Install Guide

Table of Contents

WIN-911 Installation 1
WIN-911 4.21.5 System Requirements 1
WIN-911 Server 1
WIN-911 Client 3
SQL Server Requirements 4
Option 1: Allow WIN-911 to setup SQL 5
Option 2: Install higher edition of SQL Server prior to installing WIN-911 5
Option 3: Install SQL Server remotely prior to installing WIN-911 5
Data Source (SCADA) Compatibility Matrix 5
Installation Path 6
WIN-911 System - Distributed or Standalone 7
WIN-911 Standalone System Setup 8
SQL Server Installation 12
InstallShield Wizard 12
Modifying WIN-911 22
Adding features to your existing WIN-911 installation 22
Removing features from your existing WIN-911 installation 23
WIN-911 Network Module Mapper 23
Licensing WIN-911 24
Create Distributed System 31
SQL Server Installation 34
InstallShield Wizard 35
Join Distributed System 45
SQL Server Installation 49
InstallShield Wizard 49
Getting Started with WIN-911 63
Accessing the WIN-911 Configuration 63
Configure a Notification Method 65
Gateways 65
Connections 67
Configuring Escalation 69

Strategies 70
Configure Data Sources 72
Sources 72
Alarms 73
Labels 74

WIN-911 Installation

WIN-911 4.21.5 System Requirements

WIN-911 Server

- Personal Computer with dual core processor. Quad core processor is recommended.

  Please note: Two physical processor cores are required. A single processor core with hyper-threading enabled will not meet the system requirements.

- 4 GB of RAM or more. Additional RAM is recommended if additional programs are to be run simultaneously.
- 4 GB of hard disk space.
- Compatible OS environment - one of the following (64-bit OS) with all Windows updates applied:
  Please note: Since Microsoft operating systems feature continuous updates, you should run the Windows update feature to get the most up to date software.

  - Microsoft® Windows® 7 Service Pack 1
  - Microsoft® Windows® 8.1
  - Microsoft® Windows®10 (1809, 1903, 1909, and 2004), Professional Edition (or higher).
  - Microsoft® Windows® Server 2008 R2, Service Pack 1, Standard Edition (or higher).
  - Microsoft® Windows® Server 2012, Standard Edition (or higher).
  - Microsoft® Windows® Server 2012 R2, Standard Edition (or higher).
  - Microsoft® Windows® Server 2016 Standard Edition (or higher)
  - Microsoft® Windows® Server 2019 Standard Edition (or higher)

- Microsoft SQL Server 2008 R2 through 2017 (Express, Standard, and Enterprise Edition) Note: SQL Server 2014 SP2 Express (required for Windows 7 and Server 2008R2) requires Microsoft .NET 3.5.

- Internet Information Services (IIS). Application Initialization will be installed for IIS 7.5 (Windows 7/2008 R2).
- Microsoft .NET 4.5 required for install (.NET 4.8 Full will be installed)
- Optional Notification Hardware and Software:

VoIP to Analog Voice Calls	• Grandstream UCM6202 VoIP PBX required • Dedicated analog phone line (maximum of 2 phone lines) • *** Alternative to TAPI modems anywhere analog phone lines are available ***
SMS Text Messages	• RS-232/USB or Ethernet (network connected) Cellular Modem Recommended RS-232/USB: MultiTech MTC-H5, MTC-LVW2, MTC-LAT1, MTC-LNA4 Recommended Ethernet: MultiTech MTR-H5, MTR-LVW2, MTR-LAT1, Sierra Wireless RV50X • Ethernet modem required for virtual environments • Cellular account with unlimited text messages recommended
VoIP Calls	• SIP compatible VoIP Internet account or PBX • WIN-911 Recommended SIP provider for North America – SIP.US **Supported VoIP Providers**: Axvoice VoIPtalk SurVoIP **Supported VoIP PBX Systems** Ozeki Phone System XE Tribox Cisco Unified CM

	OpenSER	PBXnSIP	Cisco Call Manager Express
	Asterisk	PBXpress	SipX ECS
	FreeSwitch	FreePBX	OpenSIP
	SwyzWare	Aasta MX-One	Elastix
	Asterisk Now	Kamailio	
Mobile-911	*** Mobile-911 will reach End of Life on December 21, 2021 *** • Broadband always-on Internet connection • iOS, Android and Blackberry devices for the Mobile-911 app		
Mobile	• Broadband always-on Internet connection • iOS (12 and up) and Android devices for the Mobile app		
Email	• Email server with a DEDICATED Email account from which WIN-911 can send alarm messages and receive acknowledgement and report requests. • POP/IMAP for incoming & SMTP for outgoing messages. • Email to SMS option not supported on all carriers and devices.		

WIN-911 Client

- Internet Explorer 10 and 11 for Windows

- Microsoft Silverlight 5.1.50918.0 (January 2019)

SQL Server Requirements

WIN-911 uses an SQL Server database to store its configuration data. If an SQL Server is not already on your computer then it is important to take into consideration the requirements of the different versions of SQL Server. You can opt for the WIN-911 Launcher to install SQL Server Express 2017 for you, which is good for small to medium configurations (5,000 data points or less).

Note to Windows 7 & Server 2008R2 users: SQL Server Express 2017 is not compatible with these operating systems. Therefore, you will need to install SQL Server Express 2014. This will require .NET 3.5 be installed prior to installing SQL Server Express 2014 available here:
https://win911na.blob.core.windows.net:443/files/Products/WIN-911//4.21.5/SQL2014.zip

For more information about specific requirements for SQL Server installation and configuration, see Microsoft documentation available online.

"https://msdn.microsoft.com/en-us/library/bb545450.aspx"

- WIN-911 is not compatible with SQL Server 2000.
- In order to authenticate with a remote SQL Server, identical credentials must be configured on both machines, and the SQL instance must be configured with those credentials.

Option 1: Allow WIN-911 to setup SQL

If you install WIN-911 and an SQL Server instance named "WIN911" is not found, SQL Server 2017 Express can be installed by the Install Launcher. This version is suited for small configurations, up to 5,000 data points, and is ideal for a single-node.

Option 2: Install higher edition of SQL Server prior to installing WIN-911

If a compatible version of SQL Server is already installed and an instance named "WIN911" is available on the network or locally, WIN-911 Launcher installation will continue without interruption. If an incompatible version (SQL Server 2000) is present, the process will be halted and you must remove it before the installation can continue.

Option 3: Install SQL Server remotely prior to installing WIN-911

If you would like to install SQL Server Express on a different computer than the WIN-911 host, you should copy the *SQL Server Express* folder provided with the WIN-911 install to the desired computer. Ensure that the installing user is an administrator with the same credentials as WIN-911's host user. Then run the *WIN911SQL* executable located in the root of the *SQL Server Express* folder.

Note: Higher editions of SQL are also supported remotely.

Data Source (SCADA) Compatibility Matrix

WIN-911 is compatible with the following data source version:

Data Source (SCADA - HMI)	Versions
OPC DA	OPC Data Access Classic 1.0, 2.0, 3.0
InTouch®	10.1, 2012 (10.5), 2012 R2 (10.6), 2014 (11.0), 2014 R2 (11.1), 2017 Updates 1, 2, & 3, 2020, 2020 R2
InTouch Edge HMI®	8.1 SP3, SP4, 2020, 2020 R2
InTouch ME®	8.1, 8.1 SP1
InduSoft Web Studio®	8.1, 8.1 SP1, SP3, SP4
System Platform®	2012 R2 SP1, 2014 R2, 2014 R2 SP1, 2017 Updates 1, 2, & 3, 2020, 2020 R2
FactoryTalk Alarms and Events®	6.00.00, 6.10.00, 7.00.00, 8.00.00, 8.10.00, 8.20.00, 9.00.00, 10.00.01, 11.00.00
iFIX®	5.5, 5.8, 5.8 SP1, 5.8 SP2, 5.8 SP2 R2, 5.9, 6.0, 6.1, 6.5
CIMPLICITY®	10, 11, 11.1

Installation Path

WIN-911 will install files in two locations on your system, C:\inetpub\wwwroot and C:\Program Files (x86).

WIN-911 System - Distributed or Standalone

The WIN-911 System is defined as the sum-total of all the modules that make up the WIN-911 instance. These modules can be installed on a single computer as a standalone system or distributed over several computers (EG: allowing a notifier module access to the Internet from the DMZ while the rest of the system resides on the plant network). Each of these modules fall into one of three categories: support, source, and notifier modules. Each module is independently capable of performing its unique duties and yet they interactively depend on each other in order to fullfil the WIN-911 mission.

Support Modules:
- Dispatcher
- Navigation
- Reporting

Source Modules:
- InTouch
- InTouch Edge HMI
- System Platform
- CIMPLICITY
- iFIX
- FactoryTalk Alarms and Events
- OPC DA

Notifier Modules
- Mobile
- Mobile-911
- Email
- SMS
- Voice

To perform a standalone system installation, the user will be required to select at least the minimum manifest of modules that make up a complete WIN-911 System. These include support modules, at least

one source module and one notifier. When selecting a distributed WIN-911 System installation, the minimum module requirements are relaxed to allow physical distribution.

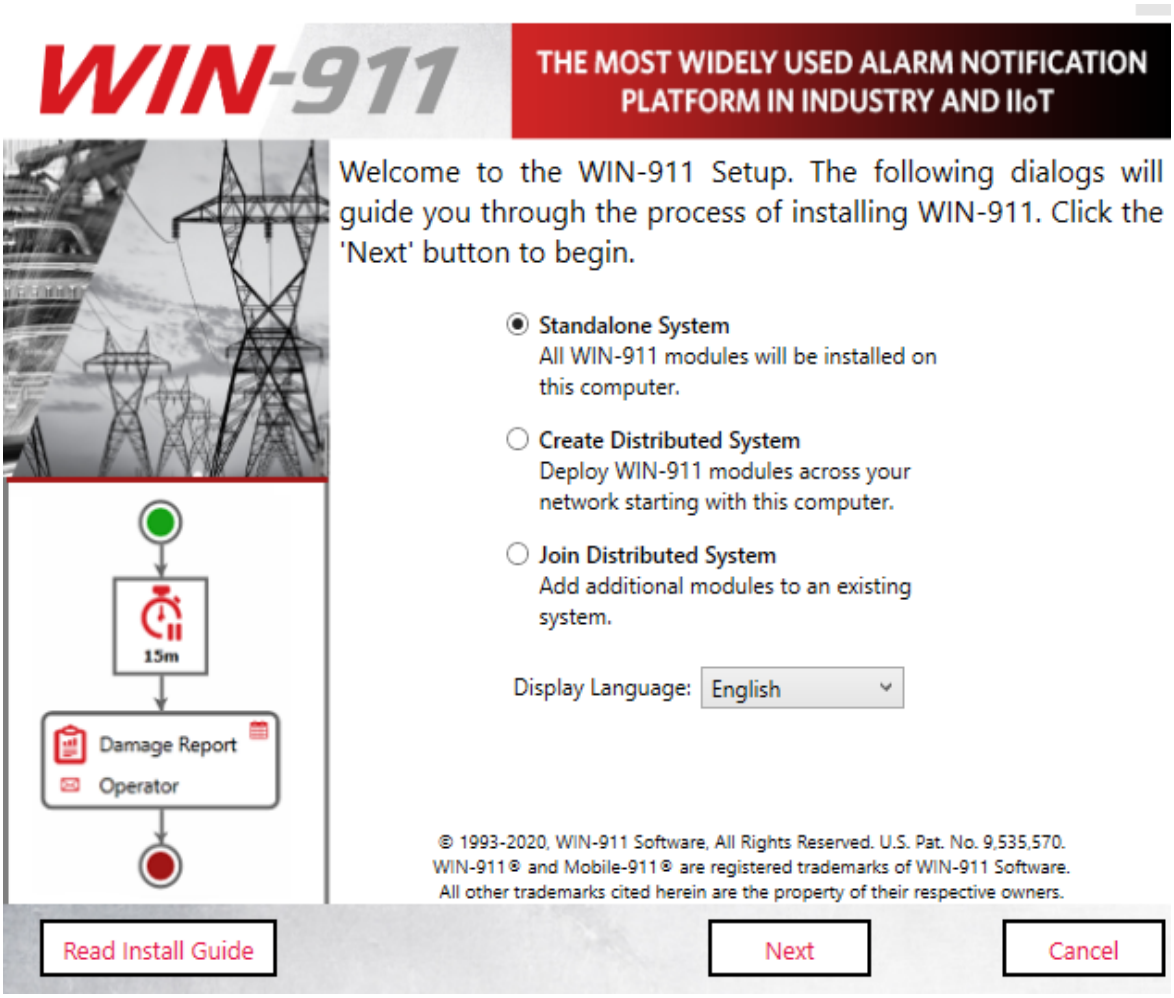
To create a distributed system, you will need to define a WIN-911 System network (Create Distributed System) and then deploy the remaining modules on each of the remote nodes that will comprise your WIN-911 System (Join Distributed System).

The following section discusses the creation of a standalone system.

WIN-911 Standalone System Setup

The WIN-911 Launcher requires .NET 4.5 (or higher). If the target machine lacks this framework, you will need to add the framework in order to commence. In Windows 8.1, this can be done through *Programs and Features> Turn Windows features on or off*. With Server operating systems use *Server Manager> Add roles and features*. Additionally, you can find an installer for the framework in the support sub folder of the installation media or online.

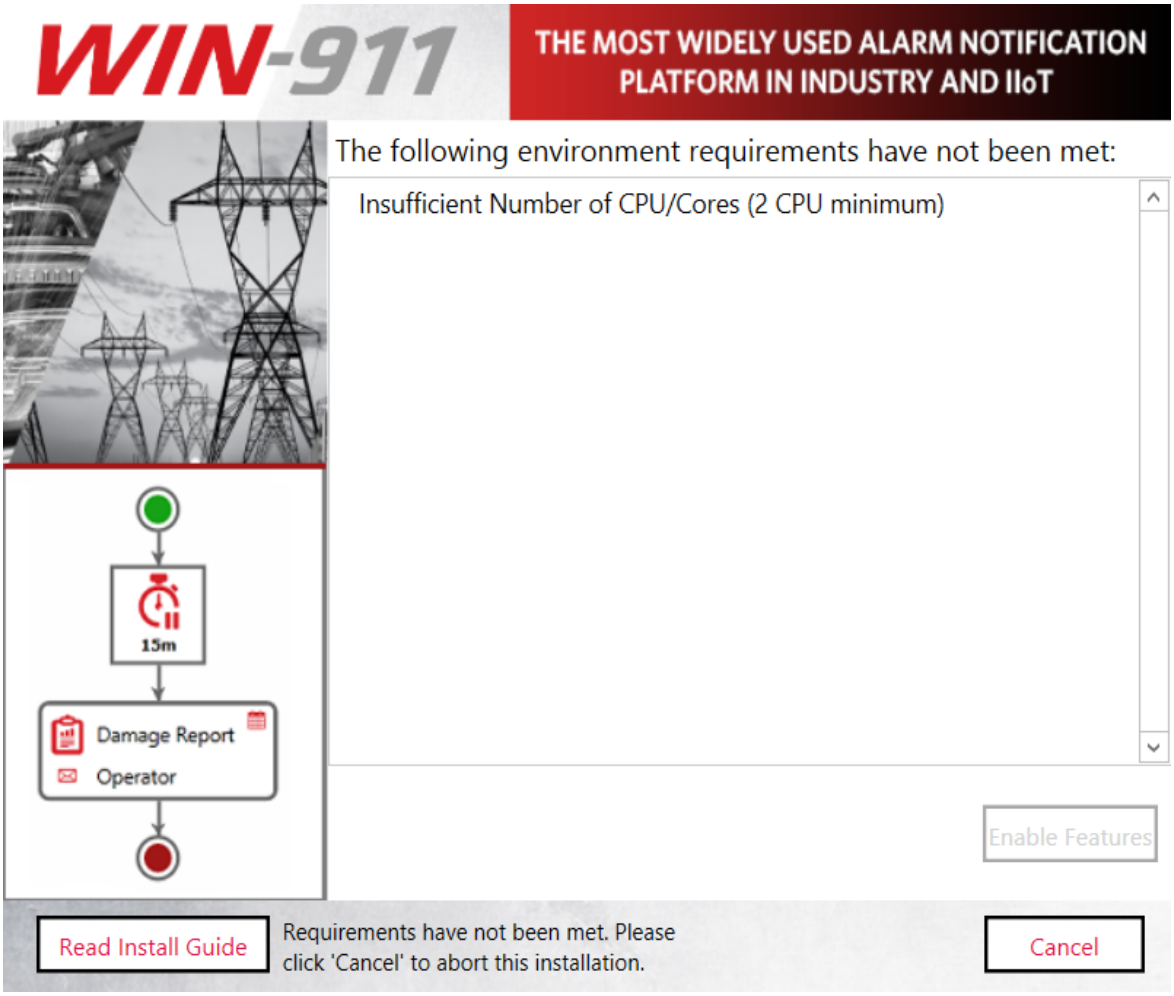
To install WIN-911



Attention: When using a language other than English select it here.

Click **"Next"** to begin WIN-911 Setup.

The installation program checks whether or not the environment requirements are met.



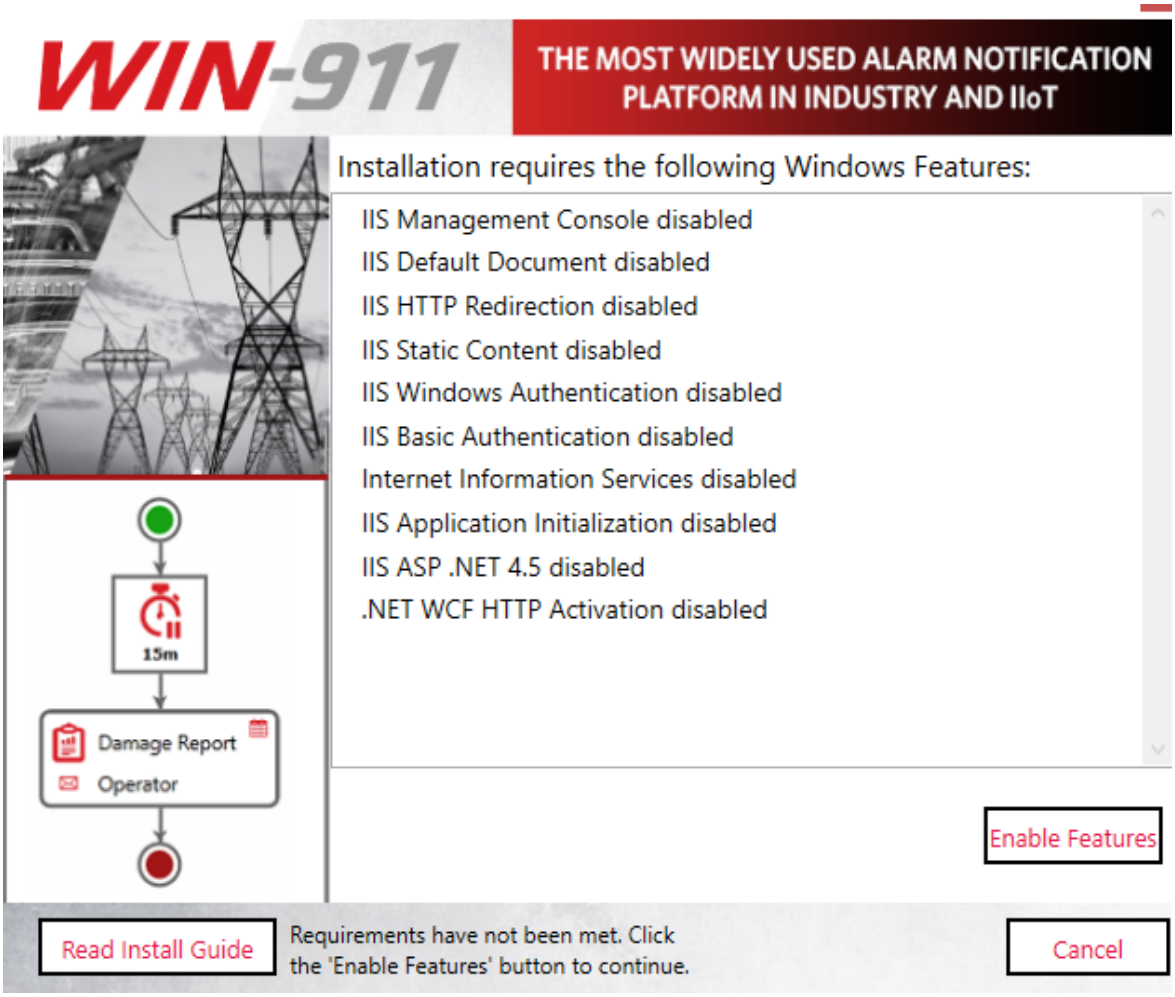
Such environment requirements include:

- Supported 64-bit OS
- Sufficient minimum disk space
- Sufficient minimum processors/cores
- Installing user be a member of local administrator's group

See WIN-911 4.21.5 System Requirements at the top of this document for more information.

Note: If these requirements are met, this page will not appear.

The installation program will then check for the required features.



Feature requirements include the following:

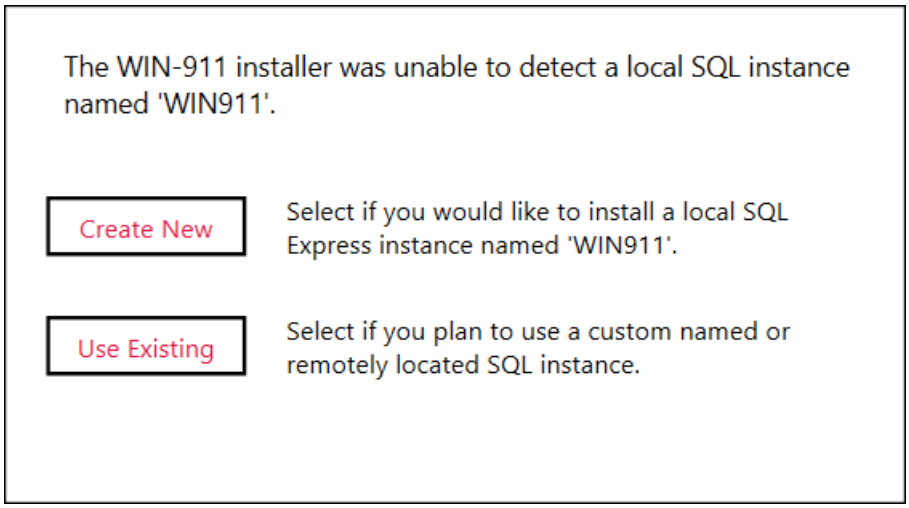
- Microsoft .NET 4.8
- Windows Edition and Feature Set Detection
- IIS Features: Application Initialization, Basic Authentication, Windows Authentication, HTTP Redirection and ASP.NET 4.5, HTTP Activation

Any missing feature can be enabled by clicking the Enable Features button at the bottom right.

Note: If these requirements are met, this page will not appear.

SQL Server Installation

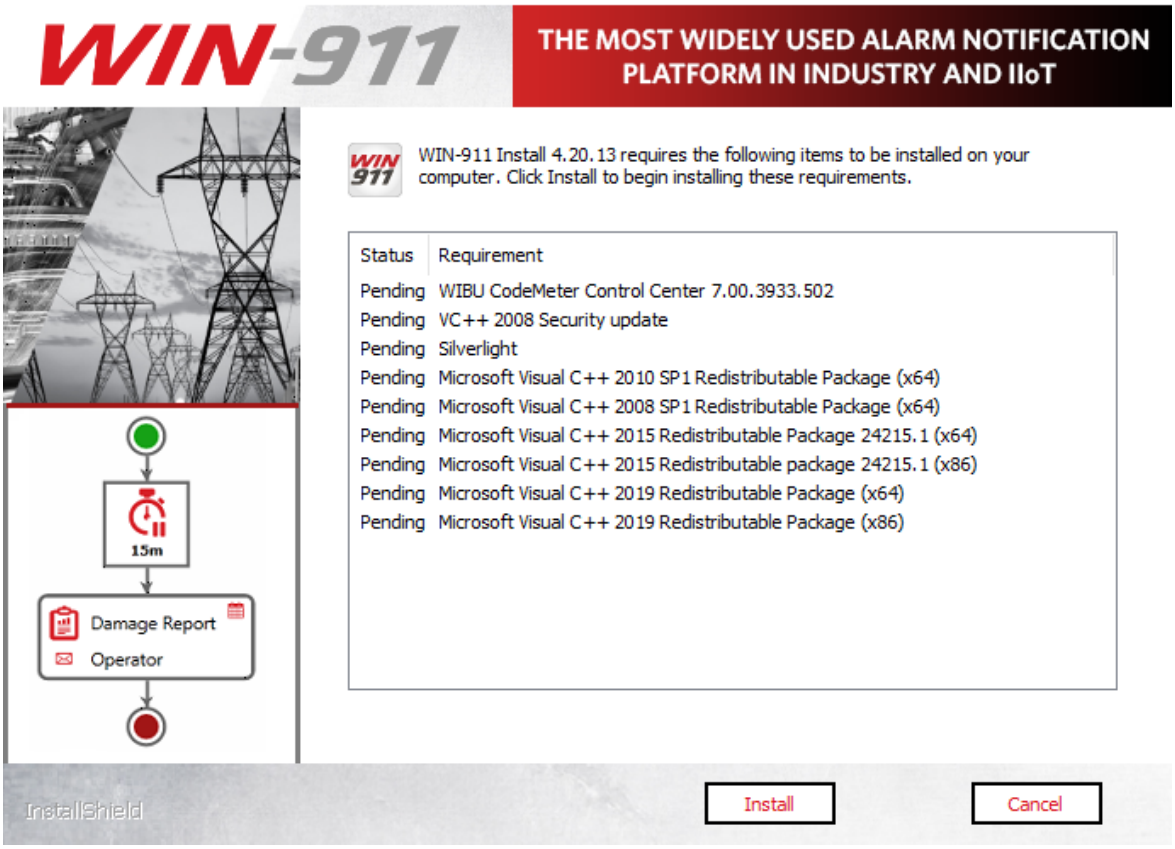
The install script will check the WIN-911 host for an SQL Server instance named "WIN911." If there is no suitable SQL Server, the following pop-up will appear:



This is an optional step and is not required in order to continue with the installation, but WIN-911 cannot be used until the SQL Server requirement is satisfied.

