transmitter > CSI > CSI 9420.
4. Click OK.

Postrequisites

Bind the asset source locations to the actual device on the AMS ARES Platform network.

14.7 Bind an asset source location to a device on the network

An asset source location remains a placeholder until it is bound to a device on the network. Similarly, before data from a monitoring device can be saved to the AMS ARES Platform database and associated with an asset or machine, you must bind the device to an asset source location in the Location navigator.

Note

When you select the Add Logical Hierarchy in addition to Physical Hierarchy when adding an AMS Device Manager system to the AMS ARES Platform, the asset source locations created in the Location navigator are already bound to the corresponding devices in Network navigator.

Prerequisites

Connect an Emerson Wireless Gateway to the Network navigator.

Procedure

1. In Asset Explorer, highlight an asset source location in the Location navigator.

   In the Asset Explorer contents pane, unbound devices display with a red exclamation mark before the device icon.
2. In the Home ribbon, select Bind.

   The Bind Device dialog opens and displays only unbound asset sources of the same type as the asset source location.
3. In the Bind Device dialog, navigate to the asset source/device.
4. Click Bind.

Example: Bind a CSI 9420 in the Location navigator to a CSI 9420 on the network

1. In the Location navigator, right-click an unbound CSI 9420 and select Home > Bind.
2. In the Bind Device dialog, expand Emerson Wireless ASI or AMS Device Manager ASI, select the specific CSI 9420 on the network and click Bind.

   Note

   You can only select unbound CSI 9420 devices from the AMS Device Manager ASI hierarchy. This should typically happen if you are re-assigning CSI 9420 devices in the AMS Device Manager ASI hierarchy. Since devices in the AMS Device Manager hierarchy are automatically bound, to re-assign them you need to unbind and bind devices, and then map the channels, if necessary.

Postrequisites

Map channels to the machine, if you have not already done so.

14.8 Unbind an asset source location from a device on the network

Unbinding a device removes its existing channel mapping information. You need to unbind a device in the following scenarios:

- When you select the Add Logical Hierarchy in addition to Physical Hierarchy when adding an AMS Device Manager system to the AMS ARES Platform, devices are automatically bound to asset source locations in the Location navigator for the AMS Device Manager hierarchy. If you attempt to map channels and the channels you want to map are not displayed. The channels may already be mapped. You need to unbind the devices before proceeding with mapping channels to measurement locations.
- When you want to replace a device that is bound and mapped to an asset. After unbinding, you need to bind the device again to another location and redo channel mappings.

Procedure

1. In Asset Explorer, highlight the device in the Location navigator.
2. In the Home ribbon, select Unbind.
3. Click OK to unbind the device and delete any channel mapping information.

   The unbound device icon displays with a red exclamation mark.

14.9 Map asset source channels to measurement locations

Channels have to be mapped to measurement points on a machine to which a sensor is mounted. Mapping assigns the channel to the assigned sensor of the device that is monitoring the asset.

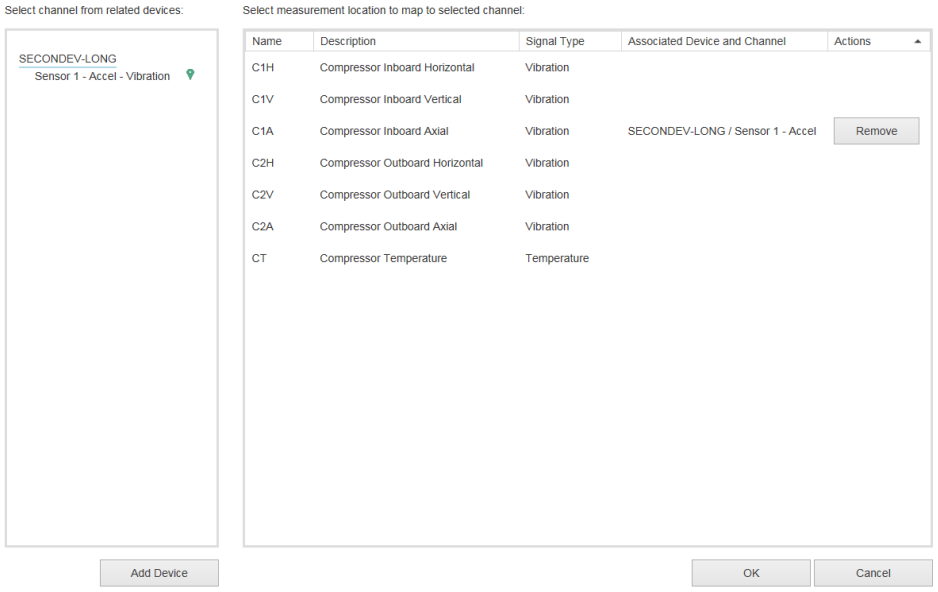
Note

When you select the Add Logical Hierarchy in addition to Physical Hierarchy when adding an AMS Device Manager system to the AMS ARES Platform, the asset source locations created in the Location navigator are already bound to the corresponding devices in Network navigator. You need to unbind these devices before proceeding with mapping asset source channels to measurement locations.

Procedure

1. In Asset Explorer, highlight a machine in the Location navigator.
2. In the Home ribbon, select Map Channels.
3. In the Map Channels dialog, select channels and measurement locations:

Figure 14-2: Map Channels dialog



On a CSI 9420, channels are labeled Sensor 1 and Sensor 2.

a. Below the "Select channel from related devices" pane, click Add Device.
b. In the Add Device dialog, select a device from the Network navigator, and click OK.
c. In the "Select channel from related devices" pane, highlight the channel that you want to map to a measurement location.
d. In the "Select measurement location to map to a selected channel" pane, highlight the measurement location where the sensor is physically mounted, and in the Actions column, click Map.

Note

The channel must be configured to match the signal type of the measurement location you want to map to; otherwise, the Map button does not appear in the Actions column.

e. Click OK.

14.10 Add a CSI 9420 location that is not yet connected to the AMS ARES Platform network

Prerequisites

Connect an Emerson Wireless Gateway ASI or AMS Device Manager ASI to the Network navigator.

Procedure

1. In Asset Explorer, add the CSI 9420 to the site:
   a. Select the area or machine where the CSI 9420 is connected, click New Asset > Device.
   b. Click Transmitter > CSI and select CSI9420.

   The new transmitter is added. You can then rename the device and give it a name specific to your plant or area.
2. Right-click the added CSI 9420 and select Bind.
3. In the Bind Device dialog, expand Emerson Wireless ASI or AMS Device Manager ASI and select gateway where the CSI 9420 is connected.

Note

You can only select unbound CSI 9420 devices from the AMS Device Manager ASI hierarchy. When you select the Add Logical Hierarchy in addition to Physical Hierarchy when adding an AMS Device Manager system to the AMS ARES Platform, the asset source locations created in the Location navigator are already bound to the corresponding devices in Network navigator. If you want to re-assign CSI 9420 devices, you can unbind and bind devices, and then redo the mapping of channels.

4. Select the specific CSI 9420 device and click Bind.
5. Select the machine where the CSI 9420 is connected and from the Home ribbon, click Map Channels.

   You can then map sensors to measurement locations in your machine.
6. Select a sensor/channel and select a measurement location to map to the selected channel.
7. Click OK.

14.11 Configure CSI 9420 data collection and storage

You can specify which data to acquire with the CSI 9420 and when to store the data for vibration analysis.

1. In Asset Explorer, select a CSI 9420 in the Network navigator or in the Location navigator.
2. In the Home ribbon, click Configure Transmitter.

   From the Location navigator, if necessary, select the transmitter that you want to configure.
3. Enter the device description.