Note: if you are upgrading, you should select "Use Existing" to keep your existing data.

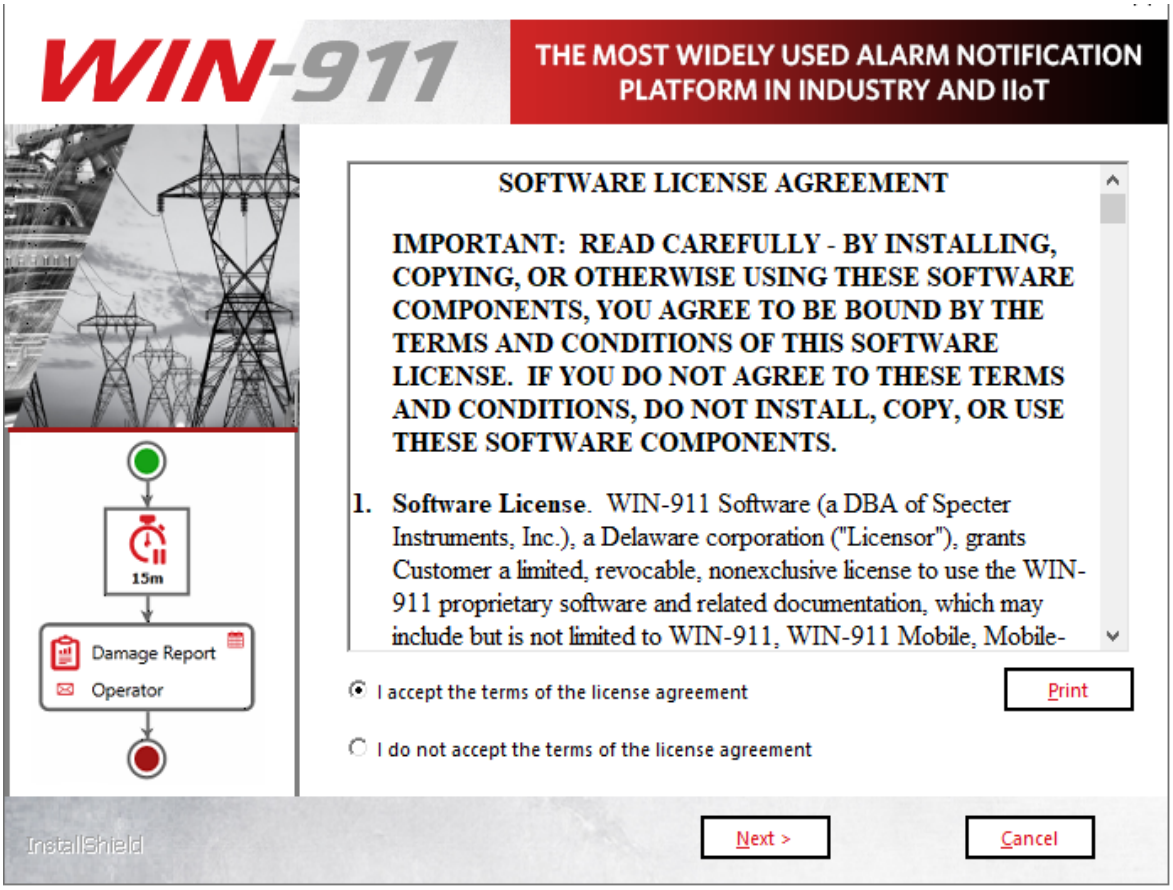
InstallShield Wizard



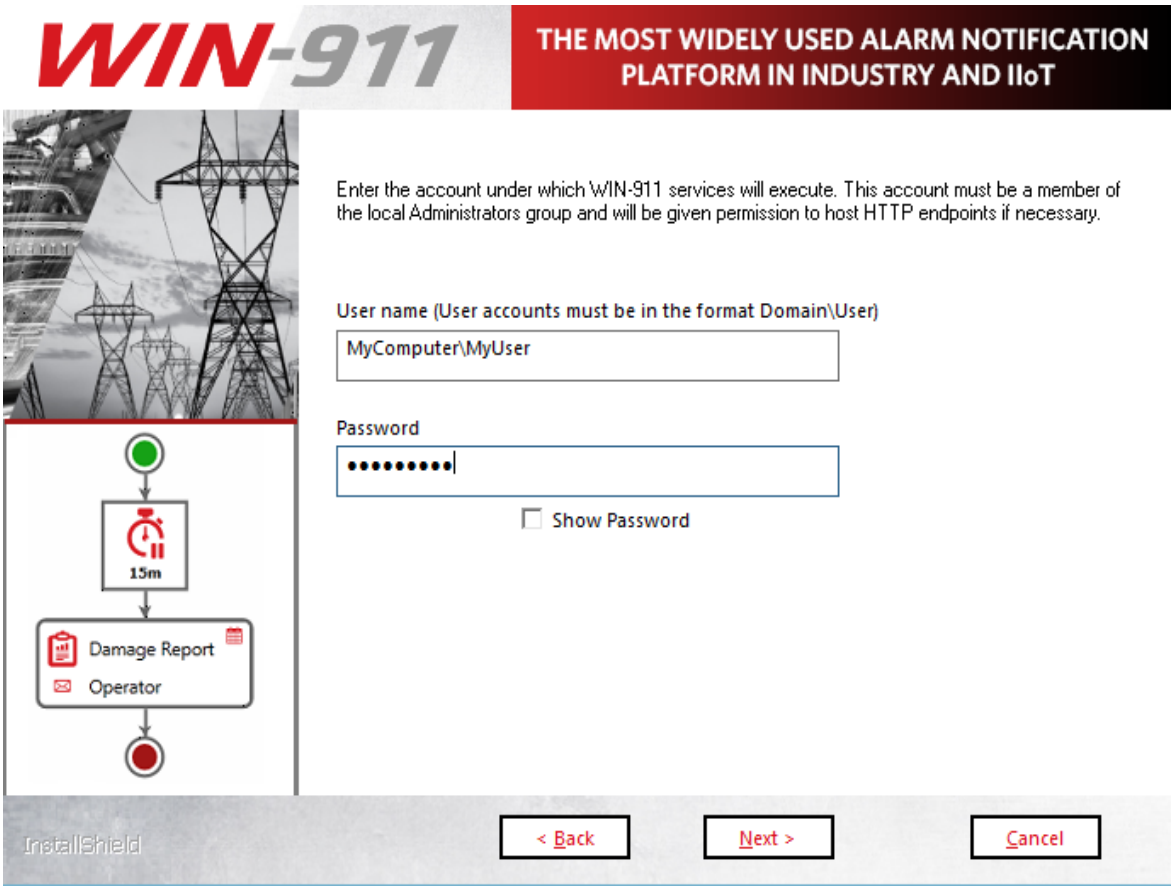
Depending on the state of .NET Framework 4.8, you may need to reboot prior to continuing.

If requested, select Yes and the install process will resume automatically once the reboot is performed.

The WIN-911 InstallShield wizard will now guide you through the WIN-911 setup. Click **"Next"** to continue.

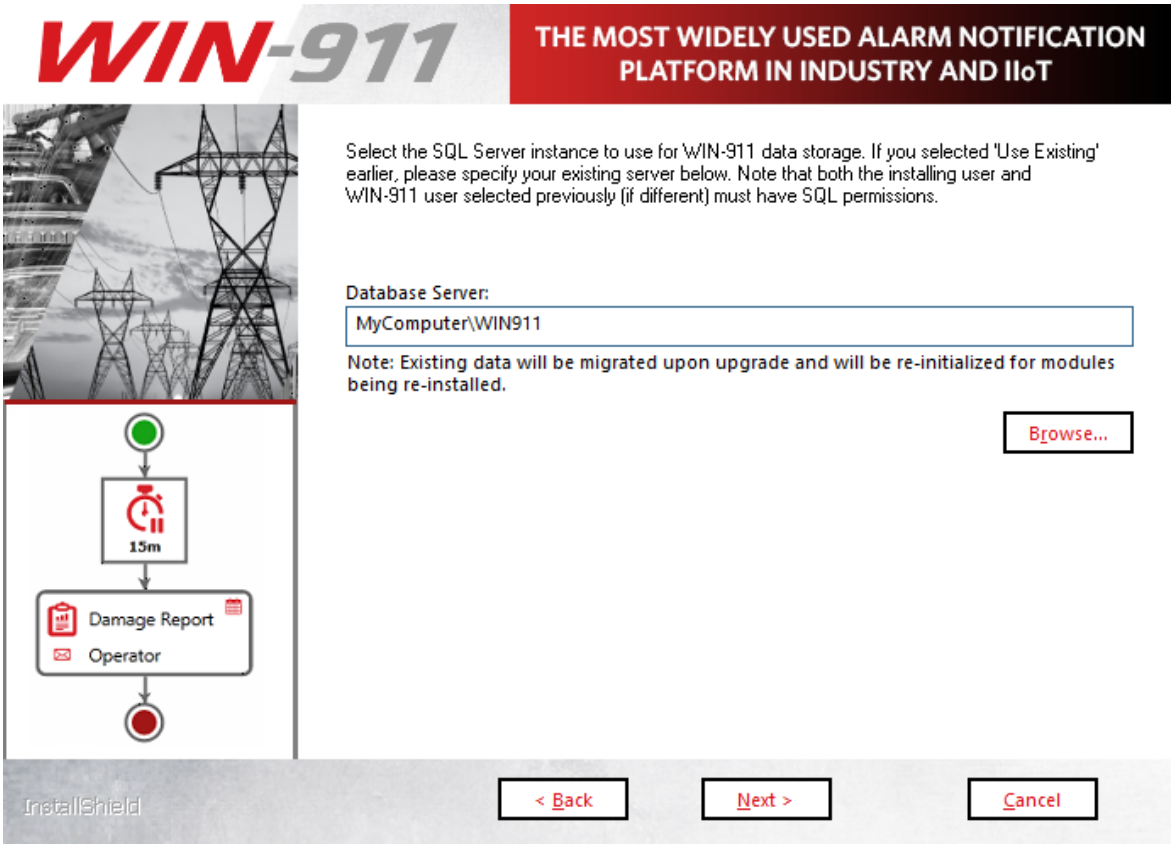


Accept the terms of the Software License Agreement by clicking the top radio button and then select **"Next"** to advance.



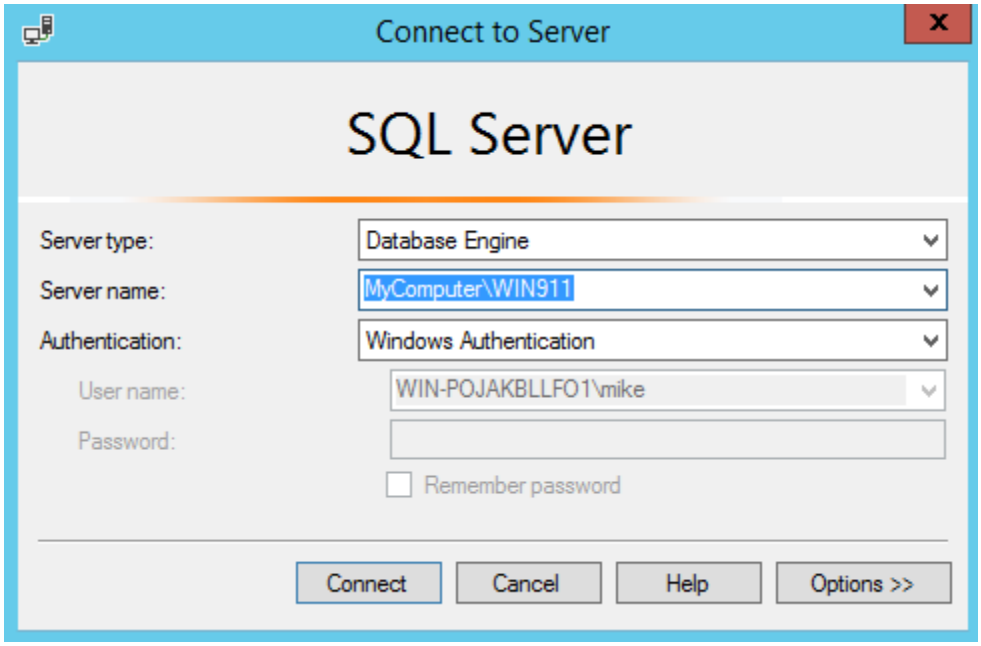
Enter the "DOMAIN\username" and password that WIN-911 Services will run under. If a user name and password are not yet set up in the operating system you can use the **"New User Information ..."** script to create one (Windows 8.1 and higher). This can be found via the control panel, User Accounts. For Active Directory users you will need to contact your network administrator or log onto a domain controller to create an account with the proper permissions. **When entering a domain user's name be sure to include the fully qualified domain name.**

Note: You must be logged in and executing this installation as an owner and administrator of the SQL instance. Additionally, the selected user here (if different) must be a member of the Windows local or domain administrator group with administrative privileges on the SQL instance.

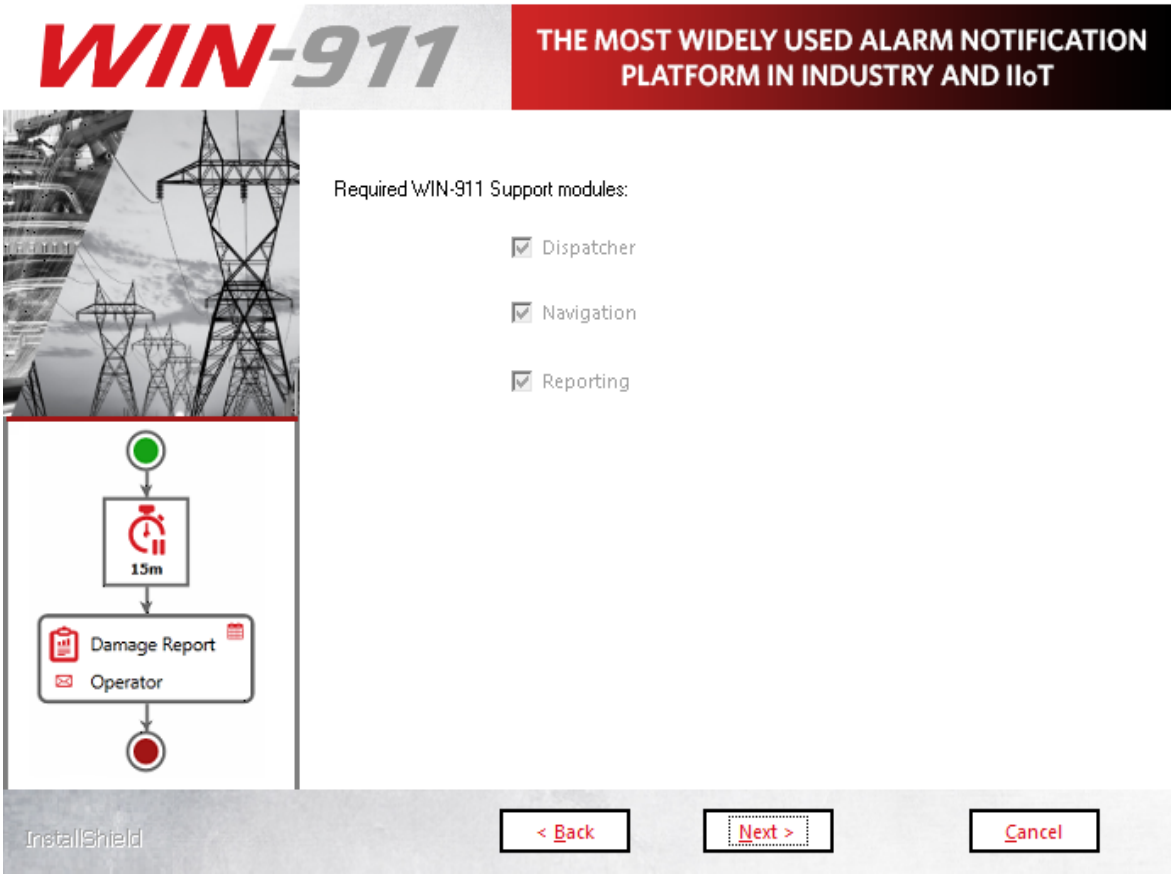


Select the desired database server from the pull-down list. (Server OS's may require you to enable/start SQL Server Browser service in order to browse for SQL Servers)

If you do not see your target server, you may type it into the text entry field as you see it from SQL Management Studio.



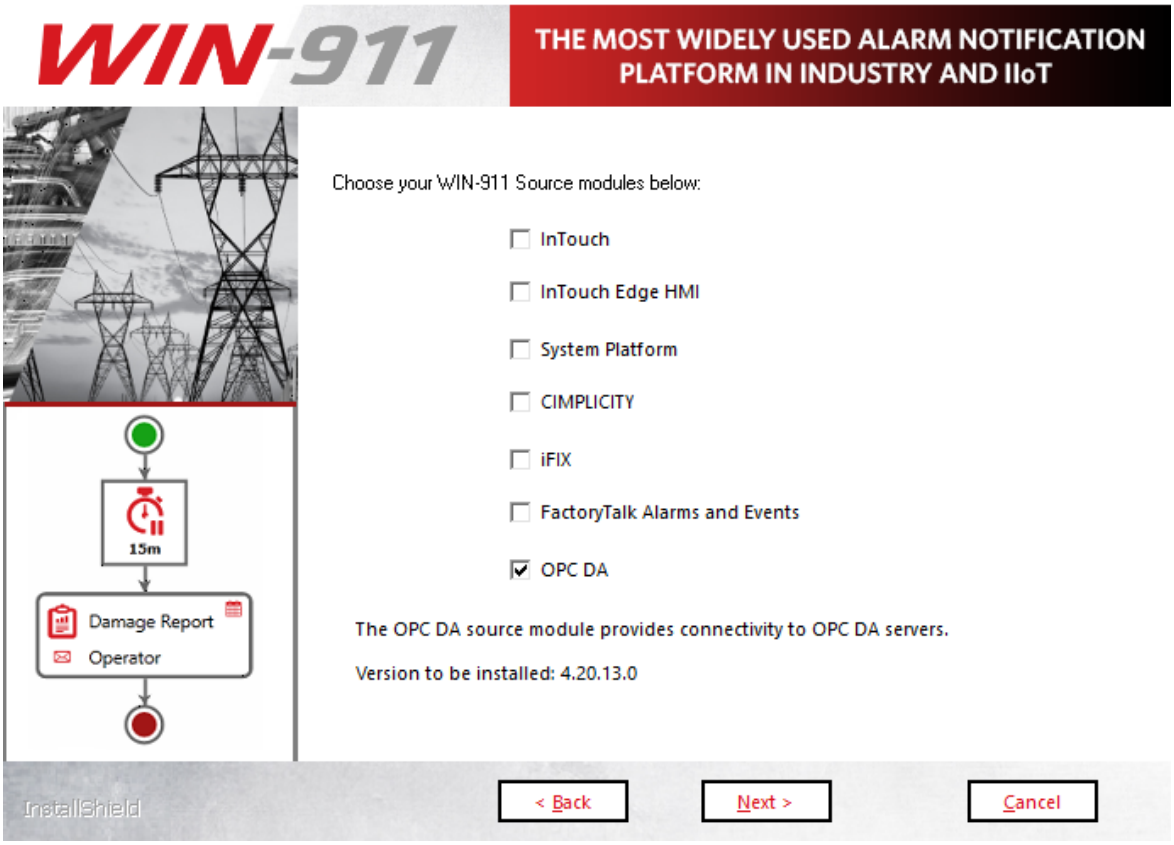
Click **"Next"** to advance.



The support module selection menu allows you to choose which components of WIN-911 you install. As a general rule, all support features should be installed.

If a selection box appears greyed out then installation/upgrade of the module is mandatory.

Click ***Next*** **>** to advance.

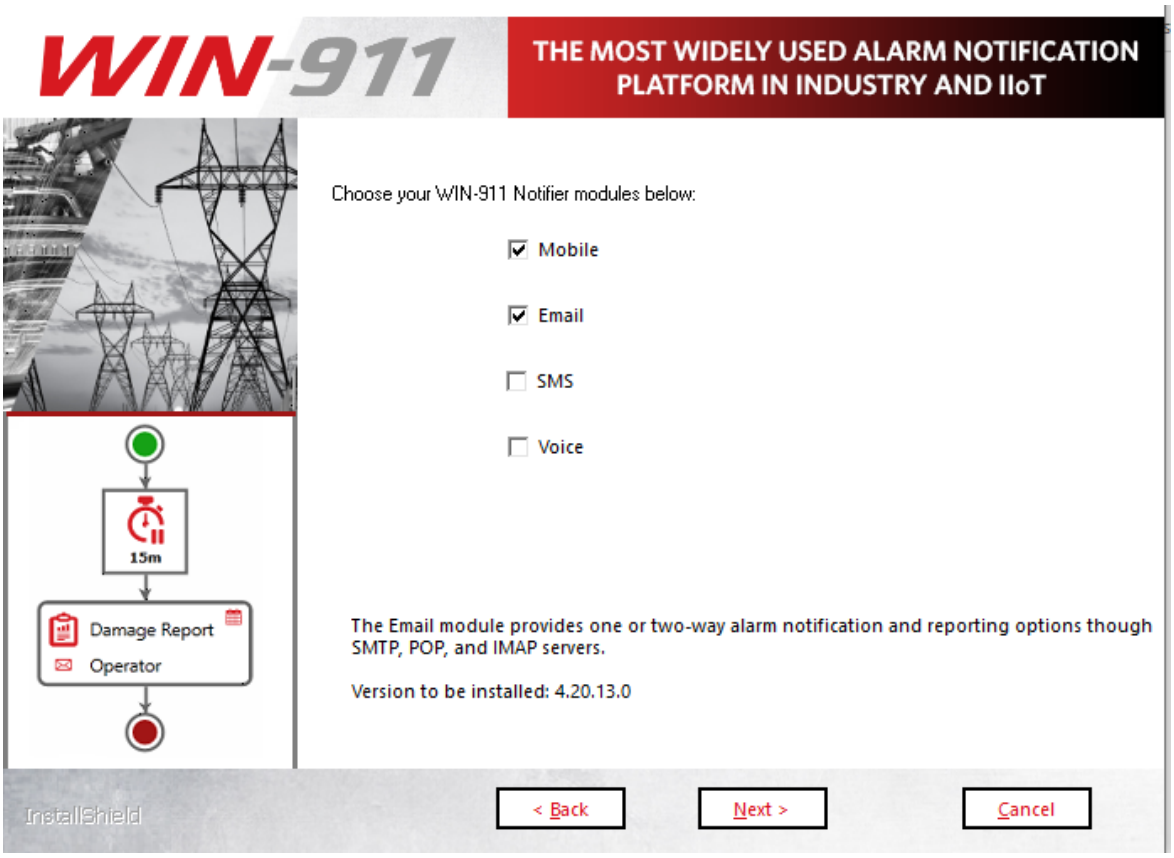


Source modules provide connectivity to various data sources that WIN-911 supports. The source module selection menu allows you to choose which components of WIN-911 you install. Only install the source modules you intend to use. You can always add features later that are not originally installed by re-running the setup. When installing a standalone WIN-911 System you must pick at least one source module to continue.

If a selection box appears greyed out, then the option is either required or already present.

Note: Some sources require selection of specific HMI/SCADA versions.

Click **"Next"** to advance.

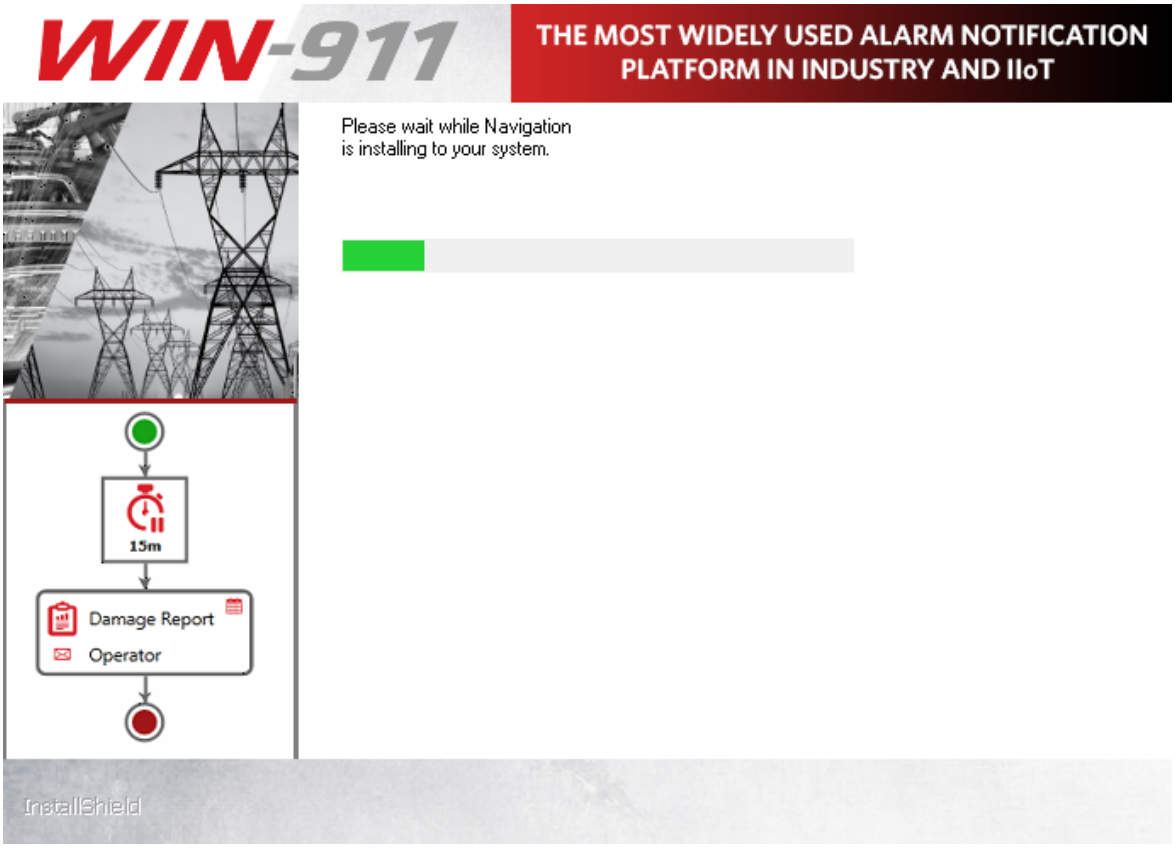


WIN-911 provides several methods of remote notification to users; including Email, Mobile (new in version 4), Voice, and SMS. The notifier module selection menu allows you to choose which components of WIN-911 to install. Only install the notifier modules you currently intend to use. You can re-run the setup program later if decide to add

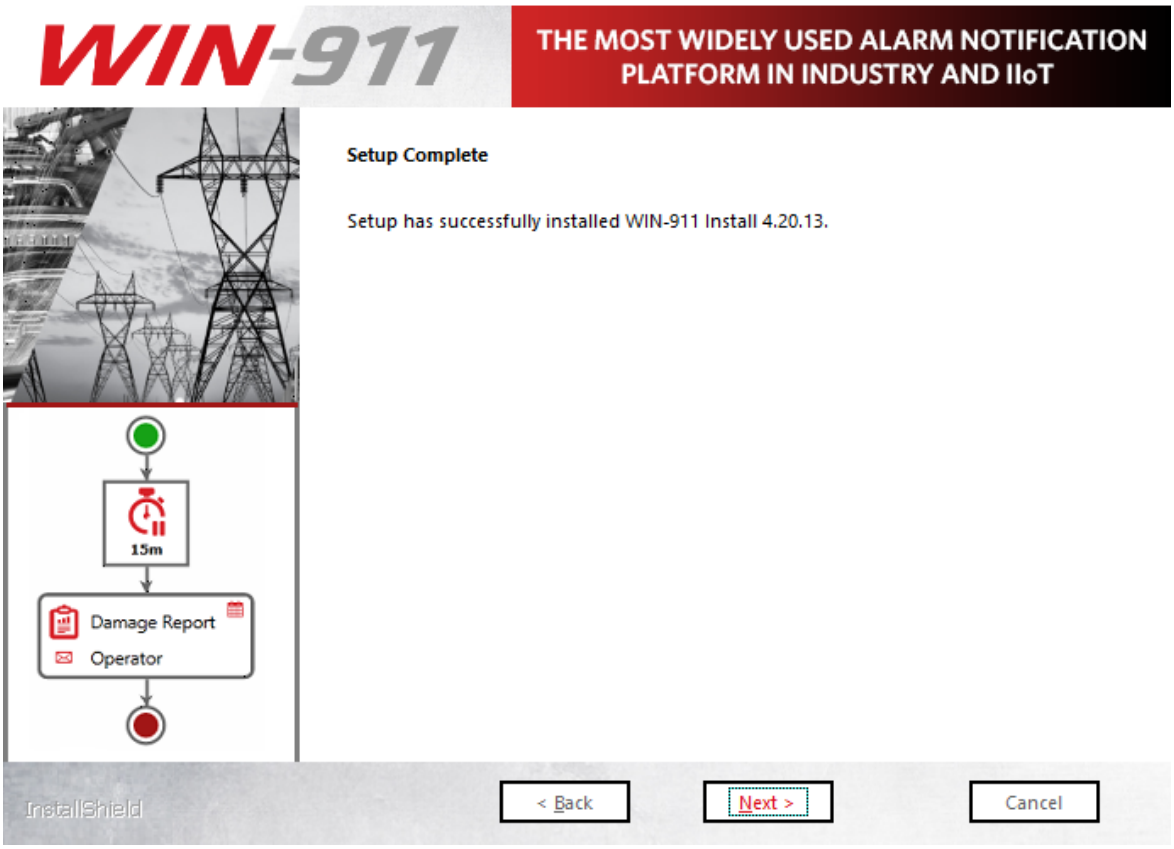
notifiers to your system. When conducting a standalone WIN-911 System you must pick at least one notifier module to continue.

If a selection box appears greyed-out, then that option has already been installed.

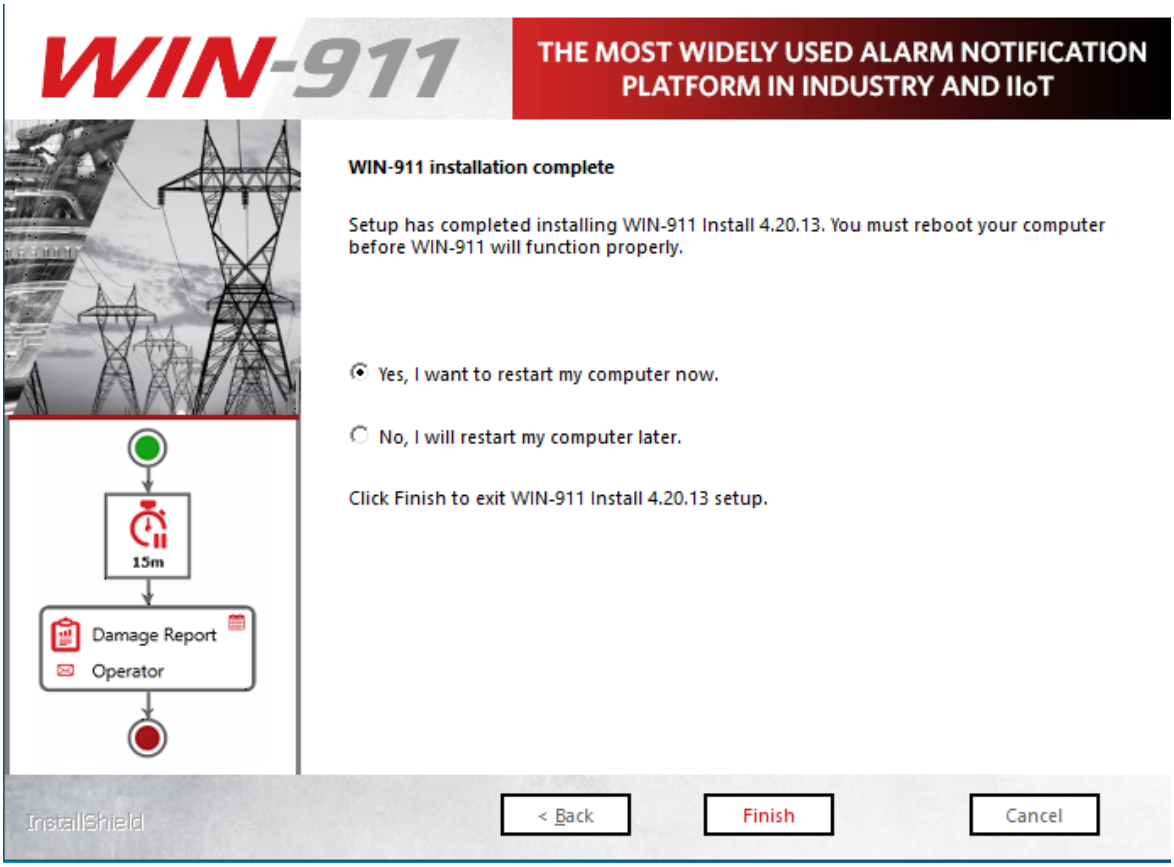
Click **"Next"** to begin the installation and initialization phase of the setup.



This portion of the install may take several minutes.



Click Finish to conclude the installation process.



Once the installation completes, a restart will be required **before WIN-911 can be used**. You can elect to do so immediately or later. Make your selection and click ***Finish***.

Modifying WIN-911

Adding features to your existing WIN-911 installation

Run the WIN-911 Install in the same manner as listed above when installing for the first time. When you get to the Select Features page the currently installed modules will appear grayed out, indicating that they are not available for installation. All currently uninstalled features should be available for selection. Select the desired check boxes and continue through the install process until you reach the Finish page.

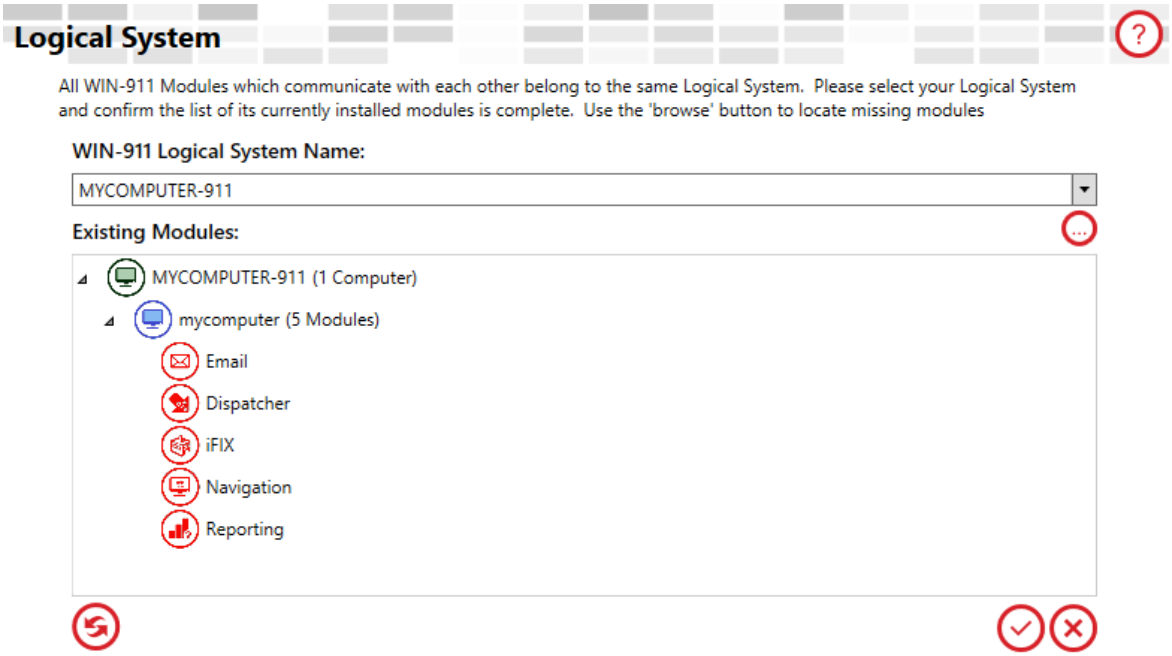
You will then be required to reboot before using WIN-911 in its modified form.

Removing features from your existing WIN-911 installation

WIN-911 features can be uninstalled via *Control Panel\Programs and Features*. Each mod3ule will have to be uninstalled individually. Right-click the WIN-911 module and select Uninstall. Repeat this process until all undesired features have been removed. You will then need to run the WIN-911 Endpoint Mapper before using WIN-911 in its modified form.

Note: To uninstall WIN-911, remove all modules.

WIN-911 Network Module Mapper



Whenever you modify your WIN-911 system by uninstalling software modules you will need to run the WIN-911 Network Module Mapper. The mapping process might take several minutes to appear and may

need to be refreshed if the proper number of modules are not listed. This is normal so allow for extra time during the post-modification reboot.

The proper number of modules depends on the number of data sources and notifiers you selected during the feature selection. If fewer modules appear, then click the refresh button until the proper number are listed. To calculate the expected number of modules in your system add the *Support + Notifiers + Data Sources* from the feature selection.

Once the proper number of modules are listed, click the save button. This will conclude this portion of the install. **You should not need to run the WIN-911 Network Module Mapper again** unless you remove certain features included in the initial install.

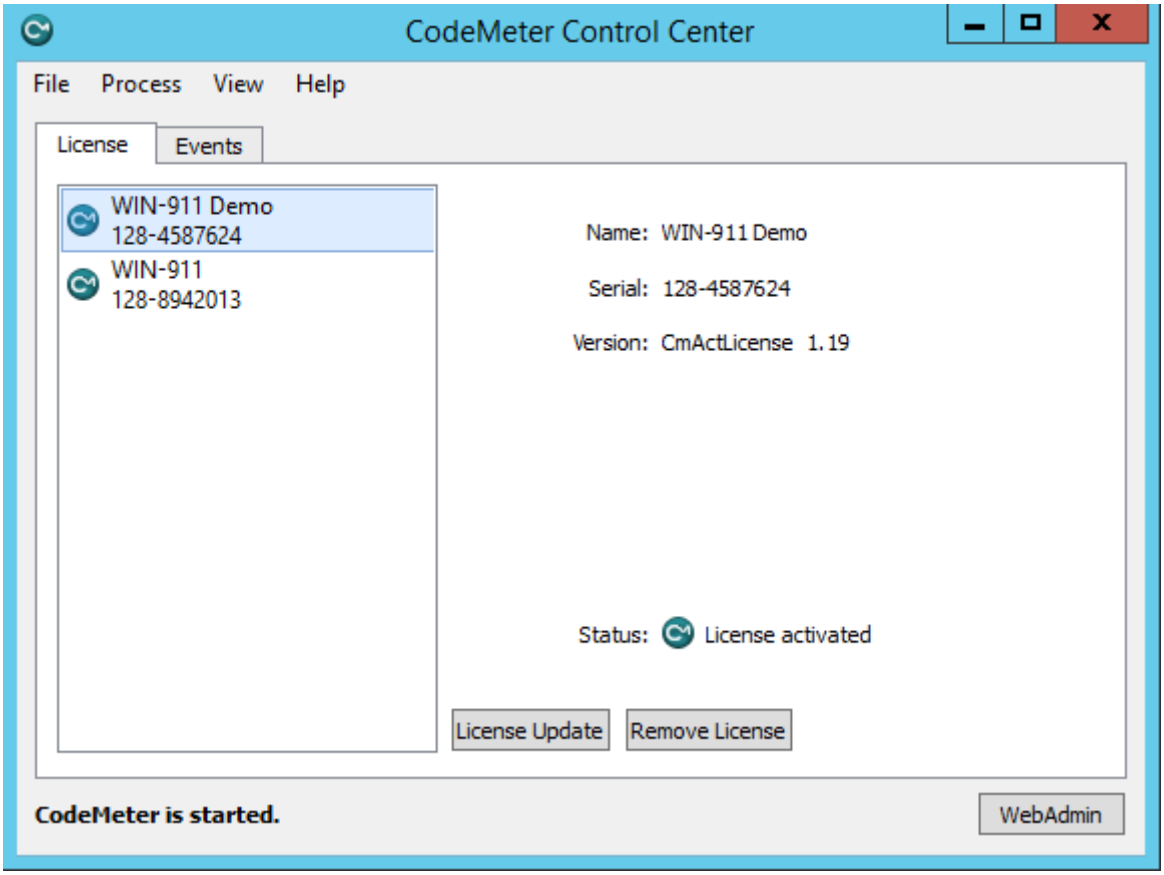
See WIN-911 Network Module Mapper for more details.

Licensing WIN-911

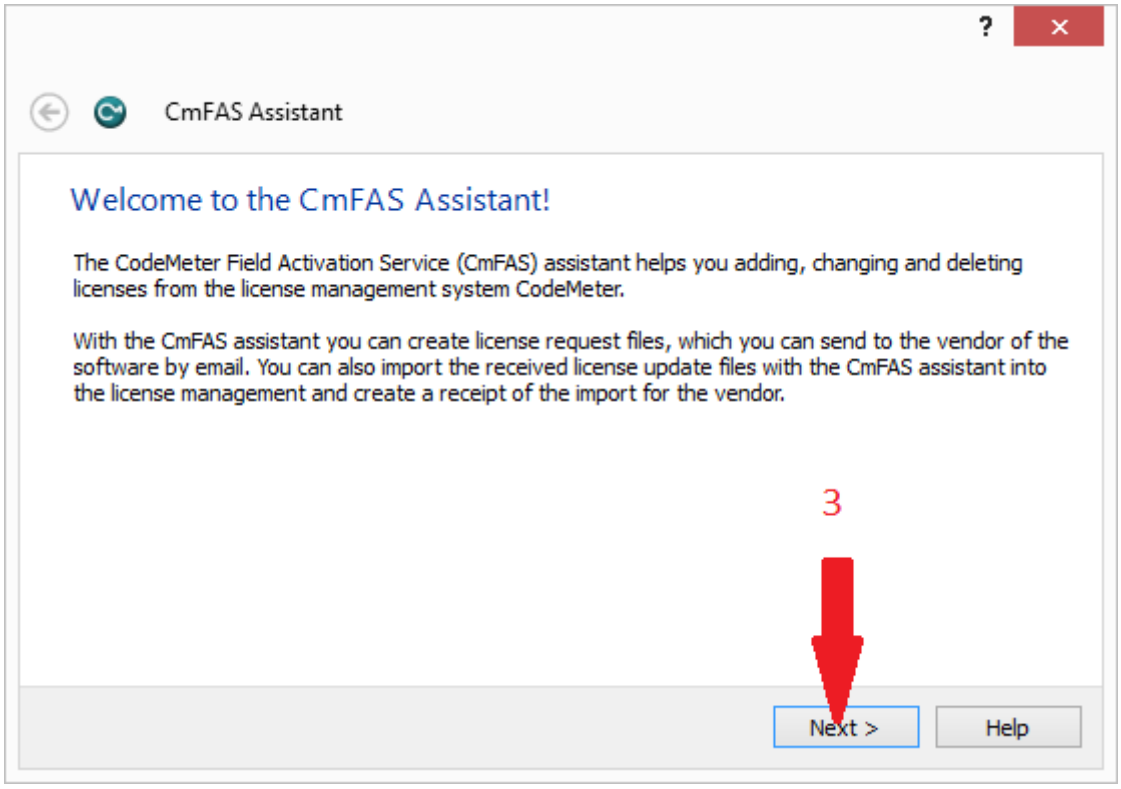
Note: After an initial installation WIN-911 will be configured with a demo license that will run 30 days without restriction.

To license WIN-911 click on the CodeMeterControl Center thumbnail located in the lower right of your tray.

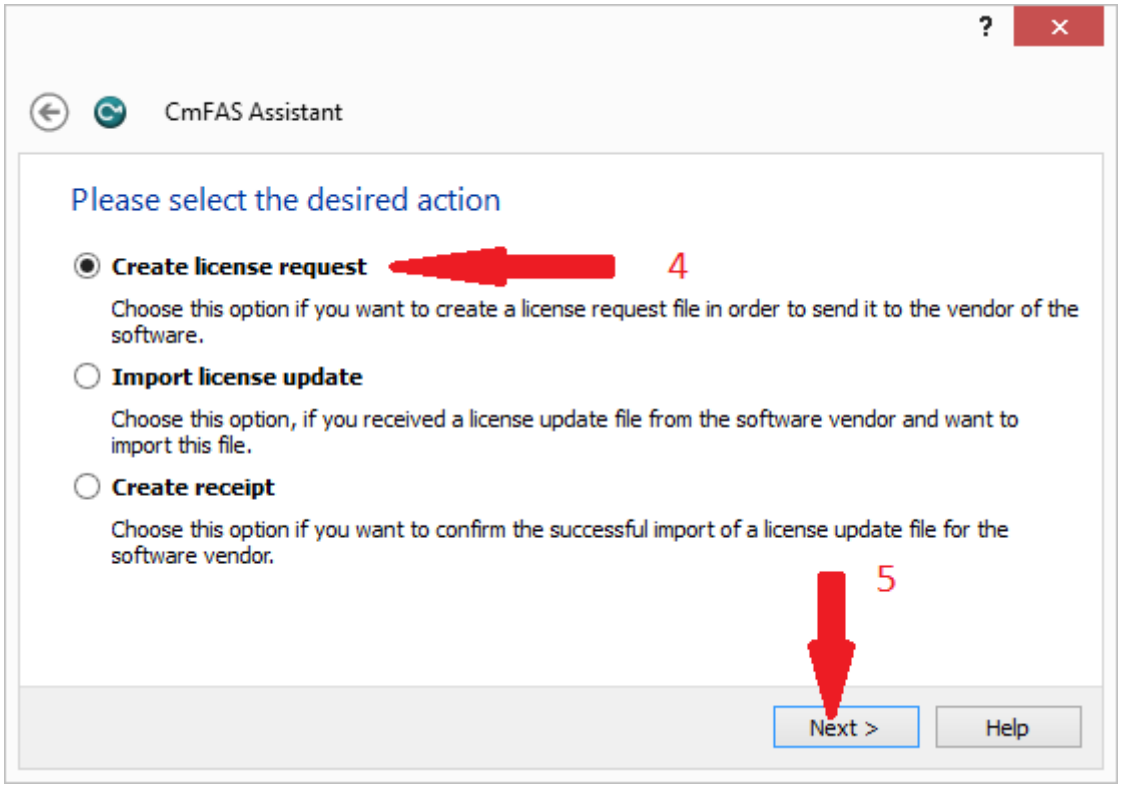
Click the “License Update” button and follow the wizard to generate a license request file.



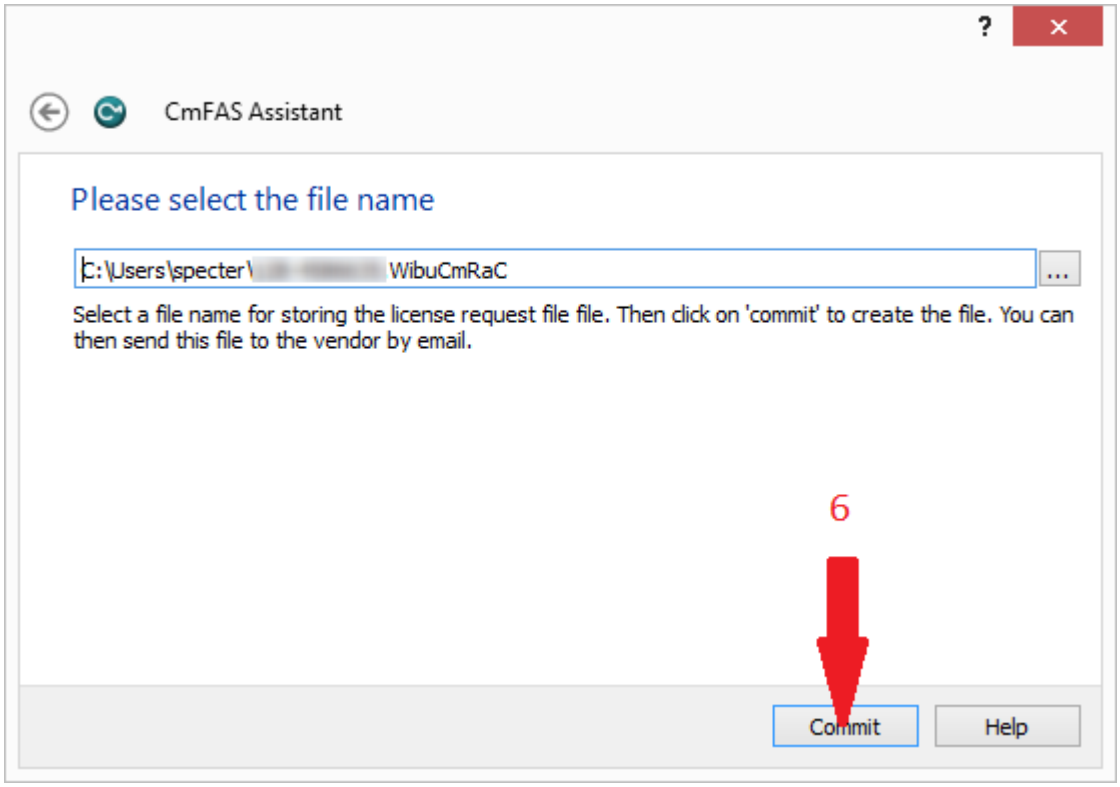
Select the container with the active license (1). The Status indication will verify "Empty license container". Then click Activate License (2).



Click the Next > (3) button to advance past the welcome screen.



Select the Create license request (4) option and then click Next > (5).

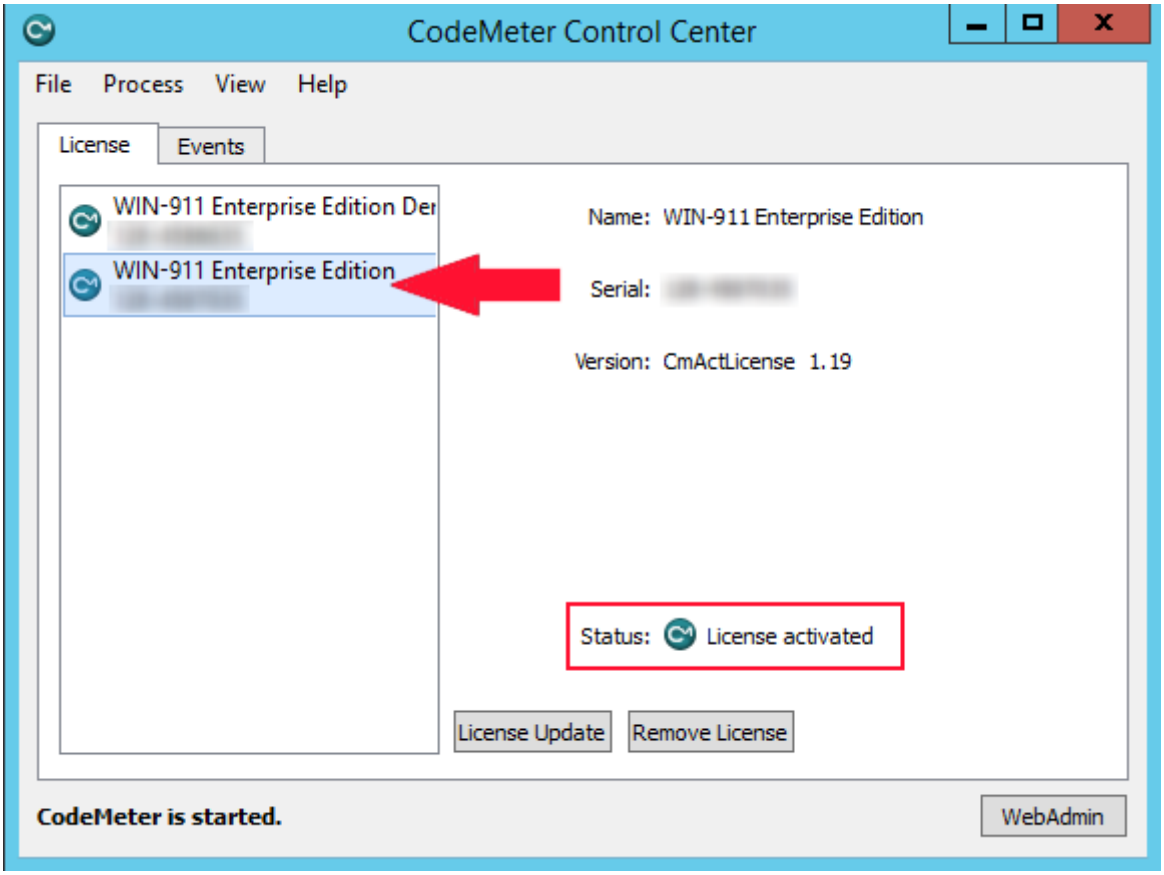


Note the location of the license request and then click Commit (6).