   The value in the "Description" field displays in the Emerson Asset Explorer Details pane, Properties tab.
4. Specify values in the DEVICE tab:

a. In the PeakVue™ True FMax drop-down menu, select 500 Hz or 1000 Hz.

   FMax is the maximum bandwidth frequency, which is determined by the highest possible fault frequency. Generally, you should set the FMax to be greater than 3 times the ball pass frequency inner race (BPFI). The preferable value is 4 times BPFI.

b. In the STANDARD SPECTRUM LINES OF RESOLUTION, select the lines of resolution of the spectrum for each of the sensors.

c. In the Update Rate drop-down menu, select a value 1–60.

   Update Rate specifies how frequently, in minutes, the CSI 9420 publishes data to the Gateway. This data is then retrieved by the AMS ARES Platform.

   Note
   The default update rate is once every 60 minutes. A faster update rate is not recommended, unless the CSI 9420 is powered by an external power source, as it significantly reduces the power module life.

d. In the PowerSave Skip Multiplier drop-down menu, select a value 1x–24x.

   PowerSave Skip Multiplier is the number of times the CSI 9420 skips data acquisitions between updates to the Gateway. When this value is set to 1x, the CSI 9420 acquires a new reading at the update rate. A PowerSave Skip Multiplier of 2x combined with a 60-minute update rate results in a new acquisition every 120 minutes (every two hours). Similarly, a PowerSave Skip Multiplier of 24x with a 60-minute update rate results in a new acquisition every 1440 minutes (once per day).

e. In the Noise Threshold text box, specify a value that the Overall vibration level must exceed before the AMS ARES Platform requests Waveform/Spectrum data.

   At each Waveform/Spectrum storage interval, the system verifies that the Overall vibration level on Sensor 1 exceeds the Noise Threshold before requesting the Waveform/Spectrum data. The Noise Threshold parameter is used with time-based acquisition to avoid transmitting or storing Waveform/Spectrum data from a machine when it is not running.

f. Check the status of the Allow configuration changes check box. If it is checked, users can edit CSI 9420 parameters.

   You can only set this in AMS Device Manager or in a Field Communicator.

g. Check the status of AMS Write Protected check box. If it is checked, device variables can be written to the device.

   You can only set this in AMS Device Manager or in a Field Communicator.

h. Check the status of the Device licensed check box. If it is checked, Advanced Features are active on the CSI 9420 and they enable collection of spectrum and waveform.

5. Specify values in the ALERT LIMITS tab:

The fields are pre-populated with the current values of the CSI 9420. You can edit these values.

Note

Overall velocity alerts are in Velocity RMS. Vibration Analyzer defaults to Velocity PK. For alerts to match, Vibration Analyzer settings must be changed for Velocity to be in RMS instead of PK.

a. In the SENSOR 1 ALERT LIMITS field, set the Advise, Maintenance, and Fail limits for each measurement type.
b. In the SENSOR 2 ALERT LIMITS field, set the Advise, Maintenance, and Fail limits for each measurement type.
c. In the SENSOR BIAS fields, set the upper and lower limits for each sensor.
d. In the DEVICE ALERT LIMITS field, set the Advise, Maintenance, and Fail limits for each measurement type.

6. Specify values in the DEVICE COLLECTION tab:

a. Select a collection from the COLLECTIONS list to configure acquisition parameters for that collection.
b. In the COLLECTION TRIGGER section, choose a Trigger Type from the drop-down menu. You can choose between Time-Based or Store on Alert.

Table 14-1: Acquisition preferences based on Trigger Type

Trigger Type	Option	Description
Store on Alert	Trigger Immediately	Check this box to acquire data when measurements reach the threshold you specify in Trigger Level.
	Trigger Level	Select the alert level at which to trigger acquisition of the spectrum or waveform associated with each sensor.
Time-Based	Collection Rate	Select a value 1–24 to specify how frequently (in hours) to acquire data. Emerson recommends 8 hours or greater.

c. In the TREND PARAMETER MEASUREMENTS field (if present), check or uncheck the Store checkbox for each measurement type.

When this is checked, the selected trend parameter measurement is stored in the AMS ARES Platform.

d. In the SPECTRUM AND WAVEFORM MEASUREMENTS field (if present), you can do the following:

- Select Analytical or Thumbnail from the Details drop-down menu (if present).

Analytical means the spectrum resolution is higher and more detailed depending on the lines of resolution selected. Thumbnail means the spectrum resolution is lower and not as detailed. Thumbnail is defined by the upper limit of the spectrum which is the percentage of the FMax selected.

- Check or uncheck the Store checkbox for each measurement type.

When Store is checked, the selected waveform or spectrum measurement is stored in the AMS ARES Platform.

Note

When you choose to store *both* spectrum and waveform, the spectrum will always be stored with 1600 lines of resolution, regardless of the settings you set in step 4b. This is the behavior for both time-based and alert-based data collection.

7. Click Save and Close.

These settings are saved to the CSI 9420.

14.12 Join an AMS Device Manager system to the AMS ARES Platform

Prerequisites

- AMS Device Manager ASI is installed and reachable on the network.
- AMS Device Manager Server is running on the computer where the AMS Device Manager ASI Service is installed. Set the AMS Device Manager server to auto-start to ensure it is running.

⚠ CAUTION!

If you install both the AMS Device Manager ASI and Emerson Wireless Gateway ASI on your AMS ARES Platform system, do not add the same Emerson Wireless Gateway to both AMS Device Manager and Emerson Wireless Gateway ASI. Duplicate devices, events, and process variables will display in the AMS ARES Platform.

If your system gets into this state, contact Emerson Product Support for help in cleaning up the underlying database components. There is no automated or user-facing methodology available to recover from this condition.

Procedure

1. In Asset Explorer select the Network tab, and click the AMS Device Manager ASI folder.
2. In the Home ribbon, select Add Asset Source.
3. Enter the following:

Field	Description
Name	Enter a name for your system. This is the name displayed in Asset Explorer.
Description	Enter the system description. This is the description displayed in Asset Explorer.
AMS Device Manager Station with ASI Service	The name or IP address of the AMS Device Manager station where you installed the AMS Device Manager ASI Service.
Add Logical Hierarchy in addition to Physical Hierarchy	Select this check box to display the AMS Device Manager Plant Locations hierarchy in Asset Explorer Location navigator. **Note** When not checked, the hierarchy is only displayed in the Network navigator. To change the setting, you need to remove and then rejoin the AMS Device Manager system to the AMS ARES Platform. The asset source locations displayed in the Location navigator are already bound to the corresponding devices in the Network navigator.

4. Click Add.

When complete, Rebuild Finished appears in Event Viewer. Alert notifications and process variables will populate 30 minutes after joining the AMS Device Manager system to the AMS ARES Platform.

15 Enable users to send and receive messages in Asset View mobile

Asset View lets users send, receive, and view messages generated in the AMS ARES Platform. With Asset View, users can access and manage messages from a computer or mobile device, depending on their responsibilities and subscriptions.

Asset View administrator function ensures users can access the mobile application by issuing mobile tokens. You need to issue a mobile token for each user that will access the Asset View mobile application. See *page 48* for instructions. You can issue and monitor issued tokens in User Manager.

Port 443 must be open to the Internet on the AMS ARES Platform server to allow Asset View mobile messaging to work.

16 View system-generated events in Event Viewer

You can choose to display events per module or view all events logged by the system.

The following modules log events:

- CSI 9420 Device Configuration—events relating to configuration of connected CSI 9420 devices, such as device discovery errors.
- AMS Device Manager—events and configurations in the AMS Device Manager hierarchy, such as health changes, device alerts, rebuild hierarchies, and adding and deleting of devices.
- Asset Explorer—events and configurations in Asset Explorer, such as adding, editing, and deleting of assets and locations, binding of assets, and asset health changes.
- Asset View—events and configurations in Asset View, such as creating of messages, flagging of assets, and adding or removing of assets from the Watch List.
- Data Highway—all events occurring in the Data Highway, such as registration and unregistration of parameters.
- Emerson Wireless Gateway—all events in the Emerson Wireless Gateway, such as device alerts and device communication status.
- Machine Configuration—all machine configurations, such as adding, editing, and deleting of components, bearings, collections, measurement definitions, alarm limits, and channel mappings.
- User Manager—all events in User Manager, such as adding, editing, and deleting of users and logging in and logging out of users.
- AMS Machine Works Vibration Analyzer—all events in the AMS Machine Works Vibration Analyzer, such as adding, editing, and deleting of plot labels and machine notes; RPM changes; machine health train changes; and alarms.

Events are displayed with the following details:

- **Date and Time**—date and time the event was recorded.
- **Event Type**—the type of event the plugin responds to.
- **Source**—the module associated with the event.
- **Asset**—the asset associated with the event.
- **Attachments**—attachment associated with the event. Events with attachments have a paperclip icon.

16.1 View events

Only system-generated events can be viewed in Event Viewer.

1. In Event Viewer, on the left pane, select to view events by Application or by Modules:

- Click Application to view all events logged by the system.
- Expand the Modules folder and click on a module to view events recorded for the specific module.

2. Select an event from the list.

   Details display in the bottom pane. If an event has an attachment, a thumbnail of the attachment is displayed.

17 OPC UA

The OPC UA is a platform-independent standard through which systems and devices can communicate by sending *Messages* between *Clients* and *Servers* over a network connection.

When the AMS ARES Platform server has the OPC UA platform extension installed, your data is available to other systems on the network that can accept OPC UA input. Use an OPC UA client to verify your connection to the AMS ARES Platform, and that you can receive data. Then, within your application, use OPC UA to query the AMS ARES Platform for the data you need.

The AMS ARES Platform OPC UA server allows you to read data via OPC, but you cannot write to the AMS ARES Platform through OPC.

17.1 Connect an OPC UA client

Note

Building the plant hierarchy can take several minutes after installation or reboot of the AMS ARES Platform. Allow several minutes after installation or reboot before attempting to connect OPC UA clients.

Prerequisites

The OPC UA platform extension is installed on the AMS ARES Platform server.

Procedure

From your OPC UA Client, supply the connection information for your AMS ARES Platform server.

The OPC URL is one of the following:

- http://[server]:4840
- opc.tcp://[server]:4841

Where [server] is the computer name or the IP address of the AMS ARES Platform server.

Note

You can use either the server name or IP address, depending on the configuration you set during installation of the AMS ARES Platform.

17.2 OPC tag information and data tree structure

The names of the OPC tags are usually dependent on the configuration of a system. Virtually all data acquired by the AMS ARES Platform is available through OPC.

In your OPC UA session, or within your OPC application, you can use an OPC browser to identify the data from a CSI 9420 sensor 1, overall. For example:

Default Enterprise > Default Site > Emerson Wireless ASI > Gateway 10.4.255.254 > CSI9420 Cooling Tower Mtr/Gearbox > Sensor 1 - Overall

In the AMS ARES Platform, the OPC tag names are created using the server name followed by each branch of the tree, then the individual parameter name; each separated by a period. Depending on the OPC browser, the parameters may or may not be listed alphabetically.

At the top level of the OPC hierarchy tree (the server name), these tags are available:

Table 17-1: OPC data tree structure

OPC path	Description
Server	Default Server name.
Server.Enterprise	Default Enterprise name.
Server.Enterprise.Site	Default Site name.
Server.Enterprise.Site.Location	Name of locations added to the site. A location can contain locations, assets, and devices.
Server.Enterprise.Site.Location.[Location|Asset|Device]	Name of a location, asset, or device.
Server.Enterprise.Site.Location.Asset	Name of an asset. An asset can contain assets, machines, and devices.
Server.Enterprise.Site.Location.Machine	A machine is a specific asset type that can contain other machines and devices.
Server.Enterprise.Site.Location.[Asset.Machine.]Device	A device contains data about the device and its measurement points.

The hardware portion of the OPC hierarchy tree is listed by Units.

Table 17-2: Device information

OPC path	Description	Data type
Server.Enterprise.Site.Location.Asset.Device.**Unitname.Status**	Status of the individual hardware device (Up, Down, Acknowledged)	String
Server.Enterprise.Site.Location.Asset.Device.**Unitname.IsOnline**	Status of the individual hardware device (On/Off)	Boolean

Table 17-3: Channel/Sensor information

OPC path	Description
Server.Device. **AI01.Description**	The hardware device name; for example, Sensor -1 on a CSI 9420.

18 Back up and restore databases

The AMS ARES Platform leverages the backup and restore capacity of MS SQL Server.

This chapter covers setting up either Simple or Full recovery for the AMS ARES Platform databases installed on a single SQL instance. Consider these database backup and restore practices as additions to your overall SQL system backup plan.

Please contact your IT department for proper backup procedures as they relate to your overall backup strategy. If you do not have an IT department, call Emerson Product Support to provide you with some database backup guidance.

Backups

Guidelines when doing backups:

- Consider your business need when doing backups. The goal is to keep your information protected.
- Back up the database on a different disk apart from where the database files are.
- Create SQL user databases that are set up for Full recovery.
- When doing backups keep in mind transactions that are in progress and have not yet been completed.
- Back up all the systems and user databases as well as transactional logs.
- Create independent maintenance plans for system databases.
- Back up databases and transactional logs to recover at the point of failure.
- Partition databases into multiple files and use per file or per filegroup backups.
- Select a backup window where there is the lowest activity affecting the database.

Restore

MS SQL has three recovery models:

Recovery model	Description
Simple	All transactions are written to the log. Point-in-time recovery is not possible.
Bulk-logged	All transactions are written to the log except operations that are minimally logged. This recovery model is not recommended for the AMS ARES Platform.
Full	All transactions are written to the log. Point-in-time recovery is possible. This is the recovery model that is recommended for the AMS ARES Platform system data. The AMS ARES Platform installation sets up databases to use Full recovery.

Emerson recommends that you restore AMS ARES Platform databases using either the Full or Simple recovery model. In Simple recovery, data since the last Full or Differential backup is lost. In Full recovery, you only lose data since the last log backup.

When restoring either the AMS ARES Platform databases or the AMS ARES Machine Works database, determine the objective of the recovery point. If it is a secondary system with data that is not that important, using Simple recovery can make your backups and log management much easier. But remember that you surrender the ability to restore to a point-in-time. For the AMS ARES Platform, Emerson recommends setting up the AMS ARES Platform and AMS ARES Machine Works databases to Full recovery. This provides the database backup and the log backups and protects against loss of data.

Due to the need for data synchronization, Emerson recommends that the database restore functionality be performed by your IT department or by an Emerson support personnel.

18.1 AMS ARES Platform databases

The AMS ARES Platform installation deploys with four separate databases into the AMS ARES Platform SQL Server instance, EMERSONCSI:

- FrameworkDb
- ImageDb
- EventDb
- MessageDb

If the AMS ARES Machine Works asset extension is installed, a single database named MhmDb is deployed into the AMS ARES Platform SQL Server instance, EMERSONCSI. This database contains all the AMS ARES Machine Works data separately from the AMS ARES Platform data.

Each database consists of several files that are created on disk in the default AMS ARES Platform data directory. The files can be installed in a folder specified during installation. The default folder is C:\EmersonCSI\Data.