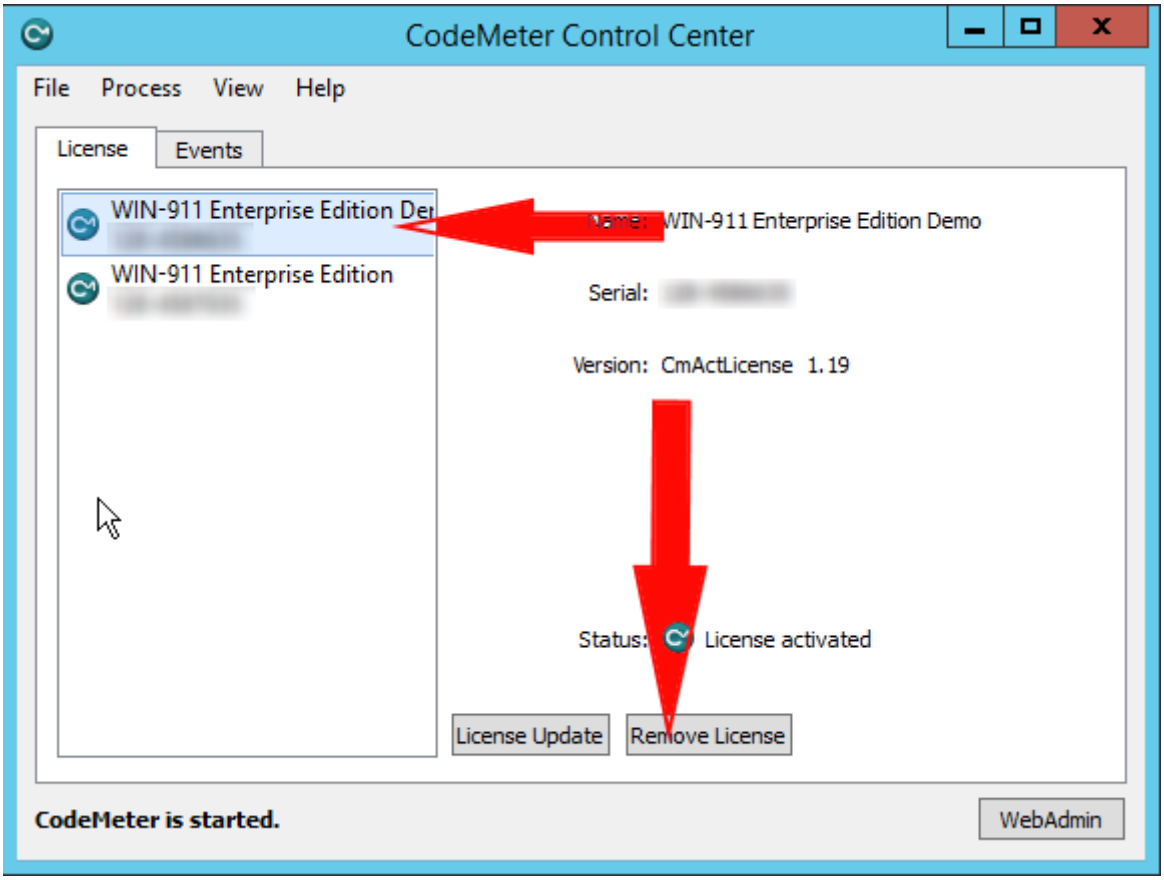
Log onto our website, complete the license request form and submit the license request file.

Upon receipt of the license file, save it to the desktop.

Double-click on the license file. This will import and activate the license.



Remove the Demo license by highlighting it and clicking "Remove License".

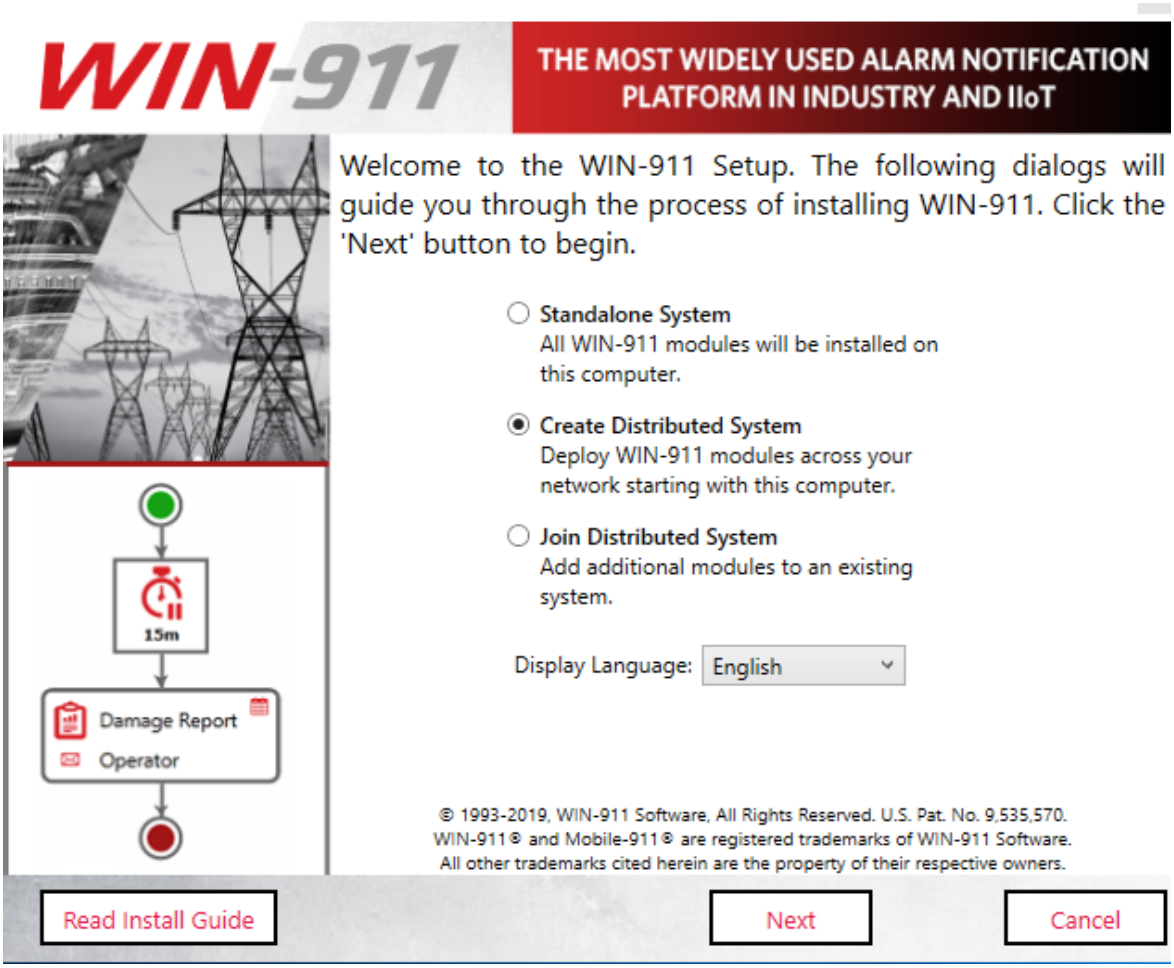


To verify proper licensing, reboot the host machine, then check the Event Logger for any WIN-911 related errors.

Create Distributed System

The WIN-911 Launcher requires .NET 4.0 (or higher). If the target machine lacks this framework, you will need to add the framework in order to commence. In Windows 8.x, this can be done through *Programs and Features> Turn Windows features on or off.* With Server operating systems use *Server Manager> Add roles and features*. Additionally, you can find an installer for the framework in the support sub folder of the installation media or online.

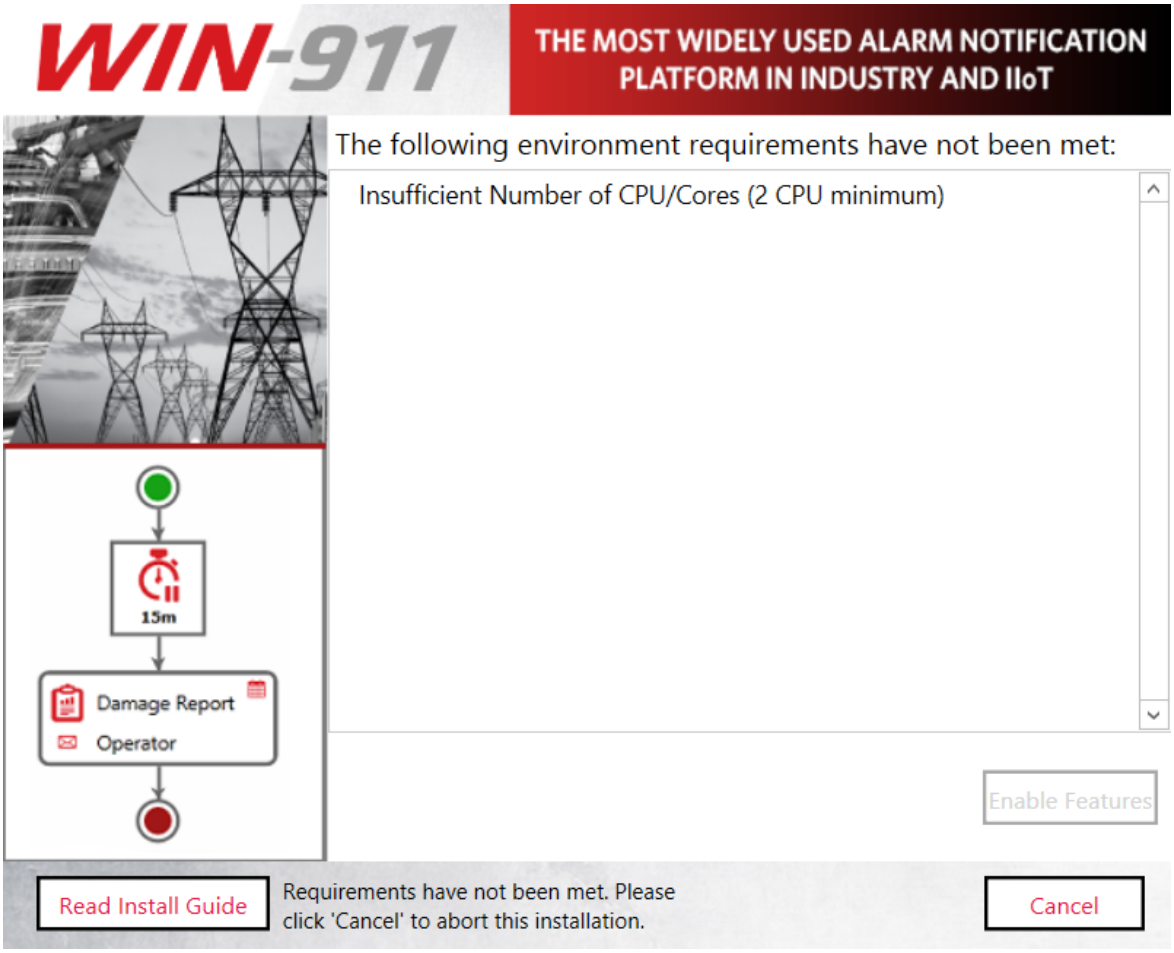
To begin creating a distributed WIN-911 System you will need to run the install on the computer that will host the support modules.



Attention: When using a language other than English select it here.

Click **"Next"** to begin WIN-911 Setup.

The installation program checks whether or not the environment requirements are met.



Such environment requirements include:

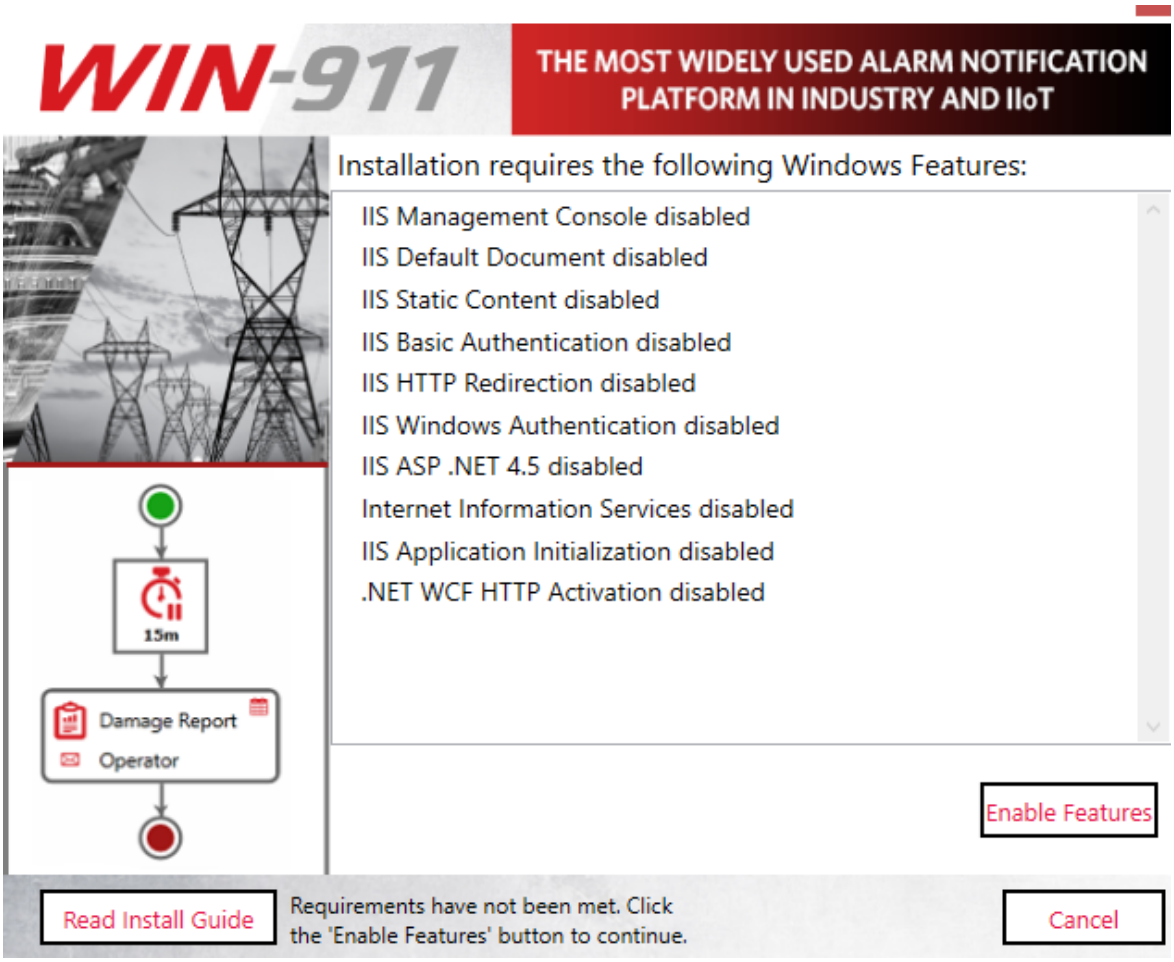
- Supported 64-bit OS
- Sufficient minimum disk space

- Sufficient minimum processors/cores
- Installing user be a member of local administrator's group

See WIN-911 4.21.5 System Requirements at the top of this document for more information.

Note: If these requirements are met, this page will not appear.

The installation program will then check for the required features.



Feature requirements include the following:

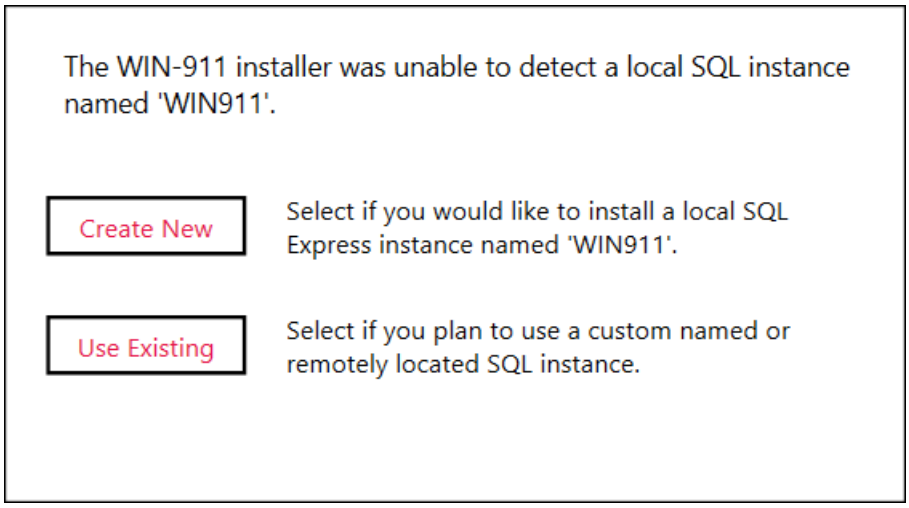
- Microsoft .NET 4.8
- Windows Edition and Feature Set Detection
- IIS Features: Application Initialization, Basic Authentication, Windows Authentication, HTTP Redirection and ASP.NET 4.5, HTTP Activation

Any missing feature can be enabled by clicking the Enable Features button at the bottom right.

Note: If these requirements are met, this page will not appear.

SQL Server Installation

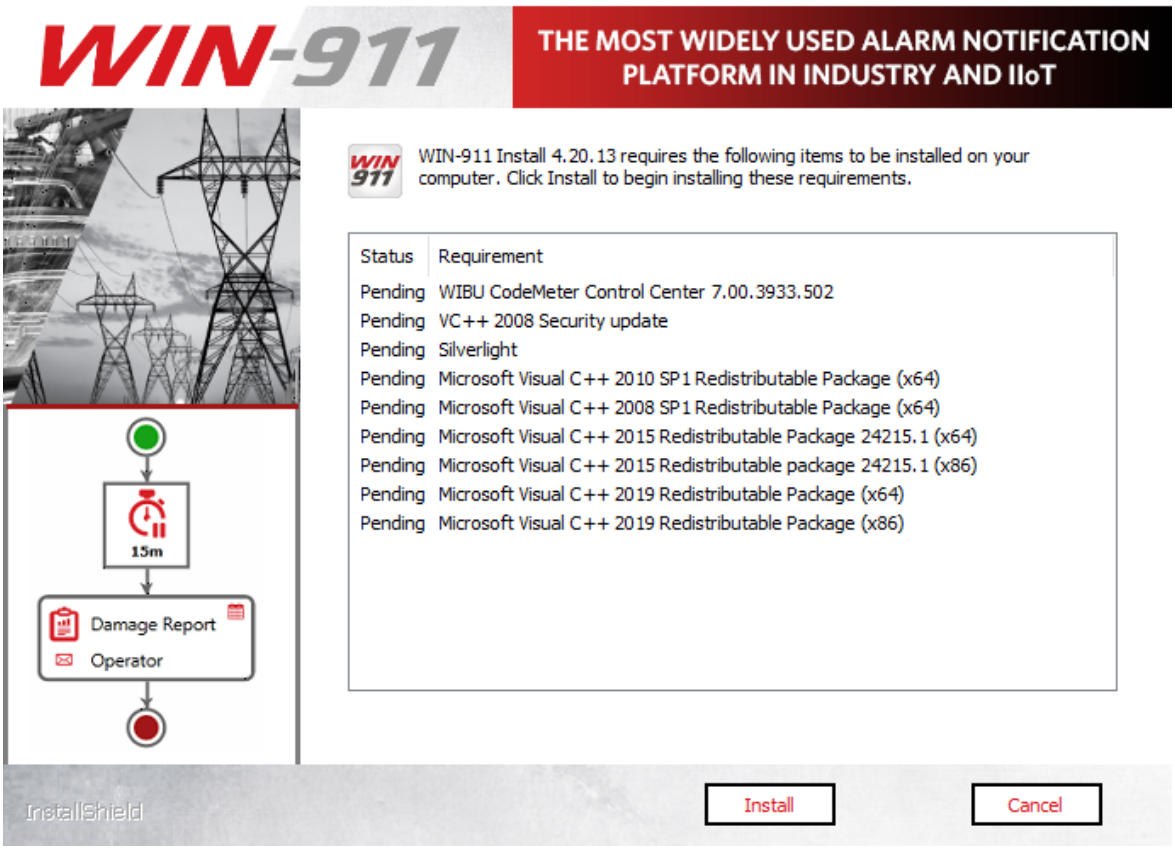
The install script will check the WIN-911 host for an SQL Server instance named "WIN911". If there is no suitable SQL Server, the following pop-up will appear:



This is an optional step and is not required in order to continue with the installation, but WIN-911 cannot be used until the SQL Server requirement is satisfied.

Note: if you are upgrading, you should select "Use Existing" to keep your existing data.

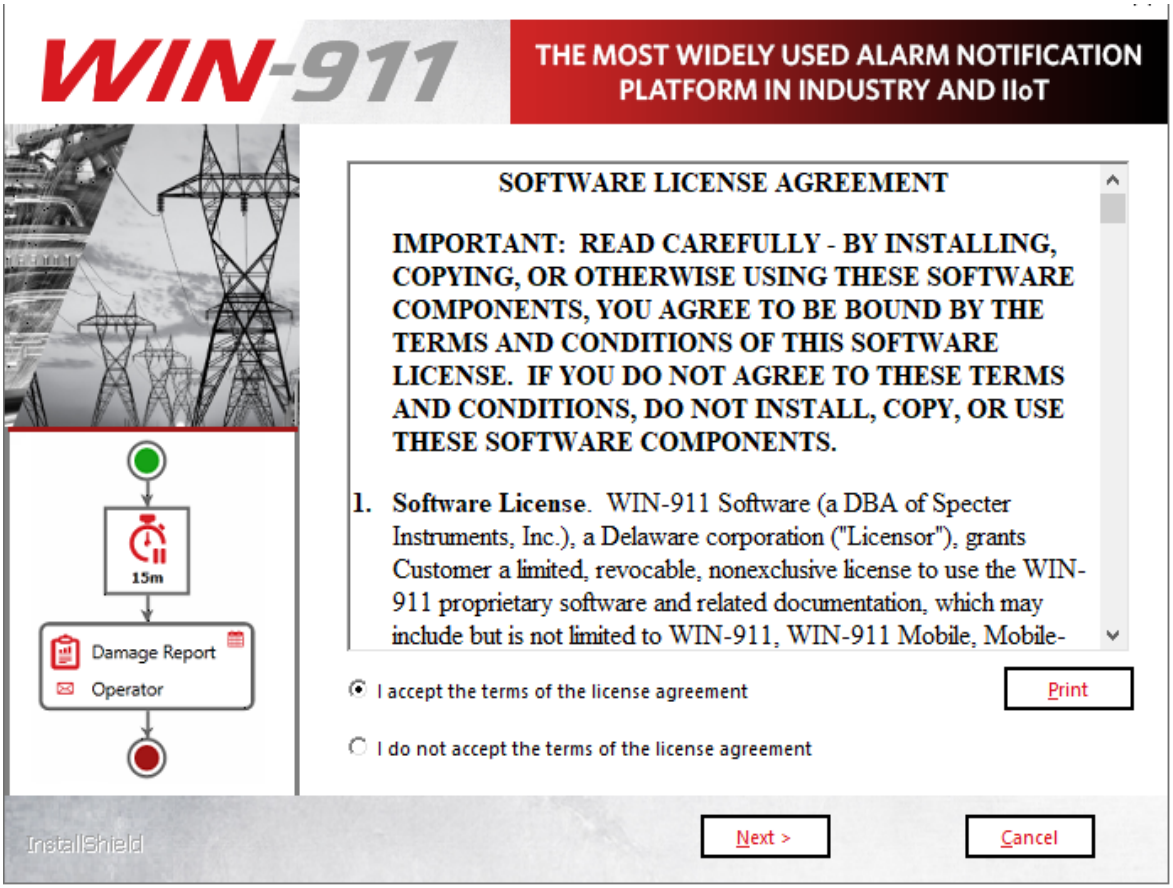
InstallShield Wizard



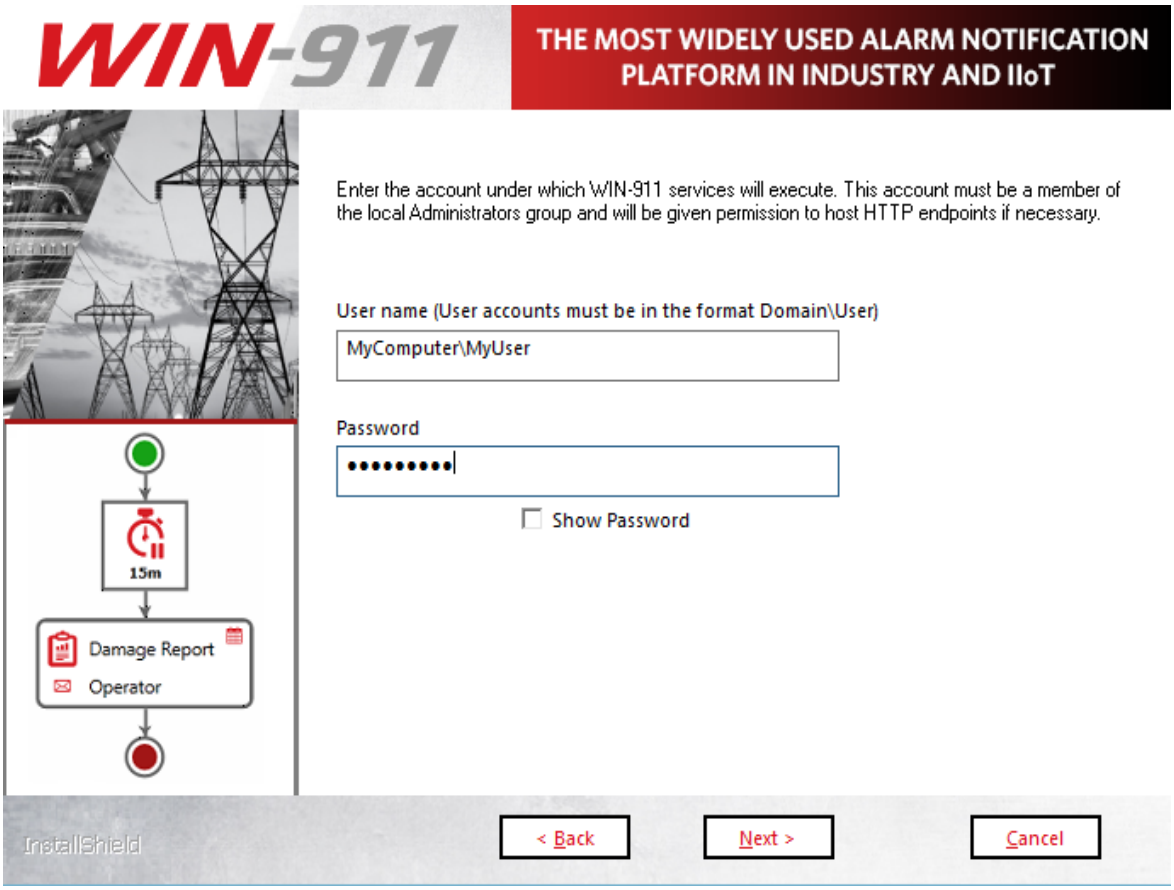
Depending on the state of .NET Framework 4.8, you may need to reboot prior to continuing.