The recovery model can be set up differently on each database. The backup schedule for each database can be configured differently. However, Emerson recommends that each database is backed up with the same frequency. For instance, if a full backup is performed on each database every night, do not back up each database on a different night.

18.2 Back up the AMS ARES Platform databases

The AMS ARES Platform installation deploys with four separate databases. You must execute commands specific to the database to back up individual databases.

Please contact your IT department for proper backup procedures as they relate to your overall backup strategy. If you do not have an IT department, call Emerson Product Support to provide you with some database backup guidance.

Prerequisites

- Identify or create a location for your backup files. Emerson recommends a storage location on a disk or media separate from the databases.

Note
The following procedure assumes that you will store the backup files in D:\Emerson\BU. You can change this location. If you do, make sure to also change the path for the commands below.

- Determine the amount of disk space needed for your backup files.

Procedure

1. Launch Microsoft SQL Server Management Studio.

Note
Make sure your user account has access to the database.

2. Connect to the server and use Windows Authentication when prompted for the authentication type.
3. In Object Explorer, expand the Databases folder, and select a database.
4. Set the database recovery to either Simple or Full recovery. Execute the command depending on the recovery model you want.

Note
When you choose Simple recovery, you will not be able to restore the database to a point in time and you lose data since the last Full or Differential backup. In Full recovery, you only lose data since the last log backup.

- Simple recovery:

Database	Command
FrameworkDb	`ALTER DATABASE FrameworkDb SET RECOVERY SIMPLE ;`
ImageDb	`ALTER DATABASE ImageDb SET RECOVERY SIMPLE ;`
EventDb	`ALTER DATABASE EventDb SET RECOVERY SIMPLE ;`
MessageDb	`ALTER DATABASE MessageDb SET RECOVERY SIMPLE ;`

- Full recovery:

Database	Command
FrameworkDb	`ALTER DATABASE FrameworkDb SET RECOVERY FULL ;`
ImageDb	`ALTER DATABASE ImageDb SET RECOVERY FULL ;`

Database	Command
EventDb	`ALTER DATABASE EventDb SET RECOVERY FULL ;`
MessageDb	`ALTER DATABASE MessageDb SET RECOVERY FULL ;`

5. Execute the command to back up the specific database:

Database	Command
FrameworkDb	`BACKUP DATABASE FrameworkDb` `TO DISK = 'D:\Emerson\BU\FrameworkDb.bak';`
ImageDb	`BACKUP DATABASE ImageDb` `TO DISK = 'D:\Emerson\BU\ImageDb.bak';`
EventDb	`BACKUP DATABASE EventDb` `TO DISK = 'D:\Emerson\BU\EventDb.bak';`
MessageDb	`BACKUP DATABASE MessageDb` `TO DISK = 'D:\Emerson\BU\MessageDb.bak';`

This copies the complete database, including transactions that have not yet been committed.

Tip

Emerson recommends keeping Full and Differential backups as unique files and then stacking the Log backups into a single file.

a. Execute the command to perform a Differential backup:

Differential backups

If you have chosen Simple recovery, you must schedule regular Differential backups. Differential backups copy pages in the database that have been modified since the last complete backup.

Database	Command

FrameworkDb	`BACKUP DATABASE FrameworkDb`
	`TO DISK = 'D:\Emerson\BU\FrameworkDb_`
	`Differential.bak'`
	`WITH DIFFERENTIAL;`

ImageDb	`BACKUP DATABASE ImageDb`
	`TO DISK = 'D:\Emerson\BU\ImageDb_`
	`Differential.bak'`
	`WITH DIFFERENTIAL;`

Database	Command
EventDb	`BACKUP DATABASE EventDb TO DISK = 'D:\Emerson\BU\EventDb_ Differential.bak' WITH DIFFERENTIAL;`
MessageDb	`BACKUP DATABASE MessageDb TO DISK = 'D:\Emerson\BU\MessageDb_ Differential.bak' WITH DIFFERENTIAL;`

b. Execute the command to perform a Copy Only backup:

Copy Only backups

Create Copy Only backups to make sure extra and ad-hoc backups are safely performed and do not interfere with Full and Differential backups.

Database	Command
FrameworkDb	`BACKUP DATABASE FrameworkDb TO DISK = 'D:\Emerson\BU\FrameworkDb_Copy.bak' WITH COPY_ONLY;`
ImageDb	`BACKUP DATABASE ImageDb TO DISK = 'D:\Emerson\BU\ImageDb_Copy.bak' WITH COPY_ONLY;`
EventDb	`BACKUP DATABASE EventDb TO DISK = 'D:\Emerson\BU\EventDb_Copy.bak' WITH COPY_ONLY;`
MessageDb	`BACKUP DATABASE MessageDb TO DISK = 'D:\Emerson\BU\MessageDb_Copy.bak' WITH COPY_ONLY;`

c. Execute the command to perform a Log backup:

Log backups

If you have chosen Full recovery, you must create Log backups regularly. Log backups ensure that the database log file does not fill up the storage media where backups are stored.

Database	Command
FrameworkDb	`BACKUP LOG FrameworkDb TO DISK = 'D:\Emerson\BU\FrameworkDb_Log.bak';`
ImageDb	`BACKUP LOG ImageDb TO DISK = 'D:\Emerson\BU\ImageDb_Log.bak';`
EventDb	`BACKUP LOG EventDb TO DISK = 'D:\Emerson\BU\EventDb_Log.bak';`

Database	Command
MessageDb	`BACKUP LOG MessageDb` `TO DISK = 'D:\Emerson\BU\MessageDb_Log.bak';`

This copies all transactions in the log, including those that are not yet committed.

Tip

Emerson recommends creating Log backups every 60 minutes. However, if you run 24 backups in a day, you would still have one <database>Log.bak file. MS SQL appends backups into a file.

If you want to stop the stacking of files, enter the command specific to the database:

Database	Command

FrameworkDb	`BACKUP LOG FrameworkDb`
	`TO DISK = 'D:\Emerson\BU\FrameworkDb_Log.bak'`
	`WITH INIT, FORMAT;`

ImageDb	`BACKUP LOG ImageDb`
	`TO DISK = 'D:\Emerson\BU\ImageDb_Log.bak'`
	`WITH INIT, FORMAT;`

EventDb	`BACKUP LOG EventDb`
	`TO DISK = 'D:\Emerson\BU\EventDb_Log.bak'`
	`WITH INIT, FORMAT;`

MessageDb	`BACKUP LOG MessageDb`
	`TO DISK = 'D:\Emerson\BU\MessageDb_Log.bak'`
	`WITH INIT, FORMAT;`

18.3 Back up the AMS ARES Machine Works database

Please contact your IT department for proper backup procedures as they relate to your overall backup strategy. If you do not have an IT department, call Emerson Product Support to provide you with some database backup guidance.

Prerequisites

- Identify or create the location of your backup files.

Note

The following procedure assumes that the backup files are in D:\Emerson\BU. You can change this location. If you do, make sure to also change the path for the commands below.

- Determine the amount of disk space needed for your backup files.

Procedure

1. Launch Microsoft SQL Server Management Studio.

   Note
   Make sure your user account has access to the database.

2. Connect to the server and use Windows Authentication when prompted for the authentication type.
3. In Object Explorer, expand the Databases folder, and select the MhmDB database.
4. Set the database recovery to either Simple or Full recovery. Execute the command depending on the recovery model you want.

   Note
   When you choose Simple recovery, you will not be able to restore the database to a point in time and you lose data since the last Full or Differential backup. In Full recovery, you only lose data since the last log backup.