If requested, select Yes and the install process will resume automatically once the reboot is performed.

The WIN-911 InstallShield wizard will now guide you through the WIN-911 setup. Click **"Next"** to continue.

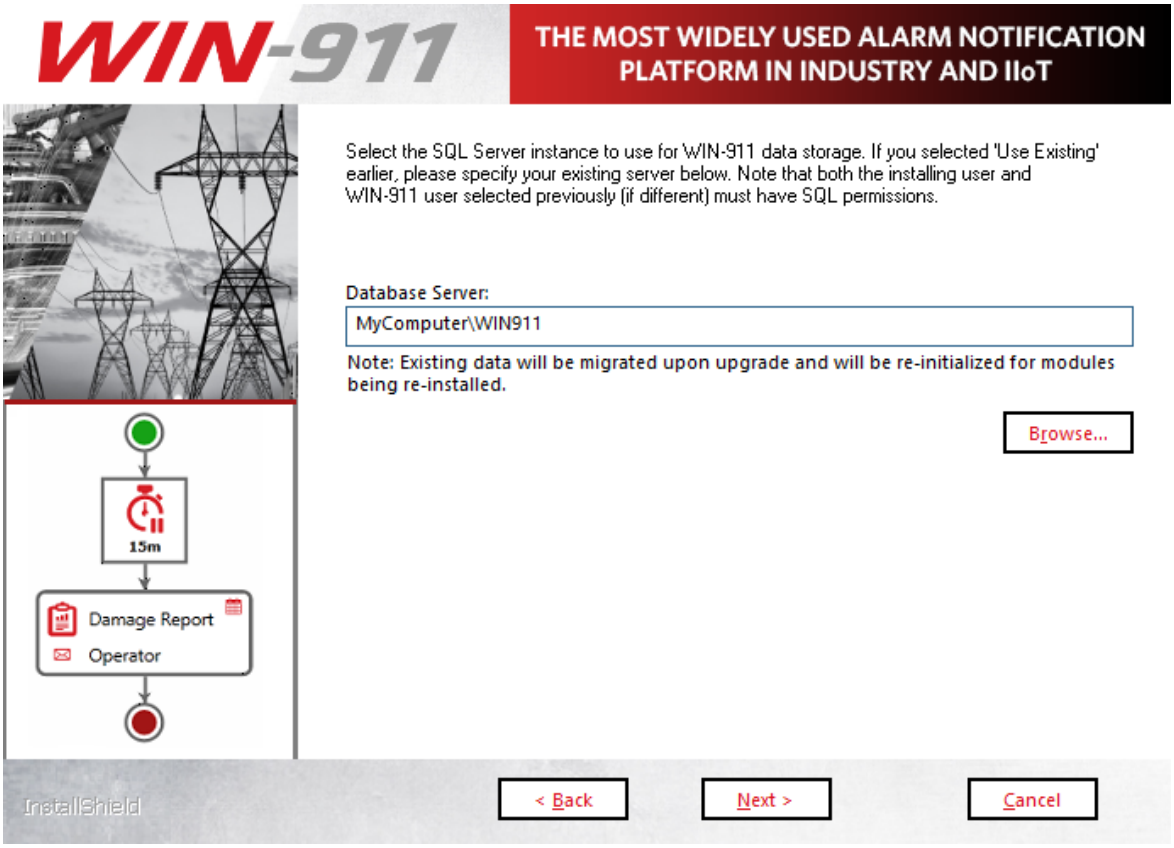


Accept the terms of the Software License Agreement by clicking the top radio button and then select **“Next”** to advance.



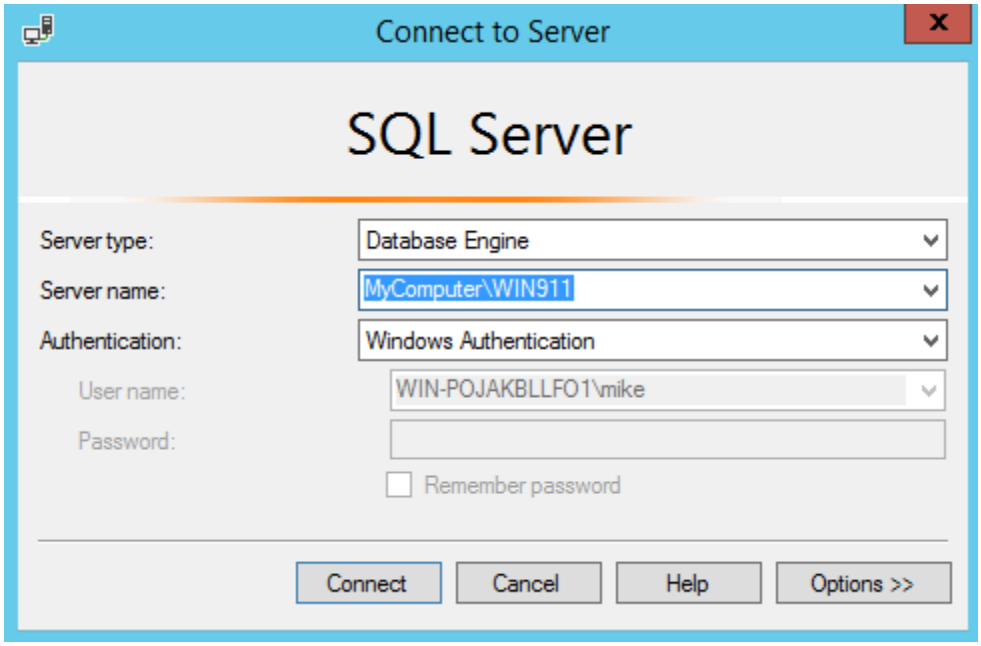
Enter the "DOMAIN\username" and password that WIN-911 Services will run under. If a user name and password are not yet set up in the operating system you can use the **"New User Information ..."** script to create one (Windows 8 and higher). This can be found via the control panel, User Accounts. For Active Directory users you will need to contact your network administrator or log onto a domain control to create an account with the proper permissions. **When entering a domain user's name be sure to include the fully qualified domain name.**

Note: You must be logged in and executing this installation as an owner and administrator of the SQL instance. Additionally, the selected user here (if different) must be a member of the Windows local or domain administrator group with administrative privileges on the SQL instance.

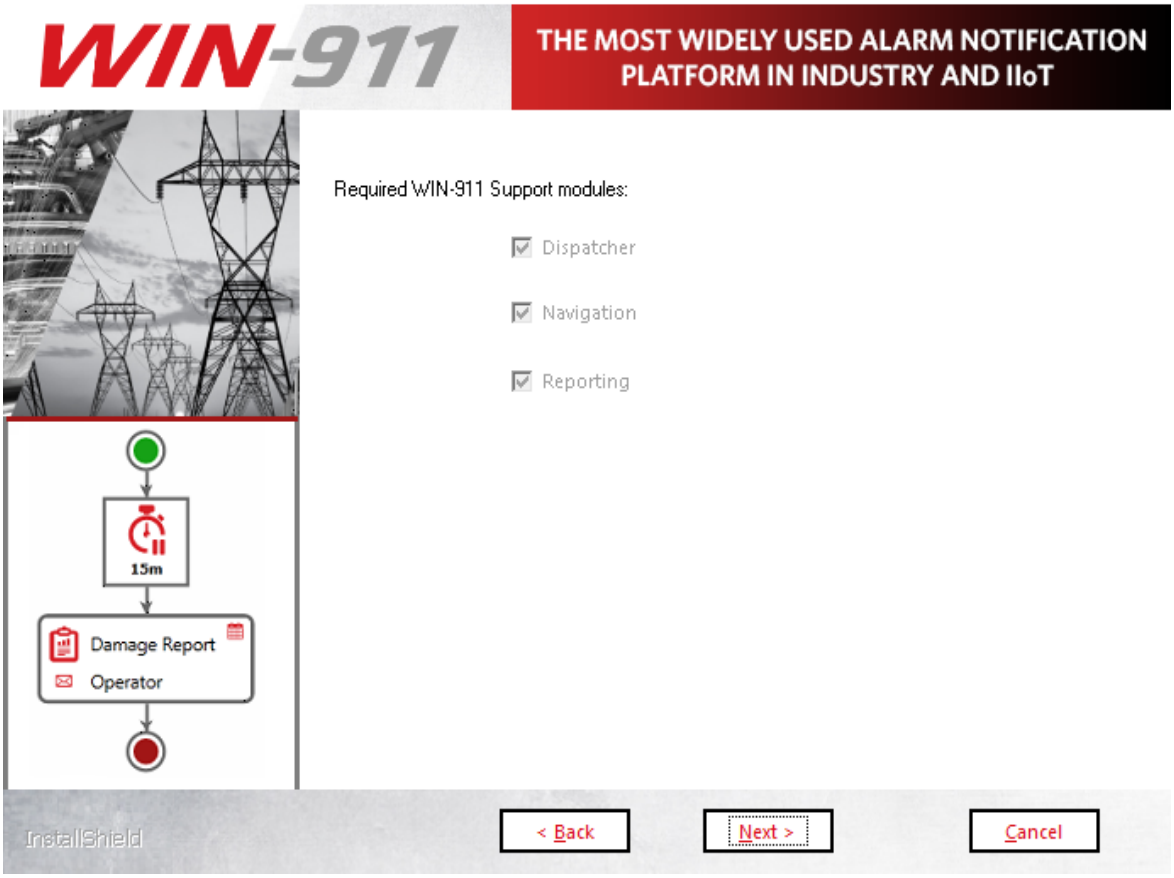


Select the desired database server from the pull-down list. (Server OS's may require you to enable/start SQL Server Browser service in order to browse for SQL Servers)

If you do not see your target server, you may type it into the text entry field as you see it from SQL Management Studio.

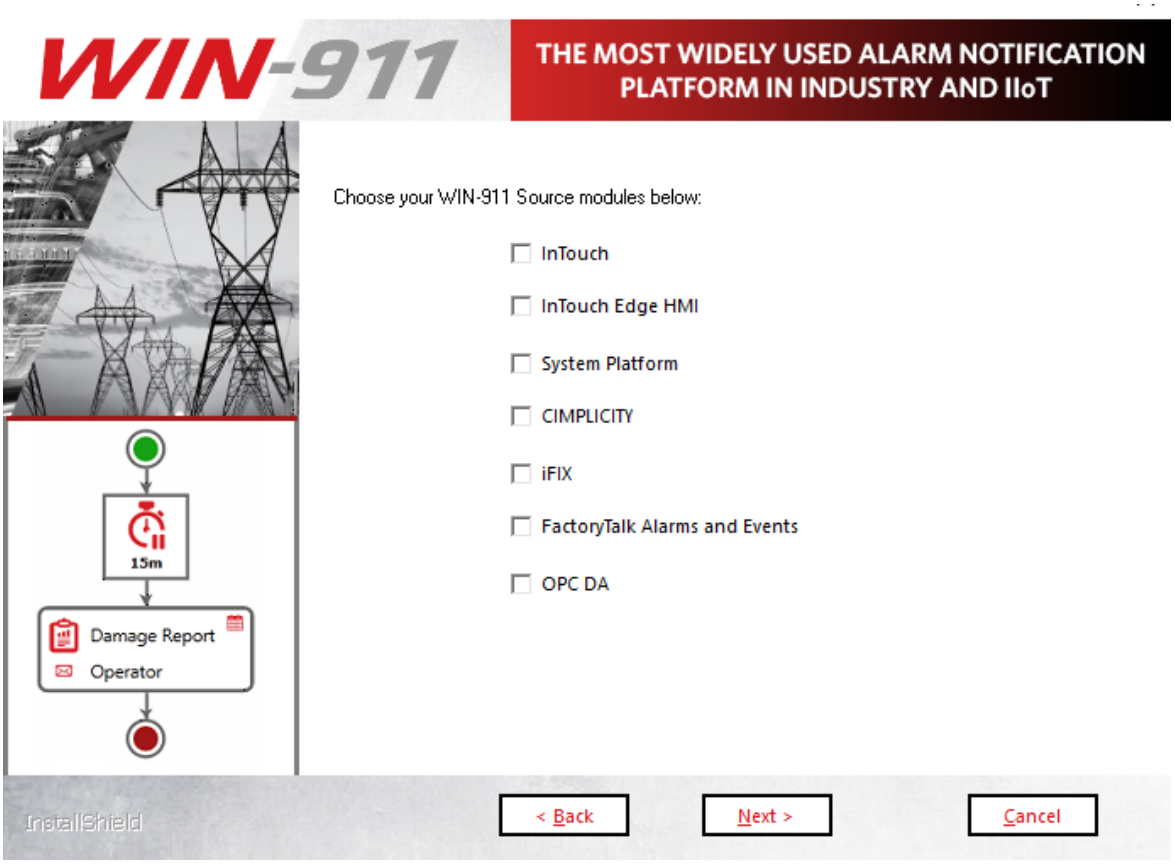


Click **"Next"** to advance.



To create a distributed WIN-911 System you must install all support modules on the primary (Dispatcher) WIN-911 host. Thus, all support modules are required and selected by default.

Click ***Next*** **>** to advance.



Source modules provide connectivity to various data sources that WIN-911 supports. The source module selection menu allows you to choose which components of WIN-911 you install. Only install the source modules you intend to use. You can always add features later that are not originally installed by re-running the setup.

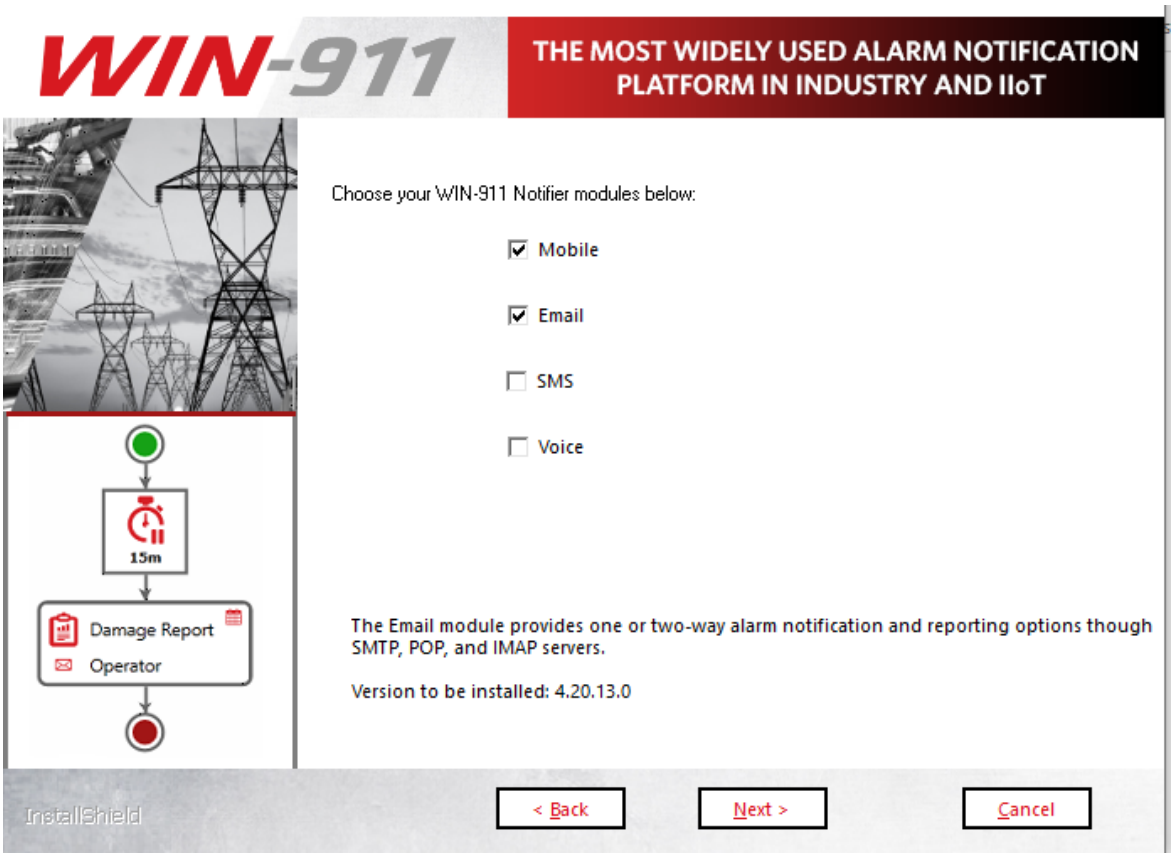
When finalizing a distributed WIN-911 System, at least one source module is required, but it does not need to be on the same computer as your support modules. Thus, you can proceed with the current install without selecting a source module. To finalize your WIN-911

System, you will need to install a source module to another computer using the "Join Distributed System" option.

If a selection box appears greyed out, then the option is either required or already present.

Note: Some sources require selection of specific HMI/SCADA versions.

Click **"Next"** to advance.



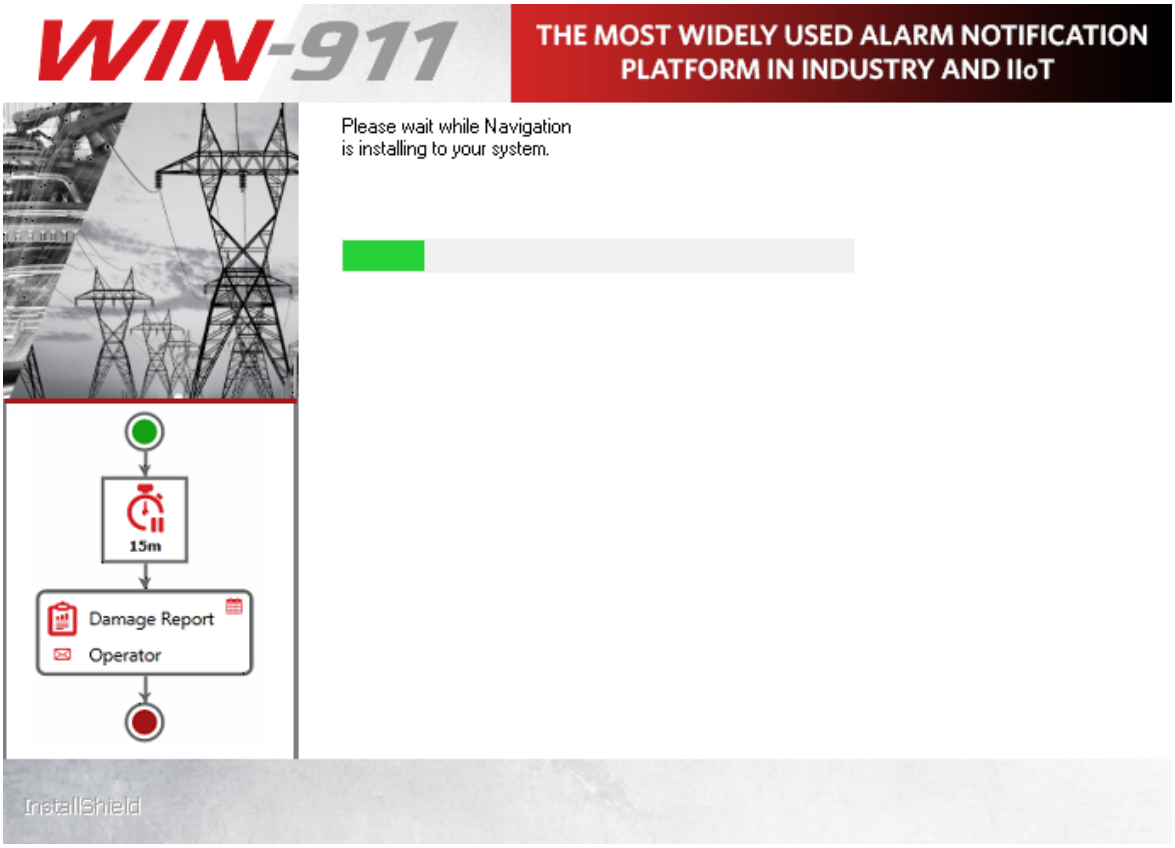
WIN-911 provides several methods of remote notification to users; including Mobile, Mobile-911, Email, SMS, and Voice. The notifier module selection menu allows you to choose which components of WIN-911 to install. Only install the notifier modules you currently

intend to use. You can re-run the setup program later if decide to add notifiers to your system.

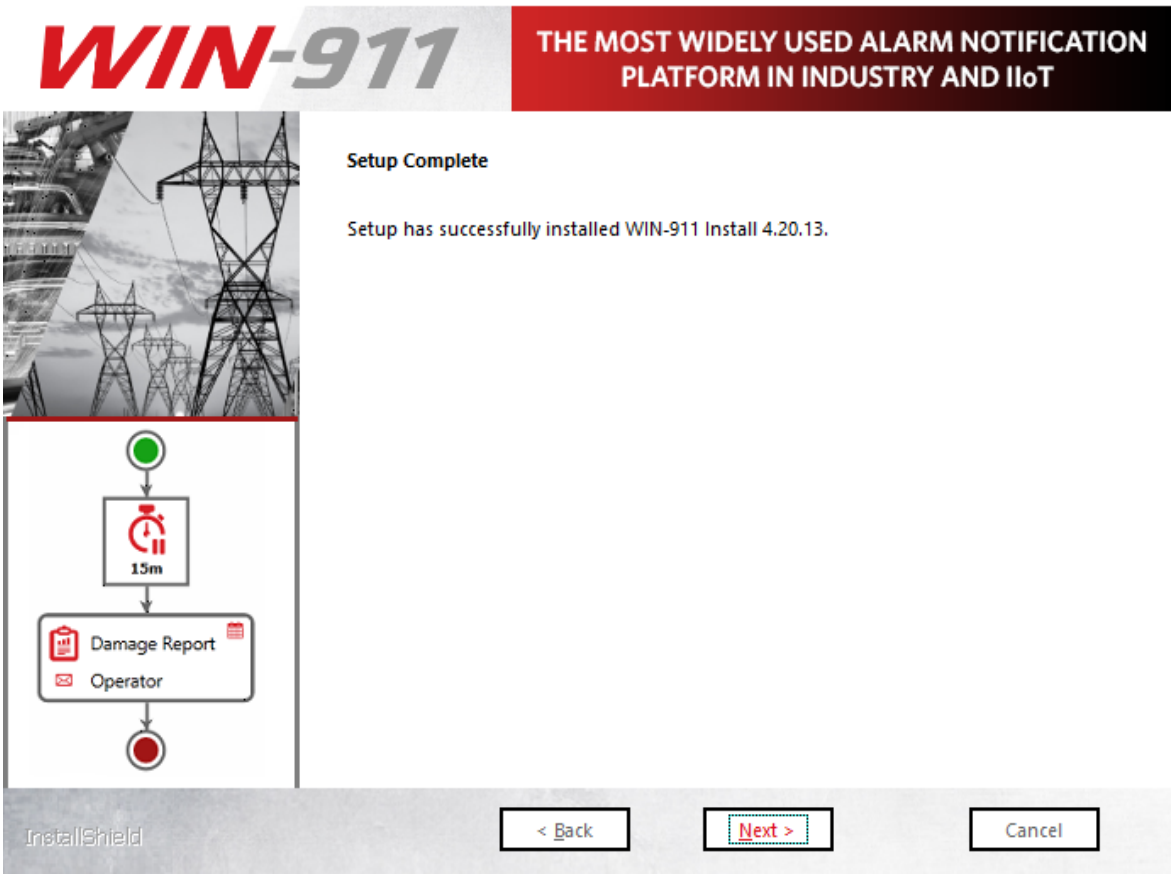
When finalizing a distributed WIN-911 System, at least one notifier module is required, but it does not need to be on the same computer as your support modules. Thus, you can proceed with the current install without selecting a notifier module. To finalize your WIN-911 System, you will need to install a notifier module to another computer using the "Join Distributed System" option.