   - Simple recovery:

     ```
     ALTER DATABASE MhmDb SET RECOVERY SIMPLE ;
     ```

   - Full recovery:

     ```
     ALTER DATABASE MhmDb SET RECOVERY FULL ;
     ```

5. Execute this command to back up the database.

   ```
   BACKUP DATABASE MhmDb
   TO DISK = 'D:\Emerson\BU\MhmDb.bak';
   ```

   This copies the complete database, including transactions that have not yet been committed.

   Tip
   - Emerson recommends keeping Full and Differential backups as unique files and then stacking the Log backups into a single file.

   a. Perform a Differential backup:

      Differential backups

      If you have chosen Simple recovery, you must schedule regular Differential backups. Differential backups copy pages in the database that have been modified since the last complete backup.

      Enter this command for a Differential backup:

      ```
      BACKUP DATABASE MhmDb
      TO DISK = 'D:\Emerson\BU\MhmDb_Differential.bak'
      WITH DIFFERENTIAL;
      ```

b. Perform a Copy Only backup:

Copy Only backups

Create Copy Only backups to make sure extra and ad-hoc backups are safely performed and do not interfere with Full and Differential backups.

Enter this command for a Copy Only backup:

```
BACKUP DATABASE MhmDb
TO DISK = 'D:\Emerson\BU\MhmDb_Copy.bak'
WITH COPY_ONLY;
```

c. Perform a Log backup:

Log backups

If you have chosen Full recovery, you must create Log backups regularly. Log backups ensure that the database log file does not fill up the storage media where backups are stored.

Enter this command for a Log backup:

```
BACKUP LOG MhmDb
TO DISK = 'D:\Emerson\BU\MhmDb_Log.bak';
```

This copies all transactions in the log, including those that are not yet committed.

Tip

Emerson recommends creating Log backups every 60 minutes. However, if you run 24 backups in a day, you would still have one MhmDb_Log.bak file. MS SQL appends backups into a file.

If you want to stop the stacking of files, enter this command:

```
BACKUP LOG MhmDb
TO DISK = 'D:\Emerson\BU\MhmDb_Log.bak'
WITH INIT, FORMAT;
```

18.4 Restore AMS ARES Platform and AMS Machine Works databases

If you need to restore any of the AMS ARES Platform databases or the AMS Machine Works database, contact your IT department or call Emerson Product Support to guide you on the proper restore procedure.

19 Troubleshooting

Installation

Error	Background	Solution
The required port to install the AMS ARES Platform is used by another application	Port 80 and port 443 are required and used by the AMS ARES Platform. If these ports are not available or used by another application, open up the ports or redirect the website using these ports.	1. Launch IIS Manager. 2. On the Connections pane, expand PC name > Sites. 3. Click Default Web Site. 4. On the Actions pane, click Bindings. 5. On the Site Bindings page, select port 80 or port 443 and click Edit. 6. On the Edit Site Binding page, enter another port number, and click OK.
.NET Framework 3.5 needs to be installed	.NET Framework is needed to install the AMS ARES Platform. Some operating systems do not have .NET Framework automatically installed/ enabled.	**Note** You need an Internet connection to enable .NET Framework 3.5. **In Windows Server 2012:** 1. Launch Server Manager. 2. Click Manage > Add Roles and Features. 3. In the Add Roles and Features Wizard, click Next. 4. Select Role-based or feature-based installation and click Next. 5. Select the server where you want to install the AMS ARES Platform and click Next. 6. Click Next on the Select server roles page. 7. In the Select features page, expand the .Net Framework 3.5 Features, check the .NET Framework 3.5 (includes .NET 2.0 and 3.0) check box, and click Next. 8. Click Install. See KBA NK-1600-0300 for more information on how to enable .NET 3.5 for other operating systems.
Installation failure	Installation may fail for several reasons.	See the installation logs for additional information on the cause of the installation failure. Installation logs are in C:\Users\<username>\AppData\Roaming\Emerson_ADMLogs\<random GUID folder>.
		A probable cause of installation failure is the total length of the installation path. It should not exceed 260 characters. Shorten or change the installation path.

Error	Background	Solution
		You may need to change your computer name before installing the AMS ARES Platform. Special characters (< > ; : " * + = \ | ? , _ !), accented characters, and other multibyte characters in a computer name can cause problems and interfere with a successful installation of the AMS ARES Platform. A valid computer name can have numbers 0-9, uppercase and lowercase letters A-Z, and the hyphen (-). Computer names cannot have only numbers, nor can they contain spaces.
		Use the same server setting, either IP address or server name as the ARES Platform configuration, when installing or upgrading, components, ASIs, asset extensions, or platform extensions. For example, when you choose the Use Server Name option in the Server and Port Binding Configuration screen during the ARES Platform installation, you must enter the server name of the ARES Platform. Failure to use the same configuration as the AMS ARES Platform when installing or upgrading components, ASIs, and platform extensions may cause the installation to fail and you will need to uninstall and reinstall the AMS ARES Platform or any ASIs, asset extensions, and platform extensions to configure the same server setting.
		Ensure the Windows Update service is running. **Note** Windows Update service is different from automatic updates. If you turn off automatic updates on Windows 7 OS, make sure the Windows Update service is not unintentionally turned off.
		Always run install.exe rather than setup.exe to install the AMS ARES Platform and its components. Installation will fail if you run setup.exe and .NET Framework 3.5.1 is not yet installed on the system. Running install.exe checks this requirement for proper installation to continue.

Error	Background	Solution
		If you chose to have the database on a separate server from where the AMS ARES Platform is installed, you must enable TCP/IP and the SQL Server (EMERSONCSI) and SQL Server Browser services have to be running on the database server. **To enable TCP/IP:** 1. Launch SQL Server Configuration Manager. 2. On the left pane, expand the SQL Server Network Configuration node. 3. Select the Protocols for EmersonCSI. 4. On right pane, right-click TCP/IP and select Enable. **To enable the services:** 1. Launch SQL Server Configuration Manager. 2. On the left pane, select SQL Server Services. 3. On the right pane, right-click SQL Server (EMERSONCSI) and select Start. 4. Right-click SQL Server Browser and select Start.
		AMS ARES Platform installation will fail if there are database files from a previous installation in the EmersonCSI\Data folder. You need to remove the database files from a previous installation. See Knowledge Base Article NK-1600-0344 for a complete list of database files to be removed.
Error when manually installing SQL Server 2014	**Note** During default installation, Microsoft SQL Server Express is automatically installed and configured for the AMS ARES Platform. There is no need to install SQL Server 2014 if there is no SQL Server currently installed on the AMS ARES Platform server. If you will manually install SQL Server 2014, make sure the account running the SQL Server setup has rights to back up files and directories, rights to manage auditing and the security log, and the right to debug programs.	1. Launch Control Panel. 2. Go to Administrative Tools > Local Security Policy. 3. Navigate to Local Policies > User Rights Assignment. 4. Double-click the Back up files and directories policy. 5. Check to see if the user account running the SQL Server setup is listed. If it is not, click Add User or Group to add it, and click OK to close the dialogs. 6. Double-click the Debug programs policy. 7. Check to see if the user account running the SQL Server setup is listed. If it is not, click Add User or Group to add it, and click OK to close the dialogs. 8. Double-click the Manage auditing and security log policy. 9. Check to see if the user account running the SQL Server setup is listed. If it is not, click Add User or Group to add it, and click OK to close the dialogs.

Launching Apps

Error	Background	Solution
Cannot launch AMS ARES Platform apps in Internet Explorer	If Enhanced Security Configuration is enabled in Internet Explorer, the AMS ARES Platform server URL must be added to the list of trusted sites.	In Internet Explorer: 1. Click Tools > Internet Options. 2. Select the Security tab and click Trusted sites. 3. Click Sites. 4. In the Add this website to the zone field, enter http://[server], where [server] is the computer name or IP address of the AMS ARES Platform server. 5. Click Add.