If a selection box appears greyed out then that option has already been installed.

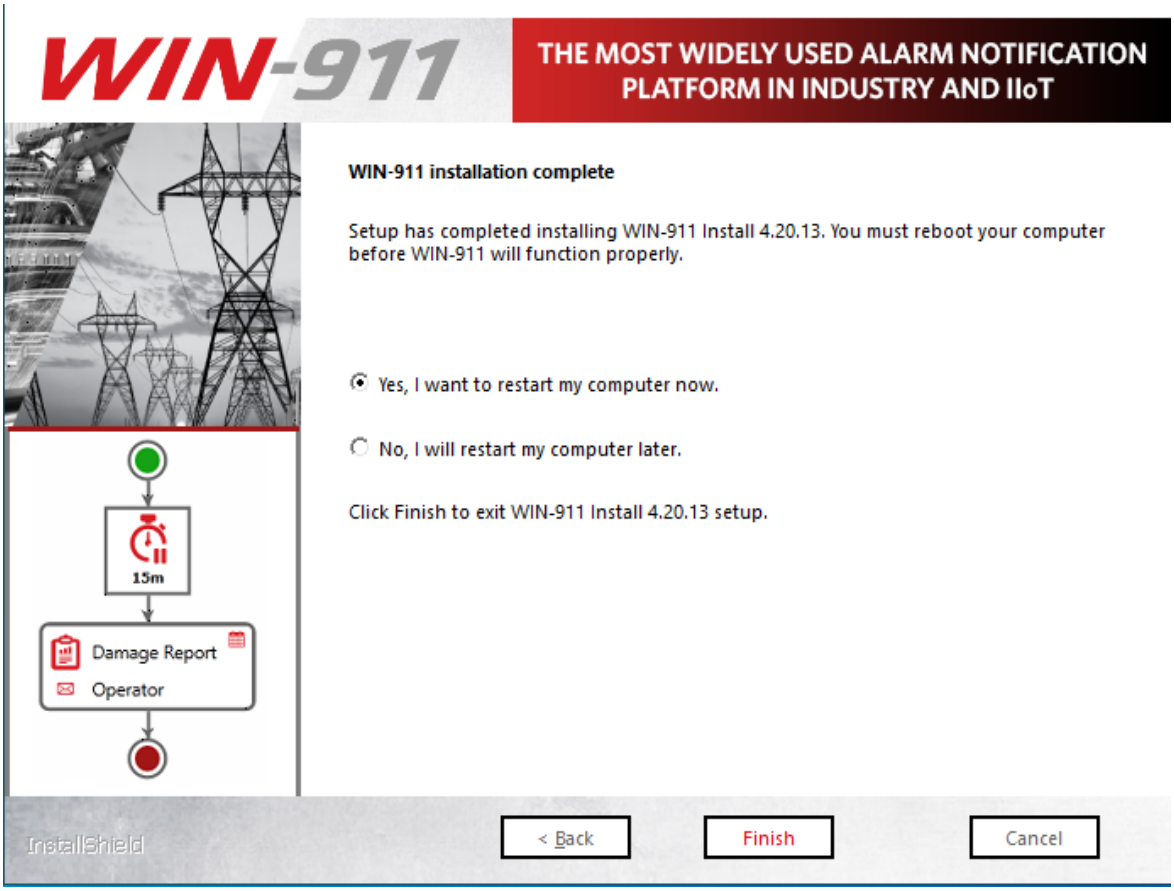
Click **"Next"** to begin the installation and initialization phase of the setup.



This portion of the install may take several minutes.



Click Finish to conclude the installation process.



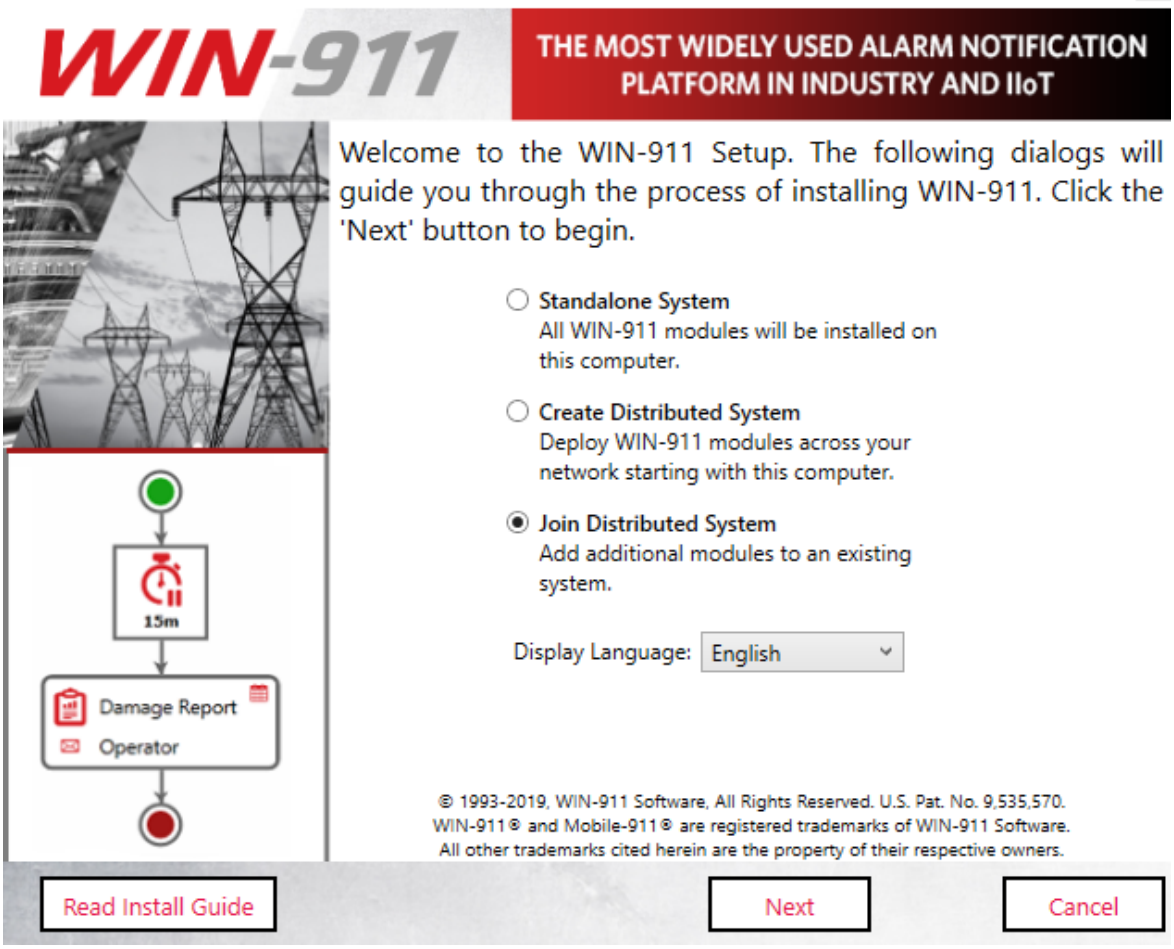
Once the installation completes, a restart will be required **before WIN-911 can be used**. You can elect to do so immediately or later. Make your selection and click ***Finish***.

[Modifying and Licensing WIN-911]

Join Distributed System

The WIN-911 Launcher requires .NET 4.0 (or higher). If the target machine lacks this framework, you will need to add the framework in order to commence. In Windows 8.x, this can be done through *Programs and Features> Turn Windows features on or off*. With Server operating systems use *Server Manager> Add roles and features*. Additionally, you can find an installer for the framework in the support sub folder of the installation media or online.

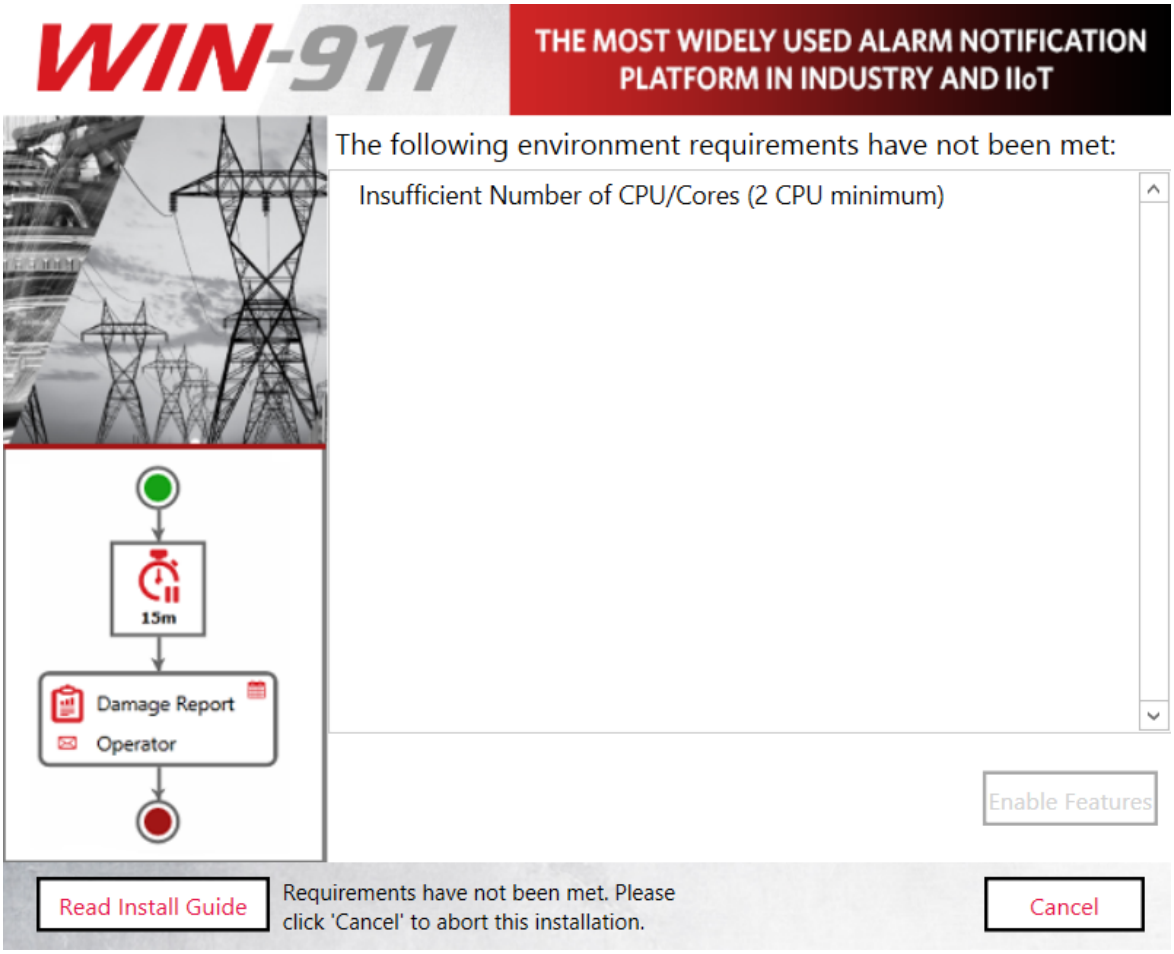
To join a distributed WIN-911 System you will first need to create a distributed WIN-911 System that includes the support modules. This is done by installing the WIN-911 Support modules on your primary (Dispatcher) host computer.



Attention: When using a language other than English select it here.

Click **"Next"** to begin WIN-911 Setup.

The installation program checks whether or not the environment requirements are met.



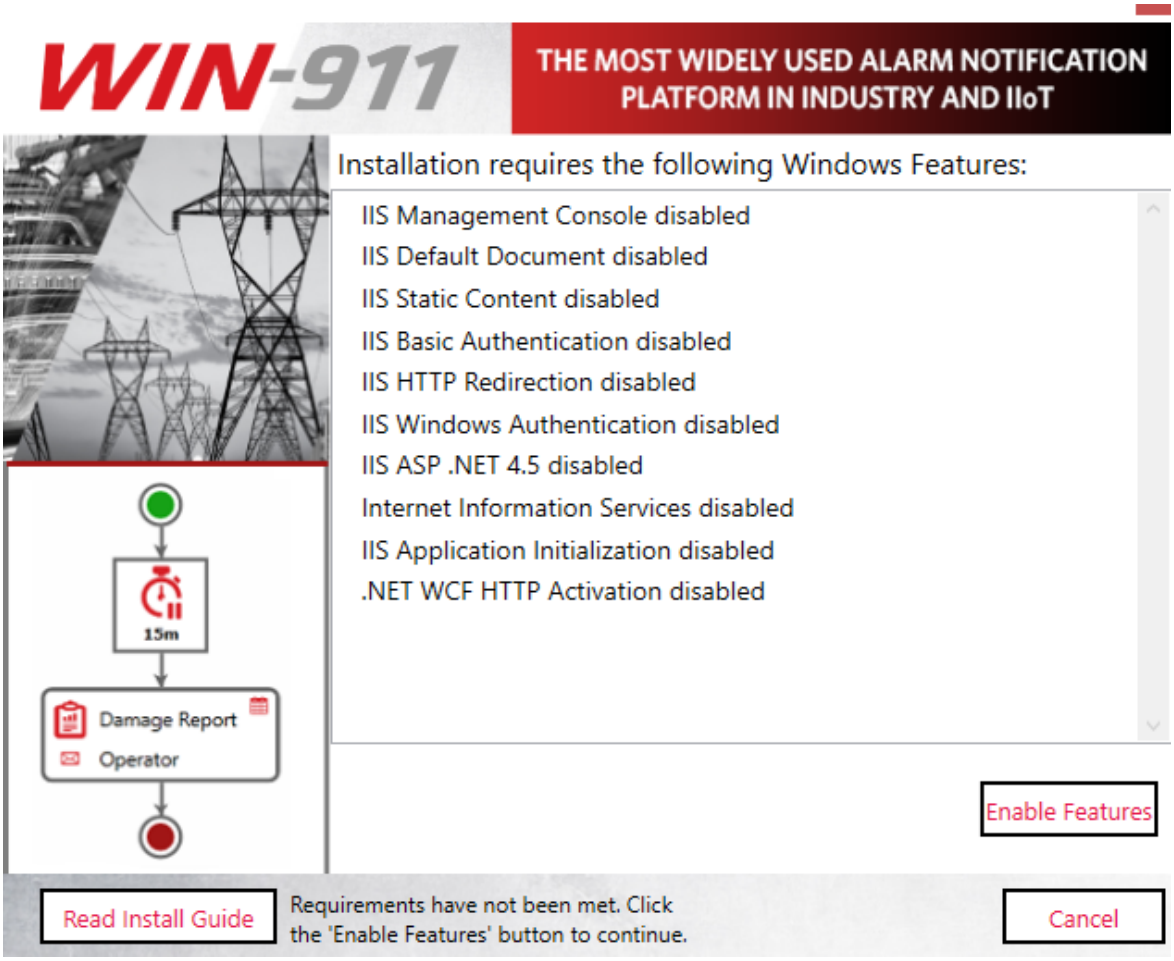
Such environment requirements include:

- Supported 64-bit OS
- Sufficient minimum disk space
- Sufficient minimum processors/cores
- Installing user be a member of local administrator's group

See WIN-911 4.21.5 System Requirements at the top of this document for more information.

Note: If these requirements are met, this page will not appear.

The installation program will then check for the required features.



Feature requirements include the following:

- Microsoft .NET 4.8
- Windows Edition and Feature Set Detection
- IIS Features: Application Initialization, Basic Authentication, Windows Authentication, HTTP Redirection and ASP.NET 4.5, HTTP Activation

Any missing feature can be enabled by clicking the Enable Features button at the bottom right.

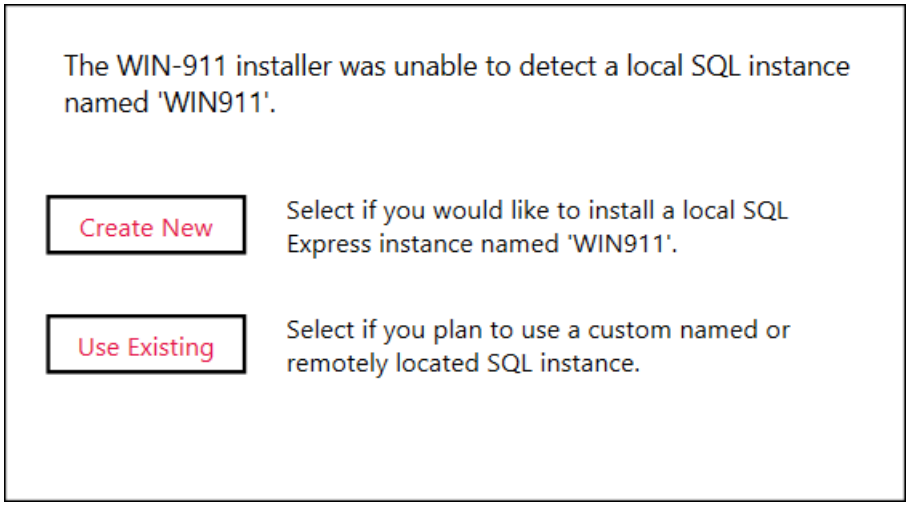
Note: If these requirements are met, this page will not appear.

SQL Server Installation

When joining an existing WIN-911 system, you have the option of creating a distinct SQL instance on the new host or you may utilize the existing SQL instance.

Note: It will be easier to conduct SQL backups when using a single instance, however, this will require network access.

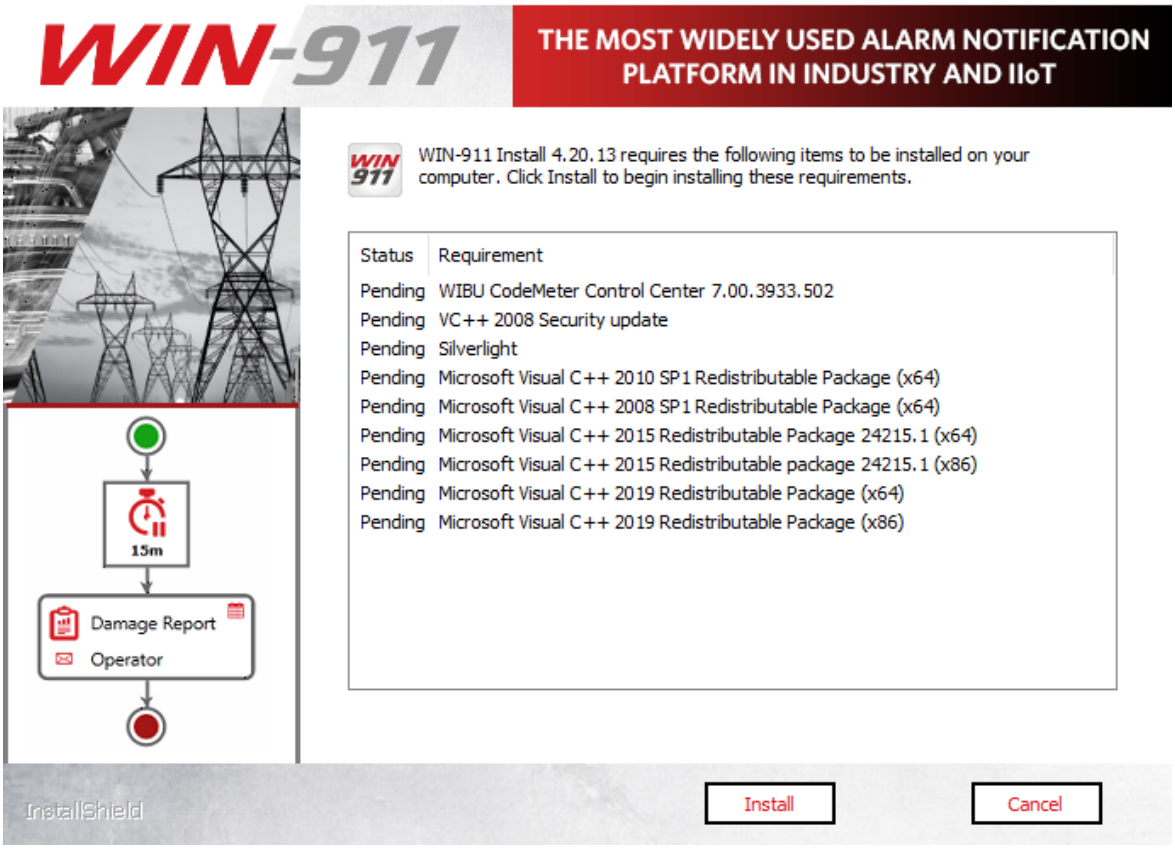
The install script will check the WIN-911 host for an SQL Server instance named "WIN911". If there is no suitable SQL Server, the following pop-up will appear:



This is an optional step and is not required in order to continue with the installation, but WIN-911 cannot be used until the SQL Server requirement is satisfied.

Note: if you are upgrading, you should select "Use Existing" to keep your existing data.

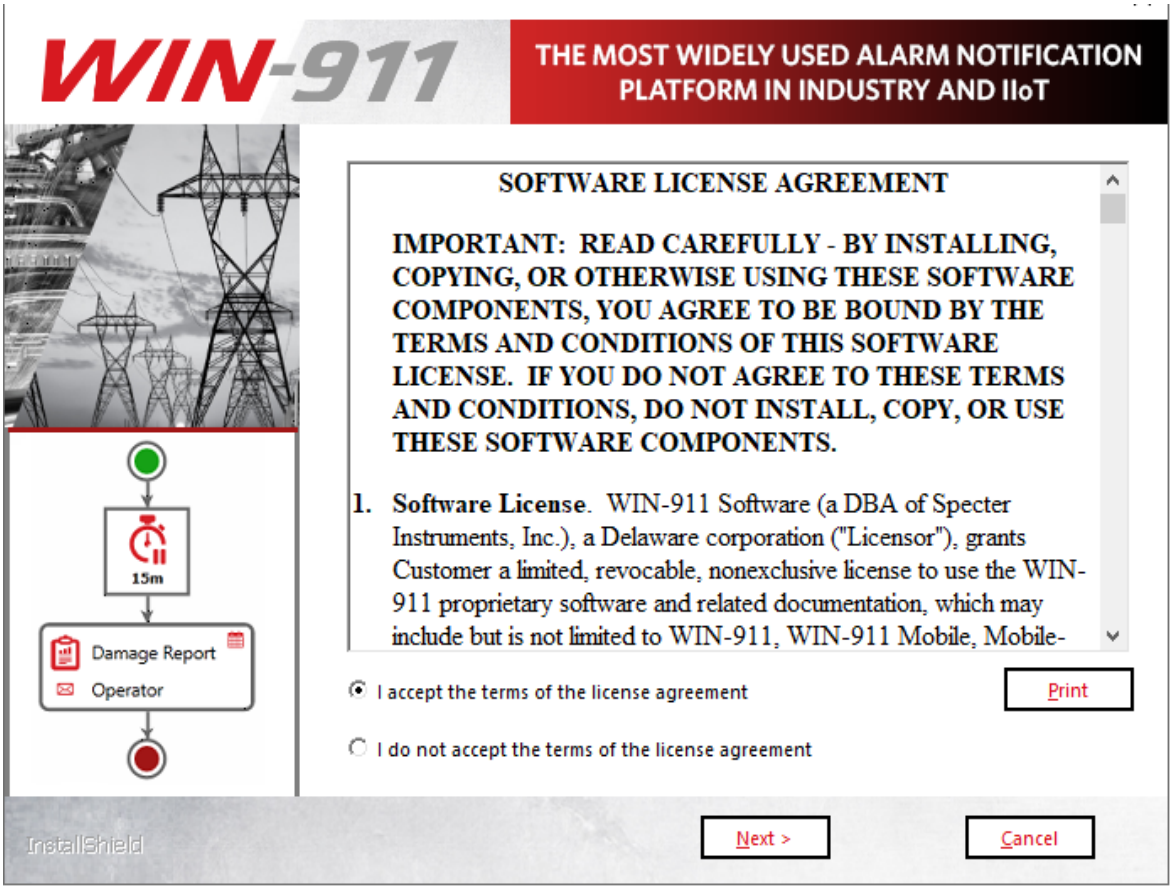
InstallShield Wizard



Depending on the state of .NET Framework 4.8, you may need to reboot prior to continuing.

If requested, select Yes and the install process will resume automatically once the reboot is performed.