Vibration Analyzer

Error	Background	Solution
Error when printing Image Summary Reports	When Windows update KB3098779 is present on your AMS ARES Platform installation, it results in error when printing Image Summary Reports.	Uninstall Windows update KB3098779. 1. Go to the Control Panel. 2. Click Programs > Programs and Features > View installed updates. 3. Select KB3098779 and click Uninstall. 4. Click Yes.

Appendix A
Internet Information Services (IIS) Reference

Module	Application Pool	Site
	ARES_Platform_Apps	EmersonCSI
ARES Platform App	ARES_Platform_Apps	\AssetExplorer
	ARES_Platform_Apps	\AssetView
	ARES_Platform_Apps	\DM
	ARES_Platform_Apps	\EventViewer
	ARES_Platform_Apps	\UserManager
	ARES_Platform_Svcs	\Actions
	ARES_Platform_Svcs	\Help
	ARES_Platform_Svcs	\LicenseMgmt
	ARES_Platform_Svcs	\MobileServices
	ARES_Platform_Svcs	\Notifications
	ARES_Platform_Svcs	\PlantEvents
	ARES_Platform_Svcs	\PlantImages
	ARES_Platform_Svcs	\PlantMessages
	ARES_Platform_Svcs	\PlantMgmt
	ARES_Platform_Svcs	\PlantStatus
	ARES_Platform_Svcs	\PluginInfo
	ARES_Platform_Svcs	\Reference
	ARES_Platform_Svcs	\Resources
	ARES_Platform_Svcs	\RuntimeDataServices
	ARES_Platform_Svcs	\Security
	ARES_Platform_Svcs	\Settings
EWG ASI	EWGASI	\EWGASI
AMS Machine Works	ARES_MW_Apps	\MachineEditorLite
	ARES_MW_Apps	\VibApp
	ARES_MW_MHMDD	\MHMDD
	ARES_MW_StatusEval	\StatusEval
	ARES_MW_Svcs	\CaseHistory
	ARES_MW_Svcs	\Historian
	ARES_MW_Svcs	\HostServices
	ARES_MW_Svcs	\MachineConfigLite

Module	Application Pool	Site
AMS Device Manager ASI	DeviceManager	\DeviceManager

Appendix B
SQL databases

Module	Database
ARES Platform App	EventDb
	FrameworkDb
	ImageDb
	MessageDb
AMS Machine Works	MHMDb

Appendix C
Automatic backup for Tier-1 installations

Automatic backups are available for Tier-1 installations and are triggered by a scheduled task named AMS ARES Platform SQL Maintenance.

You can select automatic backups during the AMS ARES Platform installation when you select a Tier-1 installation (typical single installation or network server system).

The scheduled task is triggered at different times depending on the type of installation.

- For a standalone system, it occurs on startup
- For a server OS, it is scheduled for 2:00 AM (by default)
- The scheduled task runs under the native "System" account

Processing for each AMS ARES Platform database:

1. Sets the AMS ARES Platform databases to the simple recovery model
2. Processes a database backup
3. Shrinks the database log files

It retains the two most recent backups. Files are located by default under C:\EMERSONCSI \DATA\Backups.

Note

Automatic backups are only available with new installations. If you upgrade from the previous version, this feature is not available.

Appendix D
Requirements for ASI-only installation on a separate server

During the installation of any AMS ARES Platform ASI's, the ASI installation must update the AMS ARES Platform database. This adds information so that the AMS ARES Platform is aware of the ASI, and adds images, functionality, and buttons so that it can interact seamlessly with the ASI.

D.1 Set up the ASI server before installing the ASI on a Tier-1 system

This action requires connection to the SQL Server hosting the database that has rights to insert information into AMS ARES Platform tables; this is known as “Action Registration”. The SQL communications usually require additional access through server and network firewalls. The ASI server only needs these firewall exemptions for Action Registration during installation. If the SQL communication is not available, you will get "Action Registration" failures during the ASI installation. The firewall exceptions described here can be restored (removed) after the ASI installation is complete.

Prerequisites

- This is a Tier-1 installation. The AMS ARES Platform server hosts the databases.
- The AMS ARES Platform installation is complete.

Procedure

On the target server, the AMS ARES Platform server, and any intervening firewalls, enable these ports for TCP/IP and SQL communication between servers:

SQL Communication requires ports 1433, 1434, and a dynamic port assigned to the **EMERSONCSI** SQL instance.

Table D-1: Temporary inbound/outbound communication settings required during ASI installation

Server	Direction	Type	Connections	Apply	Remote computers[2]
ASI Server	Inbound	TCP (all local ports)	Allow Secure	Domain[1]	AMS ARES Platform
ASI Server	Outbound	TCP (all local ports)	Allow Secure	Domain[1]	AMS ARES Platform
ASI Server	Outbound	UDP 1434	Allow Secure	Domain[1]	AMS ARES Platform
ASI Server	Inbound	UDP 1434	Allow Secure	Domain[1]	AMS ARES Platform

Table D-1: Temporary inbound/outbound communication settings required during ASI installation *(continued)*

Server	Direction	Type	Connections	Apply	Remote computers[2]
AMS ARES Platform	Inbound	TCP (all local ports)	Allow Secure	Domain[1]	ASI Server
AMS ARES Platform	Outbound	TCP (all local ports)	Allow Secure	Domain[1]	ASI Server
AMS ARES Platform	Inbound	UDP 1434	Allow Secure	Domain[1]	ASI Server
AMS ARES Platform	Outbound	UDP 1434	Allow Secure	Domain[1]	ASI Server

[1] Assuming you are on a domain. If desired you can select Domain, Private, and Public.

[2] You may have to save the rule and then edit it to apply the server restriction.

Postrequisites

- Install the selected ASI on the target server.
- You can remove these exceptions after the ASI installation is complete and if necessary, restore traffic rules across TCP ports between the AMS ARES Platform server and the target server.

Appendix E
Requirements for separate server (Tier-2) installations

E.1 Separate server (Tier-2) installation

A Tier-2 installation is where AMS ARES Platform is installed on one server, the AMS ARES Platform server, and the databases are hosted on a separate SQL database server. For a Tier-2 installation, you need to set up the SQL database server and the AMS ARES Platform server in a specific order.

1. Set up the separate SQL Server for a Tier-2 installation. See *page 89*.
2. Set up the AMS ARES Platform server before a Tier-2 installation. See *page 92*.
3. Install the AMS ARES Platform on the AMS ARES Platform server. During installation, choose a Tier-2 installation and supply information about the database server. See *page 20*.

Important

After the platform installation, do not start using the software or install other components until you have completely set up the system for a Tier-2 installation.

4. Finish post-installation set up on AMS ARES Platform server. See *page 93*.
5. Set up the ASI server before installing an ASI on a Tier-2 system. See *page 95*.

Note

This is only required if you install the ASI on a separate server.

E.2 Set up the separate SQL Server for a Tier-2 installation

Important

Complete these steps on the separate SQL Server before installing the AMS ARES Platform on the AMS ARES Platform server.

Prerequisites

The AMS ARES Platform is NOT yet installed on the AMS ARES Platform server.