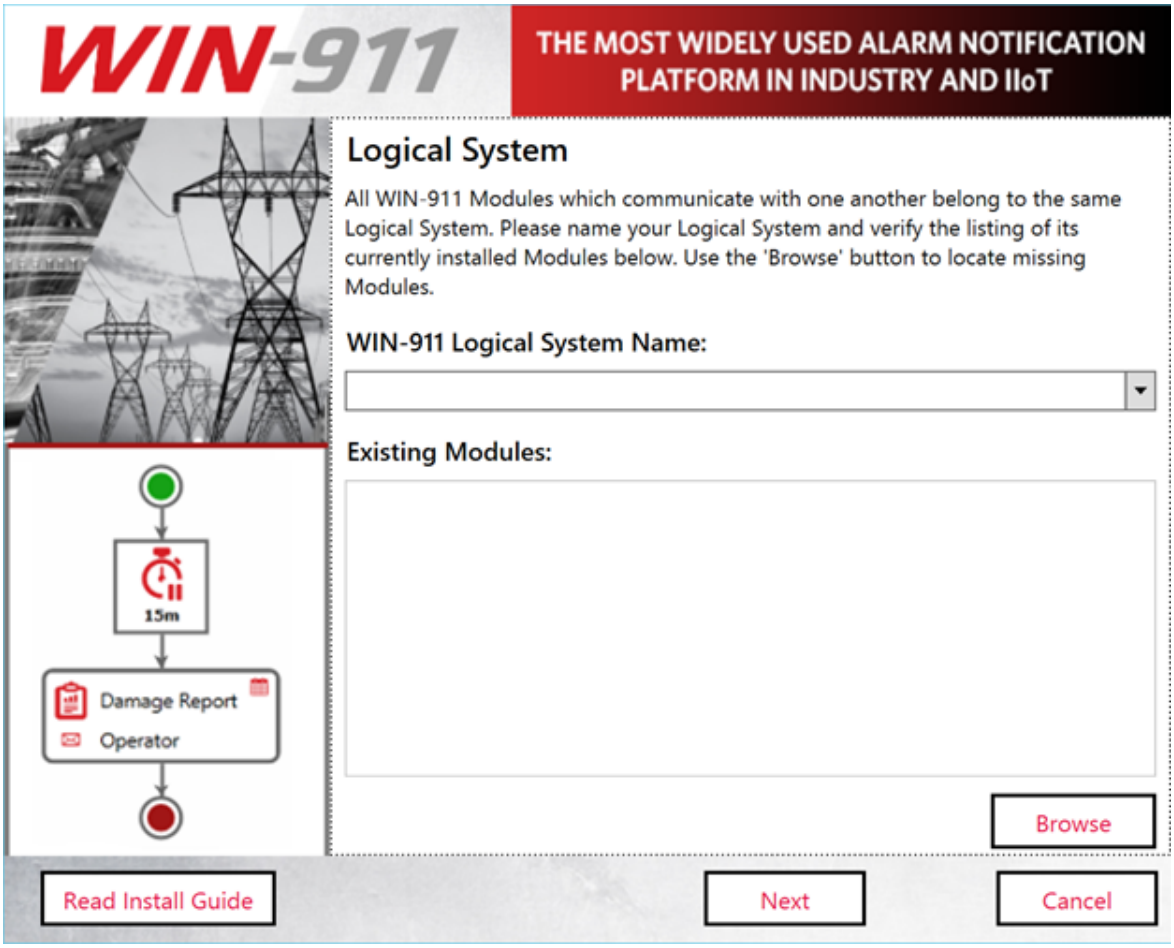
The WIN-911 InstallShield wizard will now guide you through the WIN-911 setup. Click **"Next"** to continue.



Accept the terms of the Software License Agreement by clicking the top radio button and then select **"Next"** to advance.

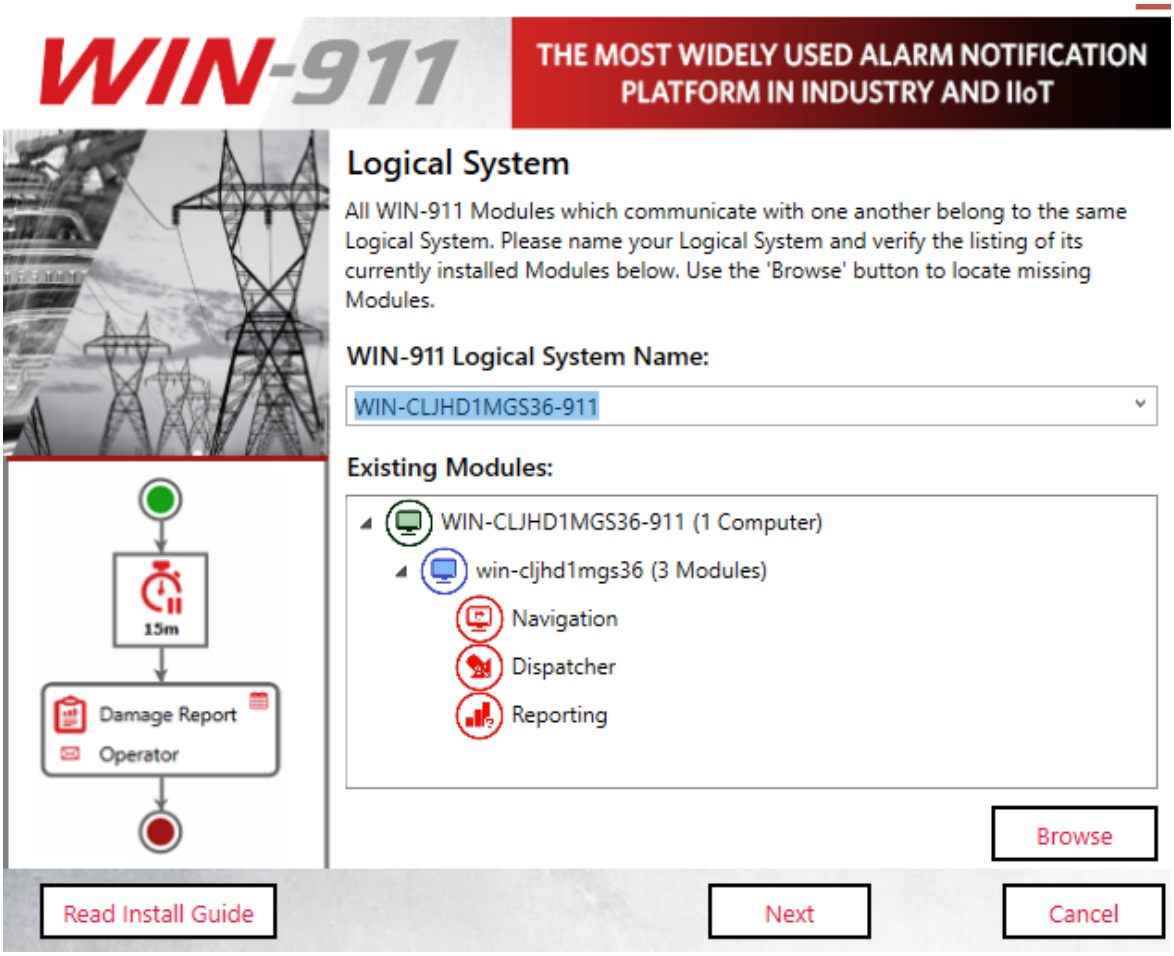
WIN-911 Distributed Systems

When you are joining an existing distributed system you will now be asked to locate all previously installed WIN-911 modules which are part of that system. If you are creating a distributed system or standalone system, then you will not see this step of the installer.



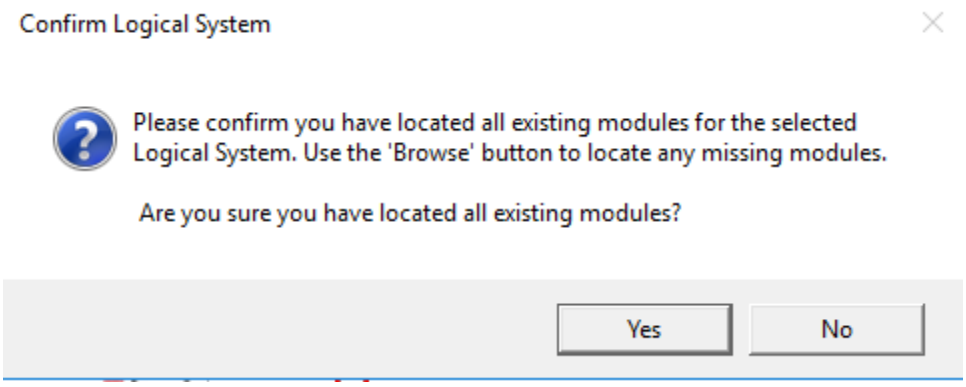
The installer will attempt to discover all previously installed modules with a broadcast on UDP port 3702; however, this discovery attempt will be blocked on many networks. If the discovery results do not display all existing modules, simply click the browse button and browse for or enter the computer name for the target system hosting WIN-911 modules. If no modules can be found on the target system, verify that your network environment allows for communication and authentication of the user attempting this install.

Once all existing modules have been located, select ‘Next’ to continue with the installation. IMPORTANT: Do not continue the installation until all existing modules appear in the list.



Ensure that all of the existing modules appear under the tree. If multiple systems are found select the system you wish to join.

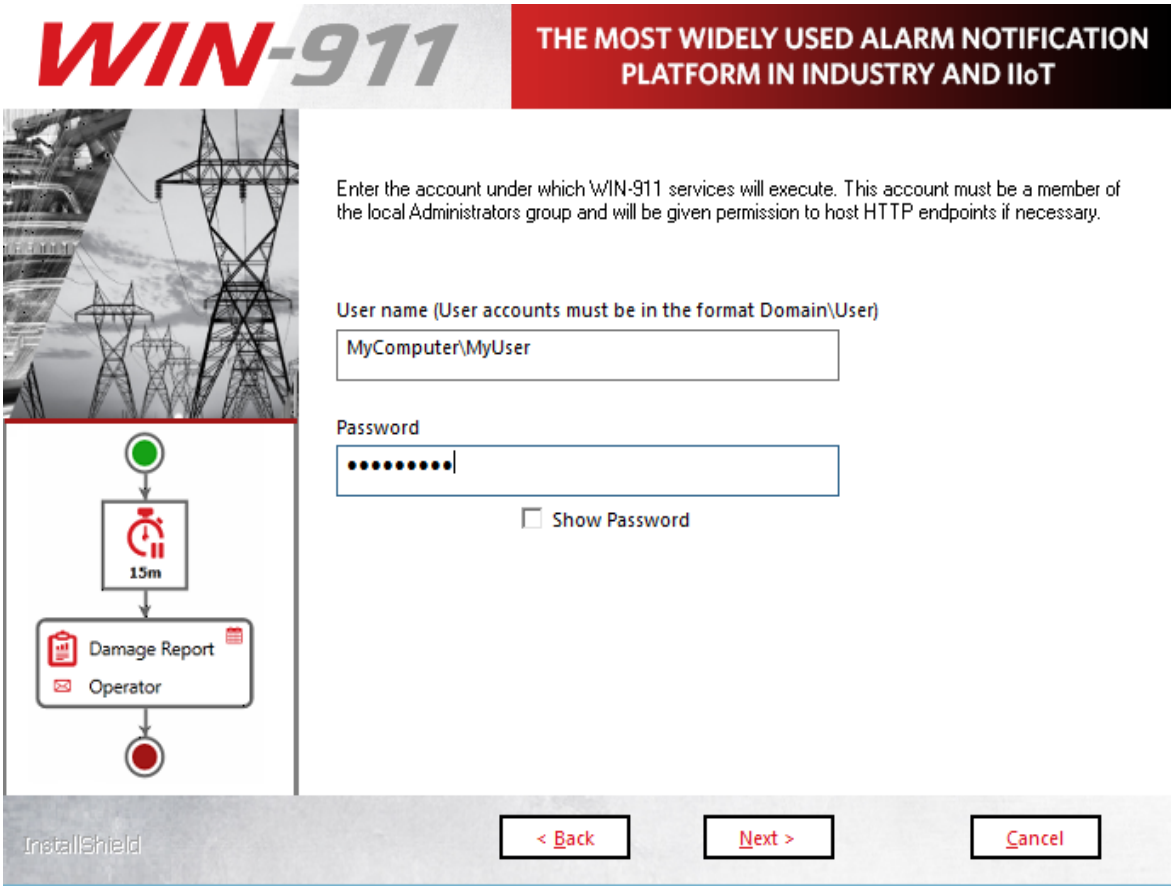
Confirm Logical System.



If all expected modules appear click Yes to continue.

Click Next to continue.

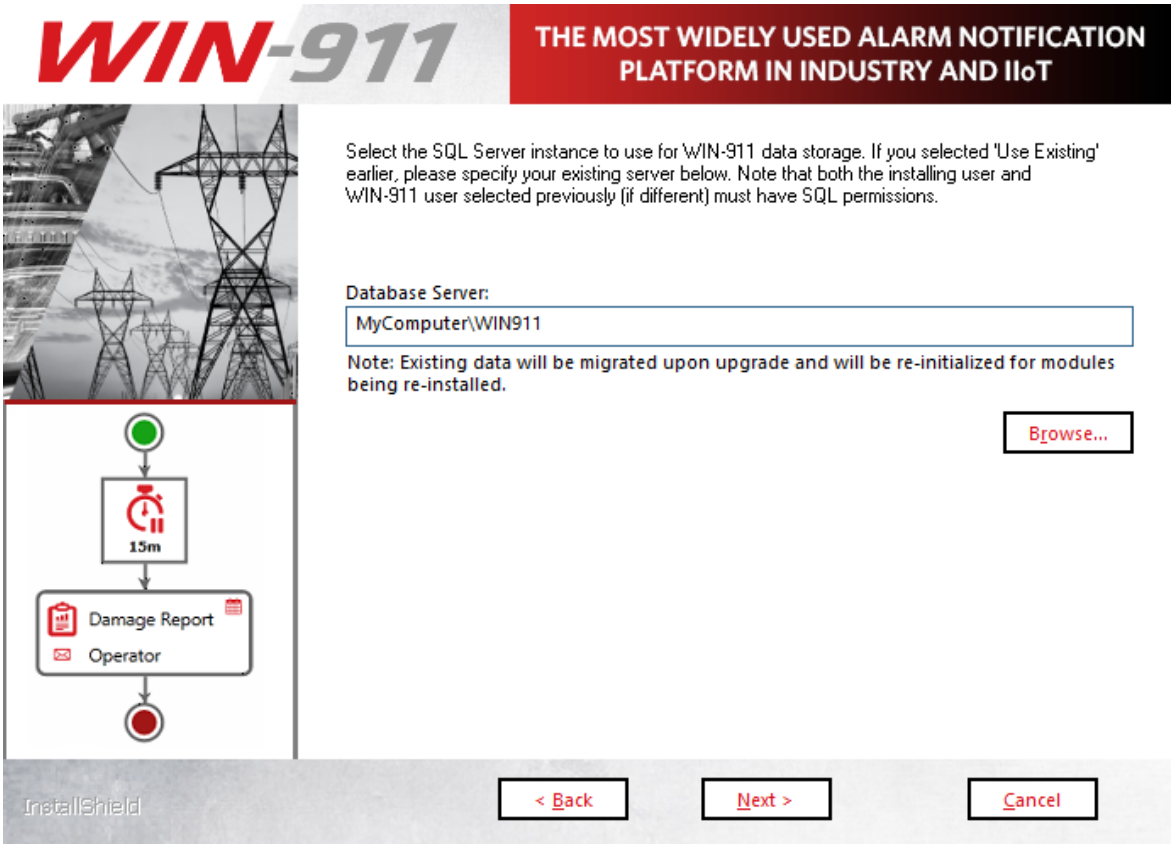
The WIN-911 InstallShield wizard will now guide you through the WIN-911 setup. Click **"Next"** to continue.



Enter the "DOMAIN\username" and password that WIN-911 Services will run under. If a user name and password are not yet set up in the operating system you can use the **"New User Information ..."** script to create one (Windows 8 and higher). This can be found via the control panel, User Accounts. For Active Directory users you will need

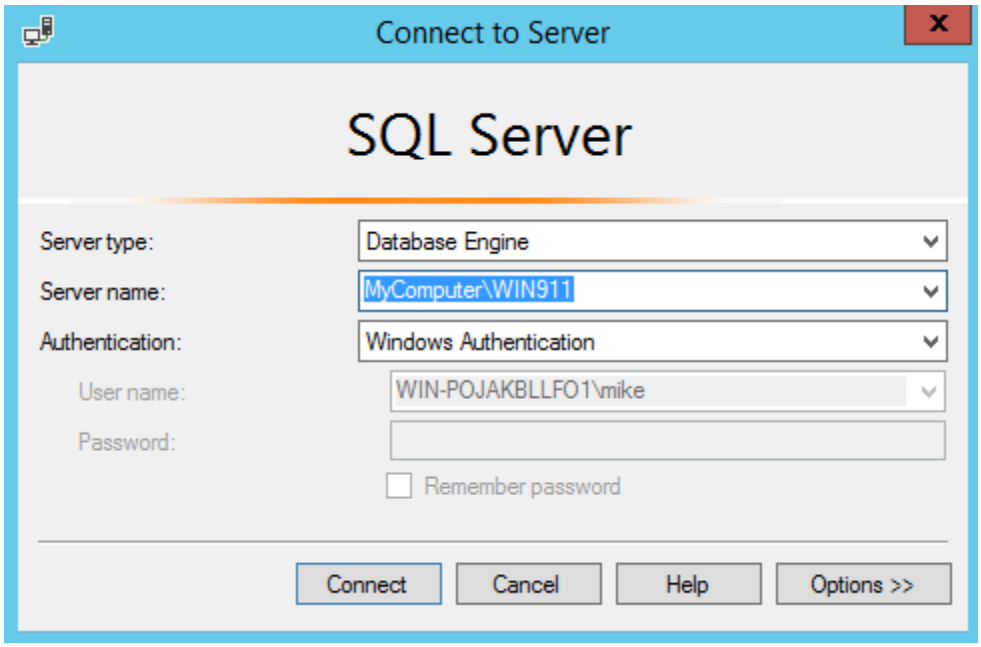
to contact your network administrator or log onto a domain control to create an account with the proper permissions. **When entering a domain user's name be sure to include the fully qualified domain name.**

Note: You must be logged in and executing this installation as an owner and administrator of the SQL instance. Additionally, the selected user here (if different) must be a member of the Windows local or domain administrator group with administrative privileges on the SQL instance.

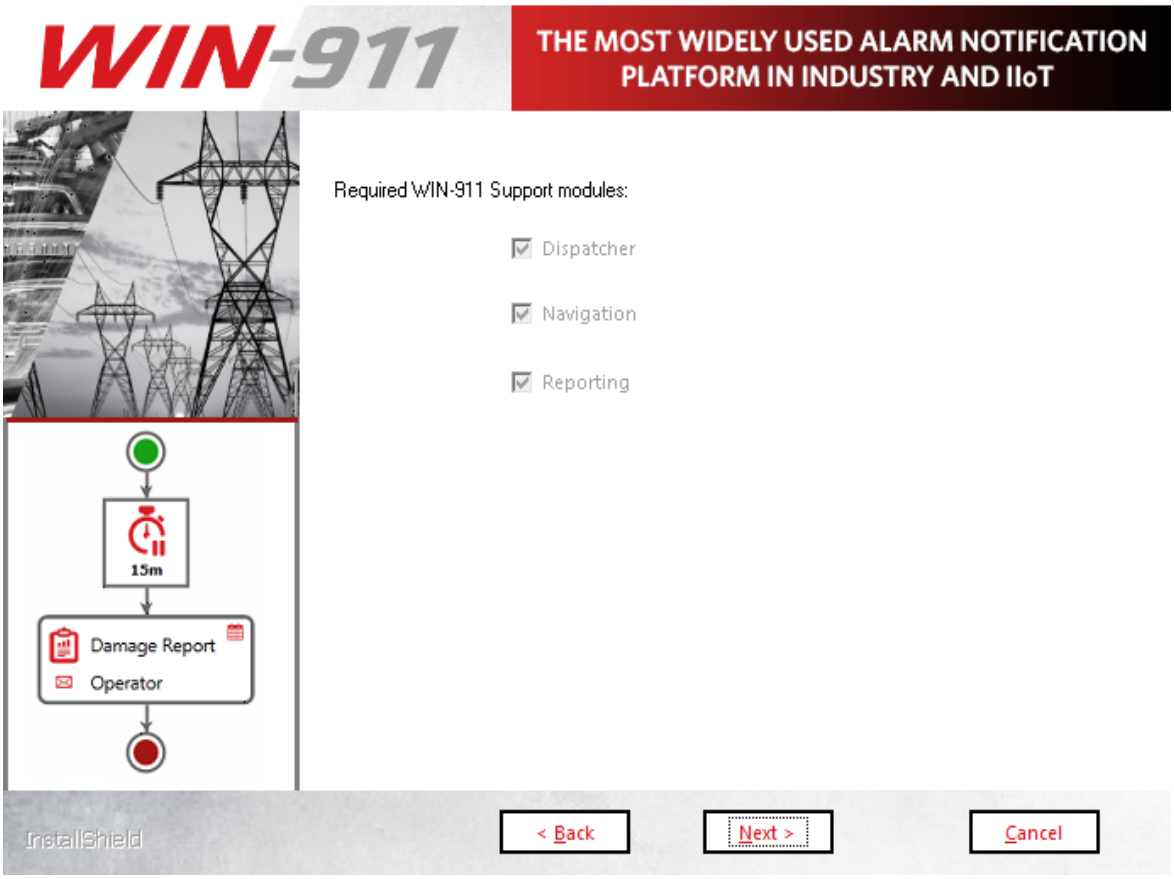


Select the desired database server from the pull-down list. (Server OS's may require you to enable/start SQL Server Browser service in order to browse for SQL Servers)

If you do not see your target server, you may type it into the text entry field as you see it from SQL Management Studio.

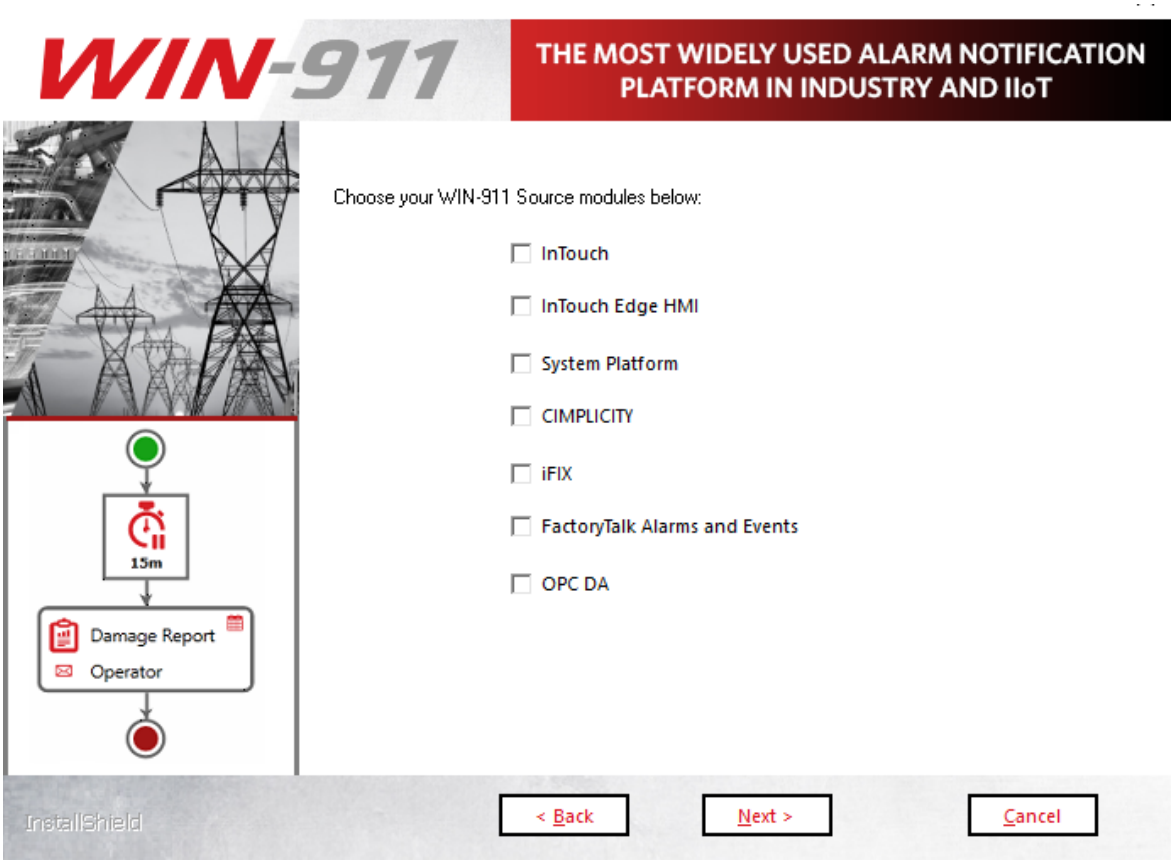


Click **"Next"** to advance.



To created a distributed WIN-911 System you must install all support modules on the primary (Dispatcher) WIN-911 host. Thus, all support modules are displayed as already existing on a remote computer.

Click ***Next >*** to advance.