Procedure

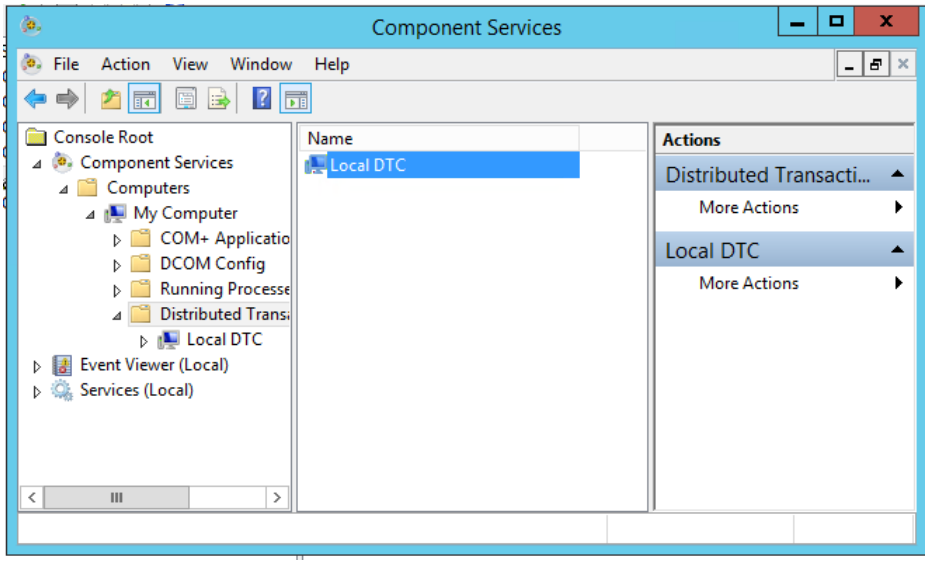
1. On the separate SQL server, ensure the server meets the following requirements to host AMS ARES Platform databases.

   - SQL 2014 is the minimum version supported
   - SQL Instance name must be **EMERSONCSI**
   - Remote connections must be enabled
   - Mixed authentication (Windows & SQL) must be enabled
   - TCP/IP protocol must be enabled for the **EmersonCSI** SQL Server Network Configuration (SQL Server Configuration Manager)
   - SQL Browser must be running and set to auto-start
   - A static port for the **EMERSONCSI** SQL Instance must be set.

2. Update settings for Microsoft Distributed Transaction Coordinator (MDTC):

   a. In Windows Component Services, browse to Component Services > Computers > My Computer > Distributed Transaction Coordinator > Local DTC.

Figure E-1: Windows Component Services expanded to Local DTC



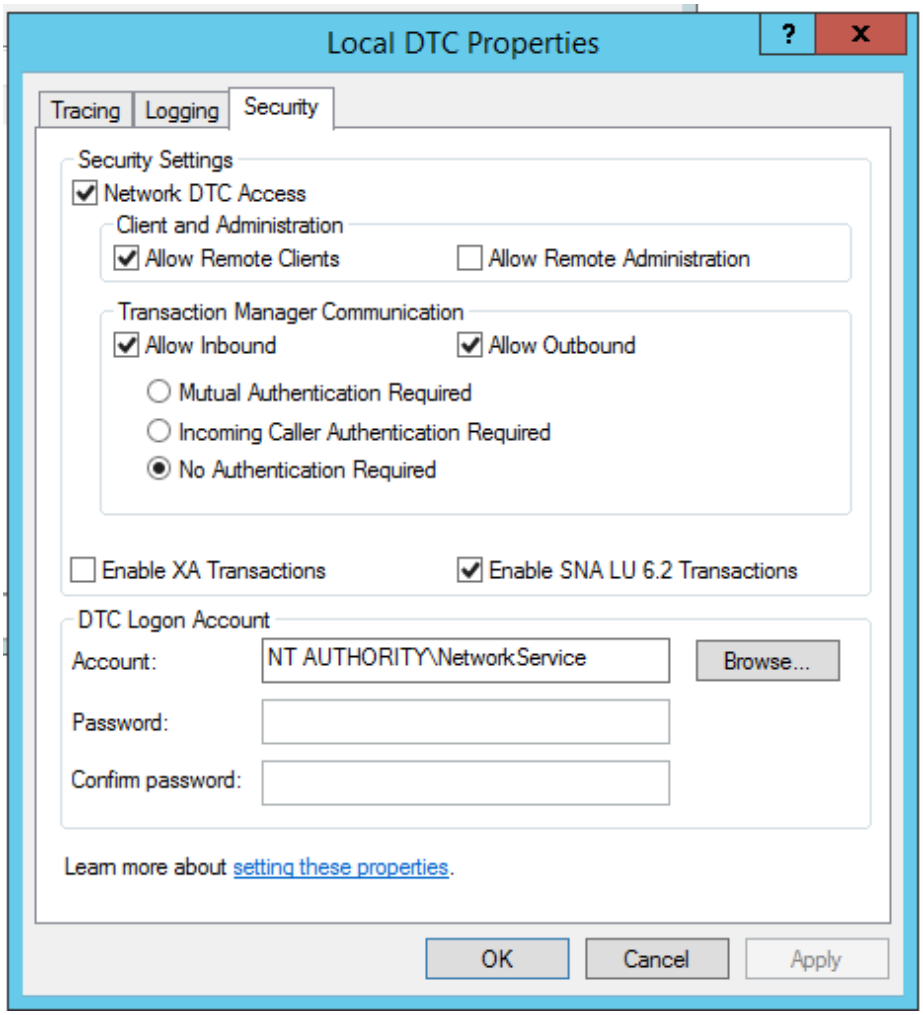
   b. Select More Actions > Properties.

   c. In the Local DTC Properties dialog, select the Security tab and change the following settings:

      - Check Network DTC Access.
      - Check Allow Remote Clients.
      - Check Allow Inbound.
      - Check Allow Outbound.
      - Select No Authentication Required.
      - Check Enable SNA LU 6.2 Transactions.

- The DTC Logon Account should be "NT AUTHORITY\Network Service"

Figure E-2: Local DTC Properties dialog with required settings



3. Set communication ports and firewall rules.

Inbound communication	Firewall rule
Distributed Transaction Coordinator (RPC)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (RPC-EPMAP)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (TCP-In)	Predefined firewall rule in Server 2012 R2
UDP Port 1434	SQL Browser
TCP Port 1433	SQL

Inbound communication	Firewall rule
EMERSONCSI SQL instance TCP port	SQL

Outbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-Out)	Predefined firewall rule in Server 2012 R2
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

E.3 Set up the AMS ARES Platform server before a Tier-2 installation

When your SQL database is on a separate server from the AMS ARES Platform, you need to change firewall settings on the AMS ARES Platform server before and after installing the platform, and before using the software. This section covers the settings you need to change on the AMS ARES Platform server before installing the software.

Prerequisites

Set up the separate SQL Server for a Tier-2 installation.

Procedure

On the AMS ARES Platform server, enable the ports for SQL communication to and from the server.

Inbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

Outbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port	SQL

Postrequisites

Make sure you have "sa" rights on the EMERSONCSI SQL instance or know the credentials of the SQL account that has those rights before proceeding with AMS ARES Platform installation.

E.4 Tier-2 post-installation setup

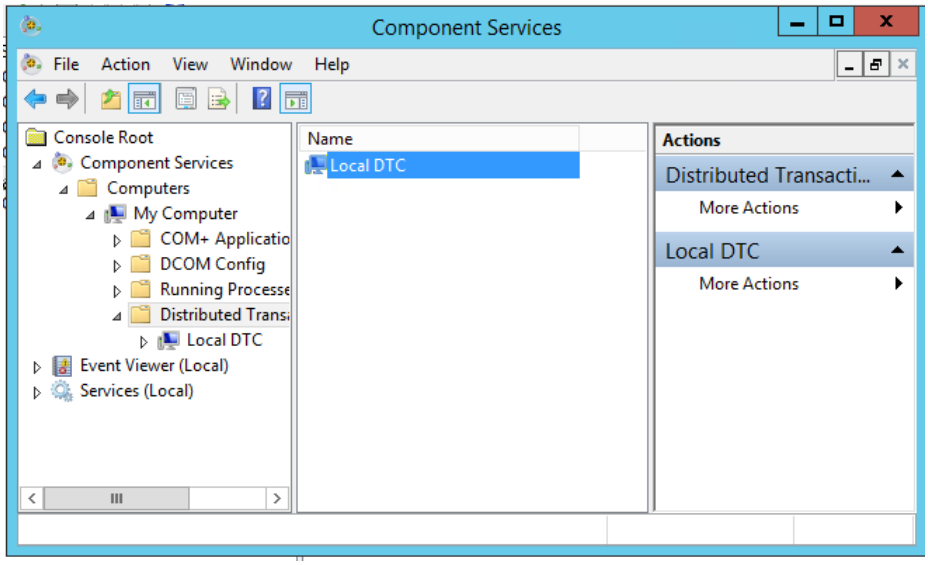
Complete this setup on the AMS ARES Platform server after installing the AMS ARES Platform and before you start using the software or installing other components.

Procedure

1. Update settings for Microsoft Distributed Transaction Coordinator (MDTC):

   a. In Windows Component Services, browse to Component Services > Computers > My Computer > Distributed Transaction Coordinator > Local DTC.

Figure E-3: Windows Component Services expanded to Local DTC



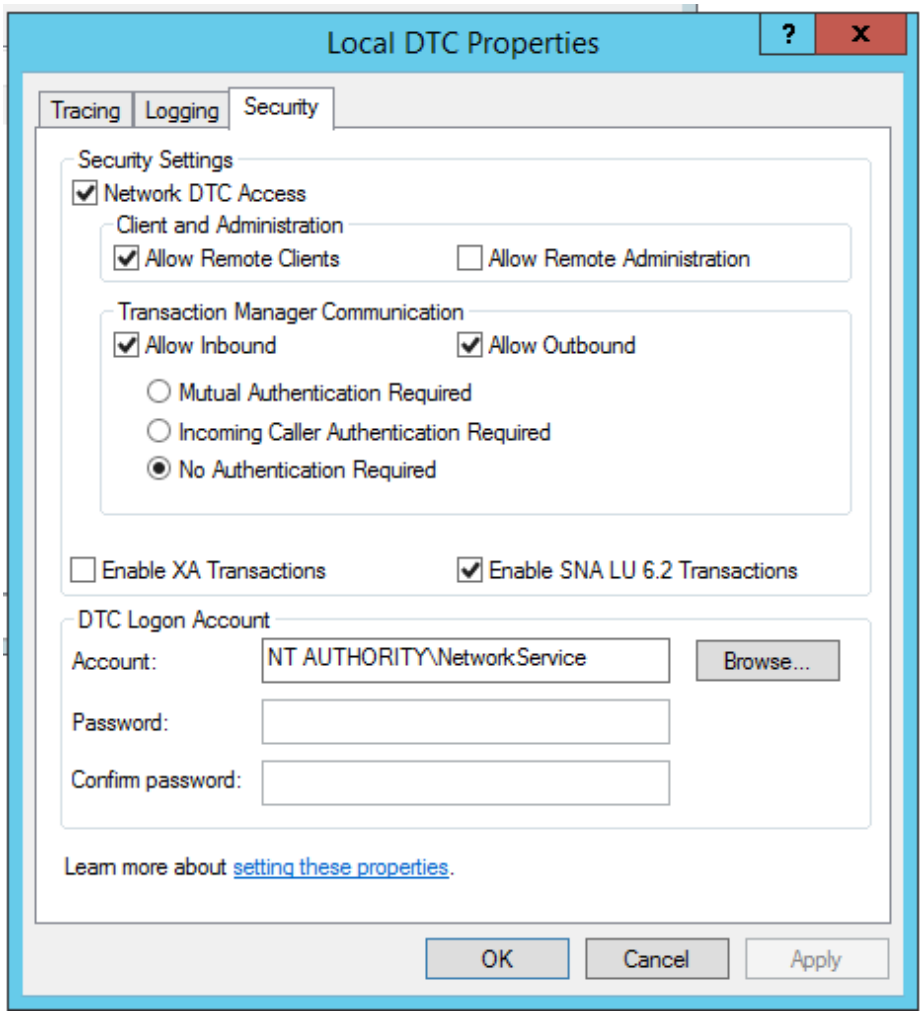
   b. Select More Actions > Properties.

   c. In the Local DTC Properties dialog, select the Security tab and change the following settings:

   - Check Network DTC Access.
   - Check Allow Remote Clients.
   - Check Allow Inbound.
   - Check Allow Outbound.
   - Select No Authentication Required.
   - Check Enable SNA LU 6.2 Transactions.

- The DTC Logon Account should be "NT AUTHORITY\Network Service"

Figure E-4: Local DTC Properties dialog with required settings



2. Enable the predefined firewall rules to allow SQL communication.

Inbound communication	Firewall rule
Distributed Transaction Coordinator (RPC)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (RPC-EPMAP)	Predefined firewall rule in Server 2012 R2
Distributed Transaction Coordinator (TCP-In)	Predefined firewall rule in Server 2012 R2

Outbound communication	Firewall rule
Distributed Transaction Coordinator (TCP-Out)	Predefined firewall rule in Server 2012 R2

Note

These predefined rules are available on the AMS ARES Platform server after you install the AMS ARES Platform. If the rules are not present, you may need to re-install the AMS ARES Platform.

Postrequisites

Install other components on the AMS ARES Platform server, as needed.

E.5 Set up the ASI server before installing the ASI on a Tier-2 system

Note

This is only required if you install the ASI on a separate server.

This action requires connection to the SQL Server hosting the database that has rights to insert information into AMS ARES Platform tables; this is known as “Action Registration”. The SQL communications usually require additional access through server and network firewalls. The ASI server only needs these firewall exemptions for Action Registration during installation. If the SQL communication is not available, you will get "Action Registration" failures during the ASI installation. The firewall exceptions described here can be restored (removed) after the ASI installation is complete.

Prerequisites

- This is a Tier-2 installation. The AMS ARES Platform server does not host the databases. The databases are hosted on a separate SQL server.
- The AMS ARES Platform installation is complete.

Procedure

On the target server, and any intervening firewalls, enable the ports for SQL communication to the SQL database server.

Inbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port (static)	SQL

Outbound communication	Firewall rule
UDP Port 1434	SQL Browser
TCP Port 1433	SQL
EMERSONCSI SQL instance TCP port (static)	SQL

Postrequisites

- Install the selected ASI on the target server.
- You can remove these exceptions on the ASI server after the ASI installation is complete.

Appendix F
Device compatibility

CSI 9420 Wireless Vibration Transmitter

The AMS ARES Platform supports the latest and older versions of the CSI 9420.

Revision	Latest version	Older versions
HART/Universal	7	7
Field device	4	3
Software	6	3 and above
Hardware	5	1, 5
DD (Device Descriptor)	1	7, 8

You can view the revision information from a Field Communicator or from AMS Device Manager. See the CSI 9420 Reference Manual for more information.

Emerson Wireless Gateway

The AMS ARES Platform supports Emerson Wireless Gateway version 3.x.x., version 4.x.x., and later versions.

AMS Device Manager

The AMS ARES Platform supports AMS Device Manager version 13.1.1 and 13.5.

MHM-97911
Rev 1
2017

Emerson
835 Innovation Drive
Knoxville, TN 37932 USA
T +1 865-675-2400
F +1 865-218-1401
www.Emerson.com