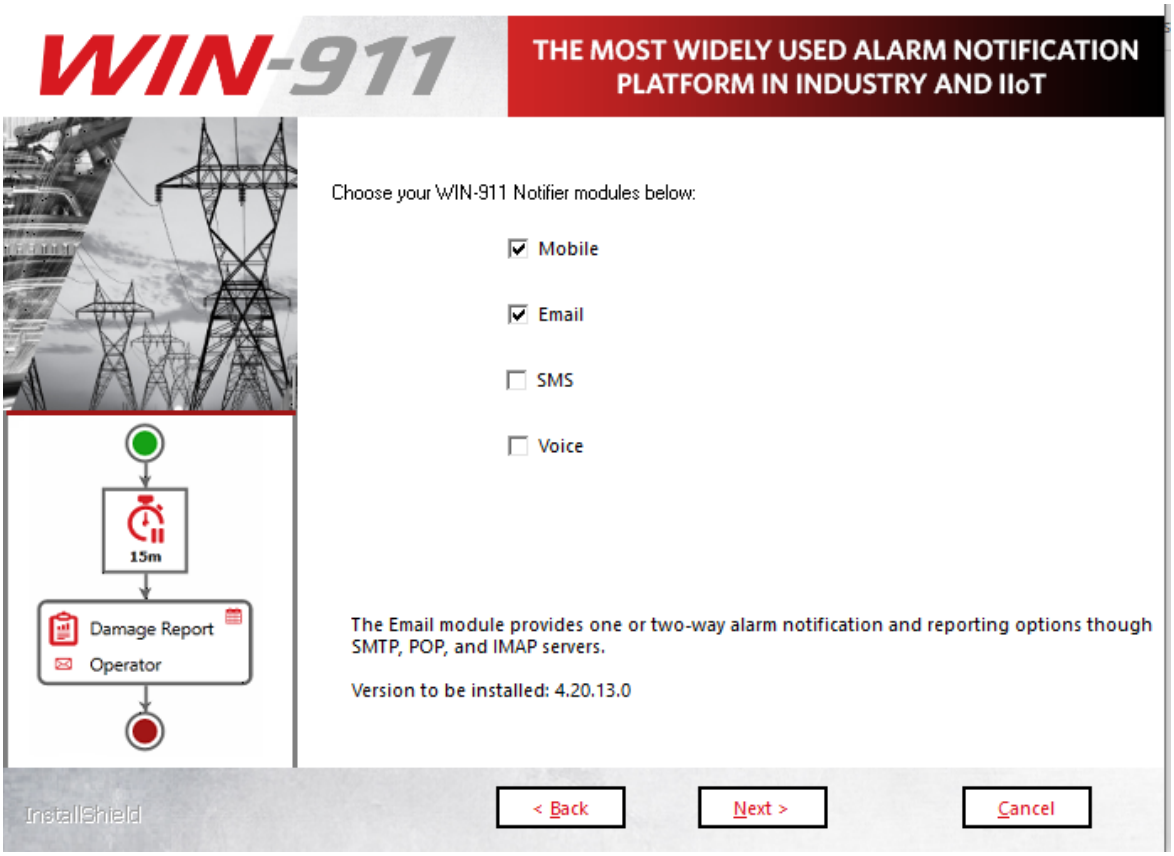
Source modules provide connectivity to various data sources that WIN-911 supports. The source module selection menu allows you to choose which components of WIN-911 you install. Only install the source modules you intend to use. You can always add features later that are not originally installed by re-running the setup.

Any existing remote modules will be displayed as such. You may install additional source modules on this computer. Your distributed system will need at least one source module.

If a selection box appears greyed out, then the option is either required or already present.

Note: Some sources require selection of specific HMI/SCADA versions.

Click **"Next"** to advance.

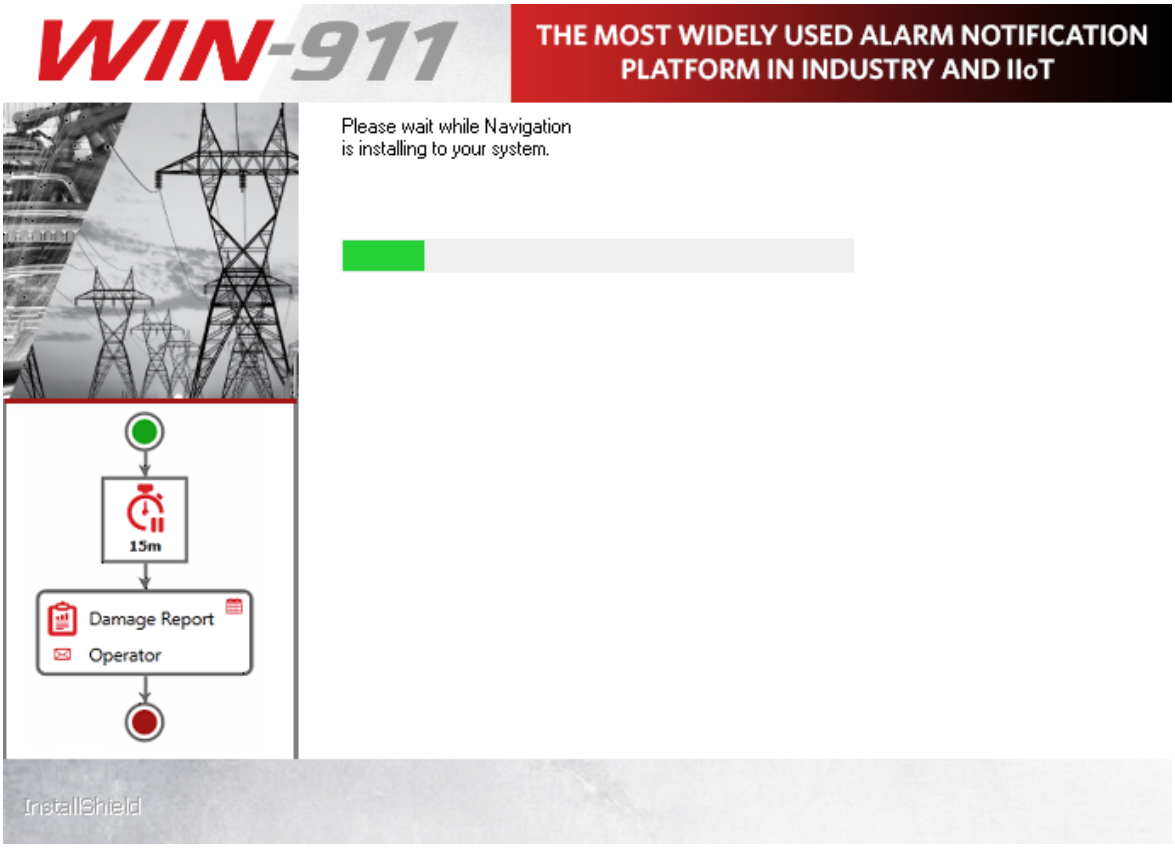


WIN-911 provides several methods of remote notification to users; including Mobile, Mobile-911, Email, SMS, and Voice. The notifier module selection menu allows you to choose which components of WIN-911 to install. Only install the notifier modules you currently intend to use. You can re-run the setup program later if decide to add notifiers to your system.

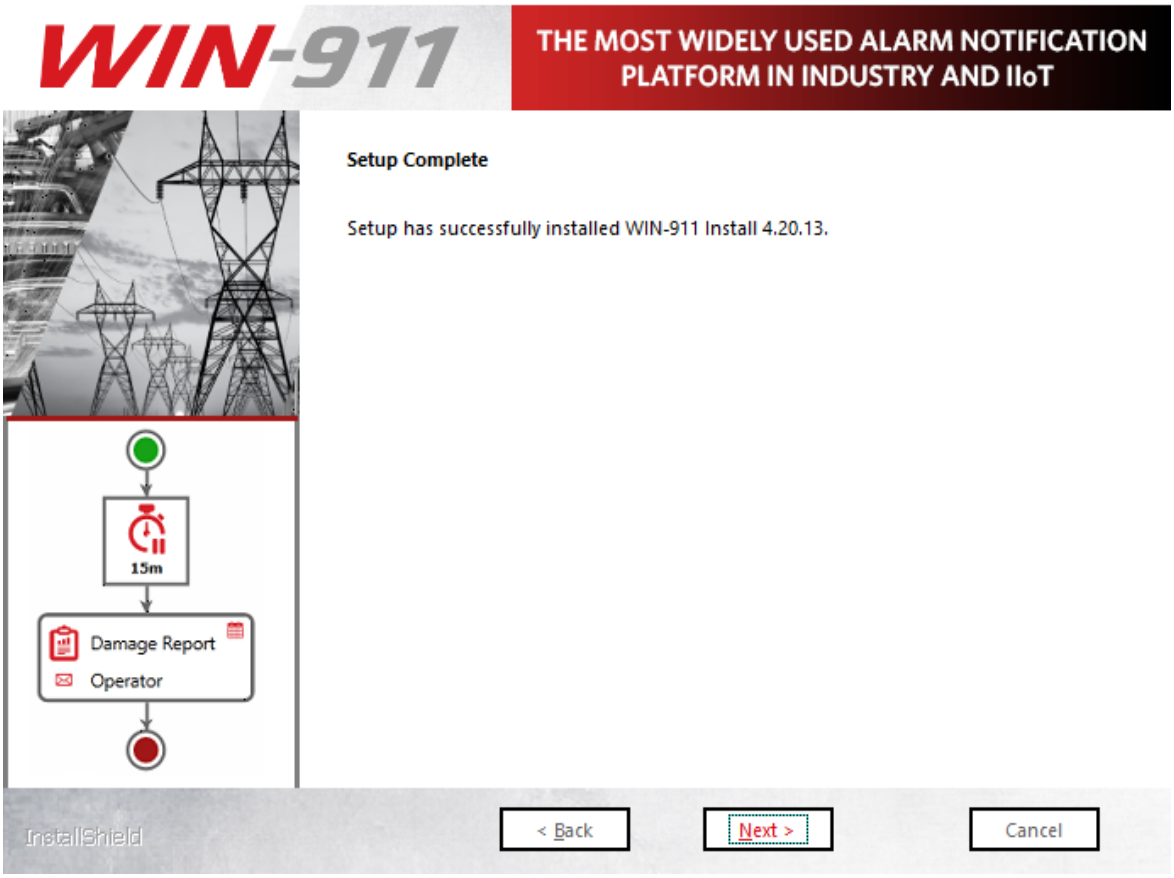
Any existing remote modules will be displayed as such. You may install additional notifier modules on this computer. Your distributed system will need at least one notifier module.

If a selection box appears greyed out then that option has already been installed.

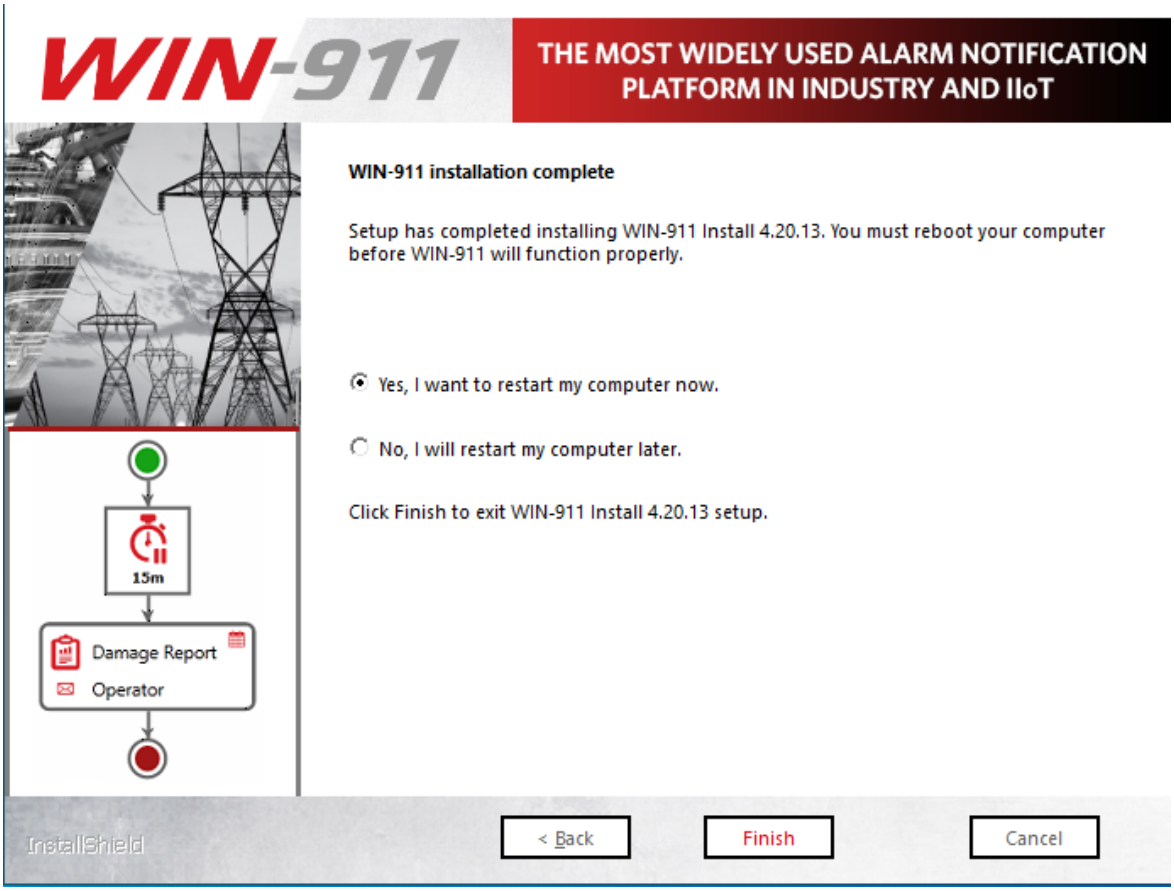
Click **"Next"** to begin the installation and initialization phase of the setup.



This portion of the install may take several minutes.



Click Finish to conclude the installation process.



Once the installation completes, a restart will be required **before WIN-911 can be used**. You can elect to do so immediately or later. Make your selection and click ***Finish***.

[Modifying and Licensing WIN-911]

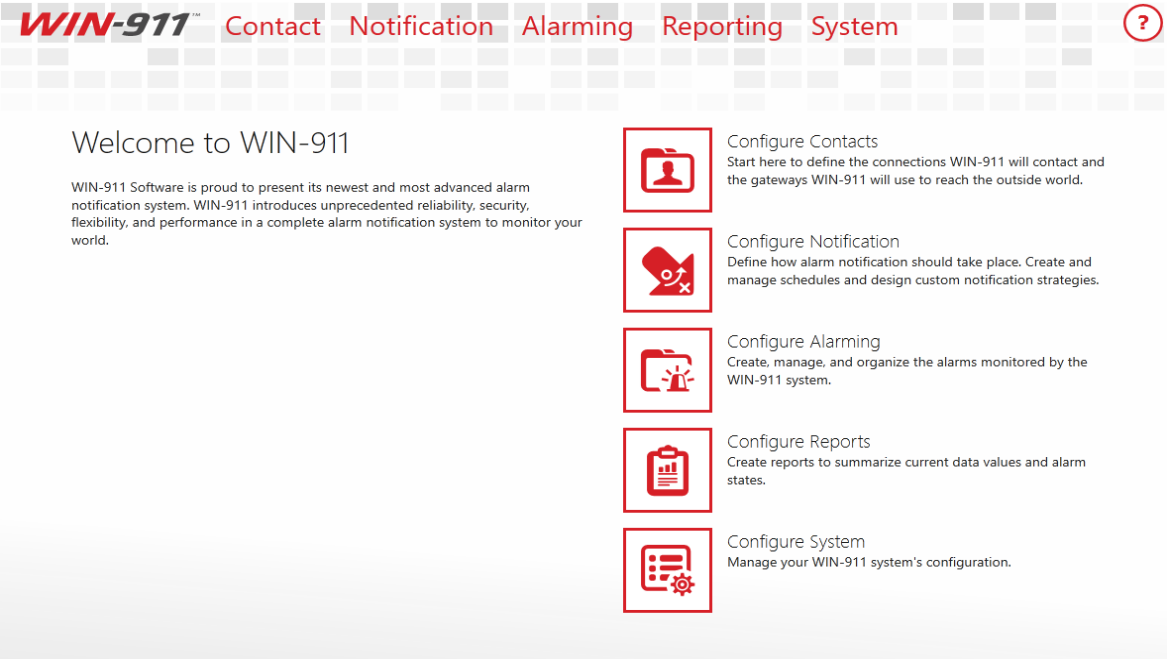
Getting Started with WIN-911

The following guide will explain some key concepts of WIN-911 by walking new users through the configuration of a simple alarm notification system with OPC DA and Email. While the specific technologies discussed may not be applicable to your system, WIN-911 has been designed in such a way that configuring a connection to one data source, or configuring a specific notification method is not that different from configuring another. The fundamental concepts are the same and this guide will serve as an introduction to the platform as a whole.

Note: This scenario is based on the OPC DA datasource, due to its generic and wide-spread use. If you are using a different datasource, the details concerning your datasource configuration are likely to be significantly different in this respect.

There are three basic things that must be configured in every WIN-911 system: who must be notified, when must he be notified, and what he must be notified about.

Accessing the WIN-911 Configuration



WIN-911 is configured with a web-driven interface that resides in the Internet Information Services (IIS) of the WIN-911 host computer. There are two ways to open this website: 1) clicking the shortcut that was created in the WIN-911 host's start menu, or, 2) opening a browser anywhere on the WIN-911 network and entering the WIN-911 Configuration URL.

The WIN-911 installation creates a "WIN-911 Configuration" shortcut in the start menu of the OS that hosts WIN-911. Simply double-click on the shortcut and your browser will open to the WIN-911 Configuration website. You will be challenged for the proper credentials before you are allowed to proceed.

The WIN-911 Configuration website can be accessed from any computer that is on the WIN-911 network, if you have the proper credentials. Simply open a browser and enter the URL: "http://'*WIN-911 computer name*'/WIN911". Note that the last segment of the URL does not contain a hyphen in WIN911. For example: if WIN-911 is installed on a computer named COMP1 and you are a remotely located user (say on computer COMP6), you would start IE and enter

http://COMP1/WIN911. From there you can enter your credentials and modify WIN-911 as desired.

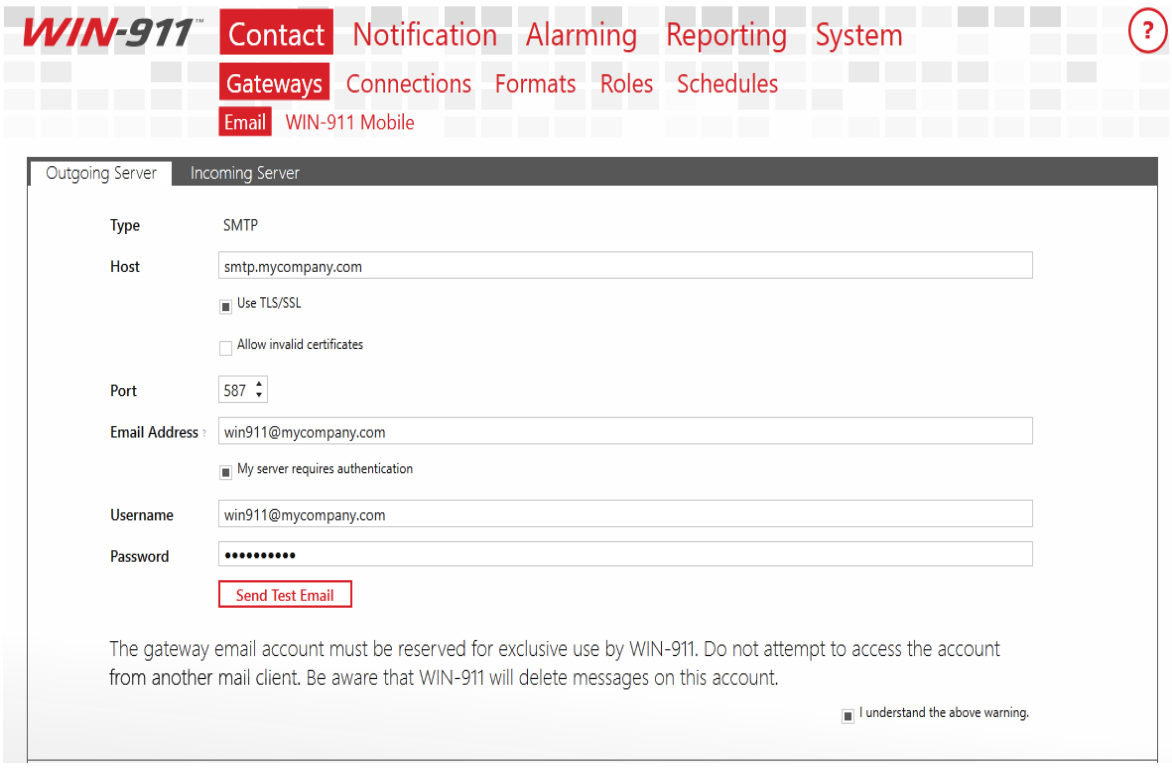
Configure a Notification Method

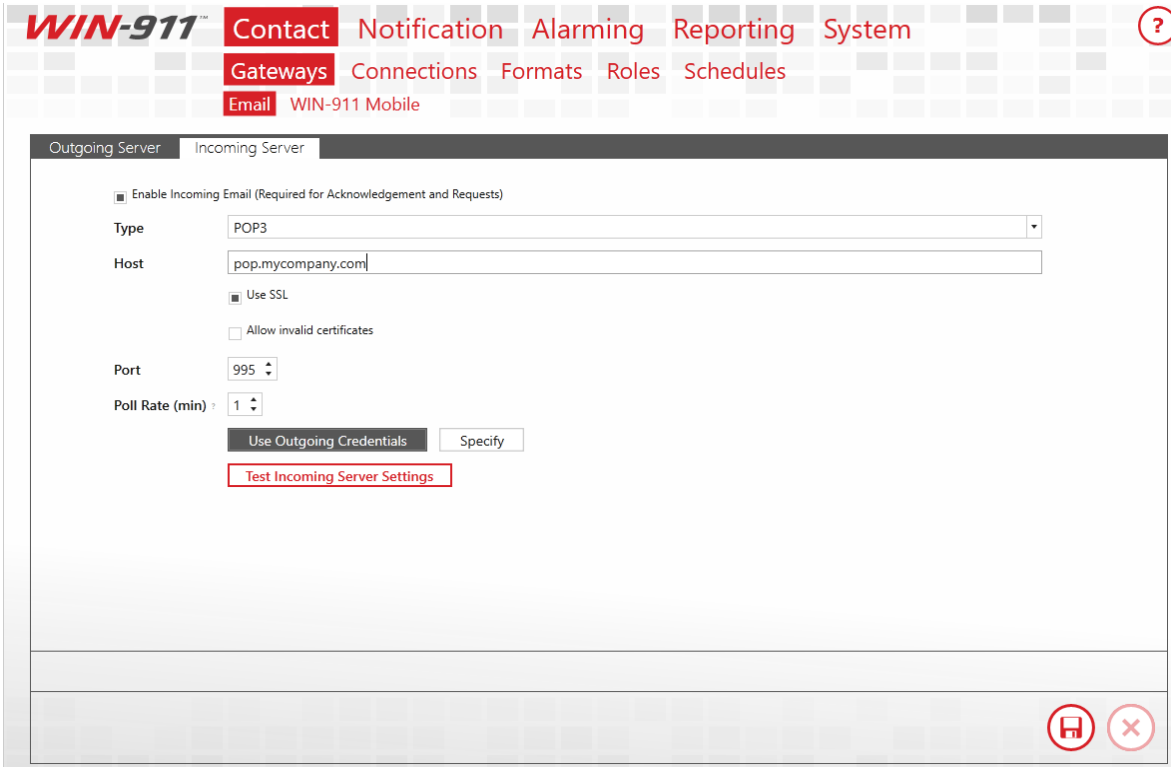
Gateways

It is considered a best practice to configure any new installation by starting on the notification side of things, so we will begin by configuring our Email Gateway. Every Notifier has a Gateway. The Gateway defines the set of information required by WIN-911 to access the outside world. In the Mobile-911 Notifier this is your Mobile-911 server address, for SMS, your modem hardware settings, for Voice, this is your SIP server address and its associated settings or your TAPI modem configuration.

Launch the WIN-911 user interface by opening the shortcut placed in your Windows Start Menu after installation. This will open your browser and navigate to the locally installed Silverlight application. Find the Email Gateway workspace by clicking Contact > Email > Gateway.

Configuring your Email Gateway is much like configuring any Email client like Outlook or a smart phone application. WIN-911 supports SMTP for outgoing mail and POP or IMAP for incoming mail. Obtain your mail server settings from your network administrator, Email hosting provider or ISP. Customers using Exchange Server should consult with their mail administrator about configuring an SMTP relay. Place the settings provided to you in their respective fields.



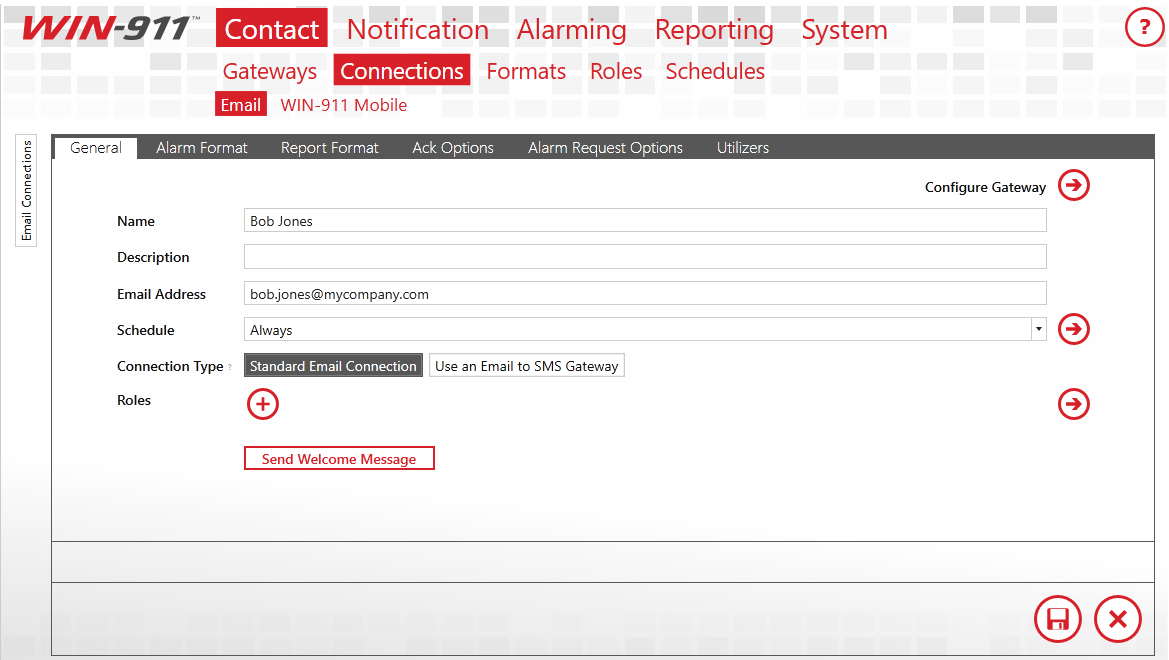


There are two configuration items worth bringing to light here. The first is, in order to connect to your mail server, you must acknowledge

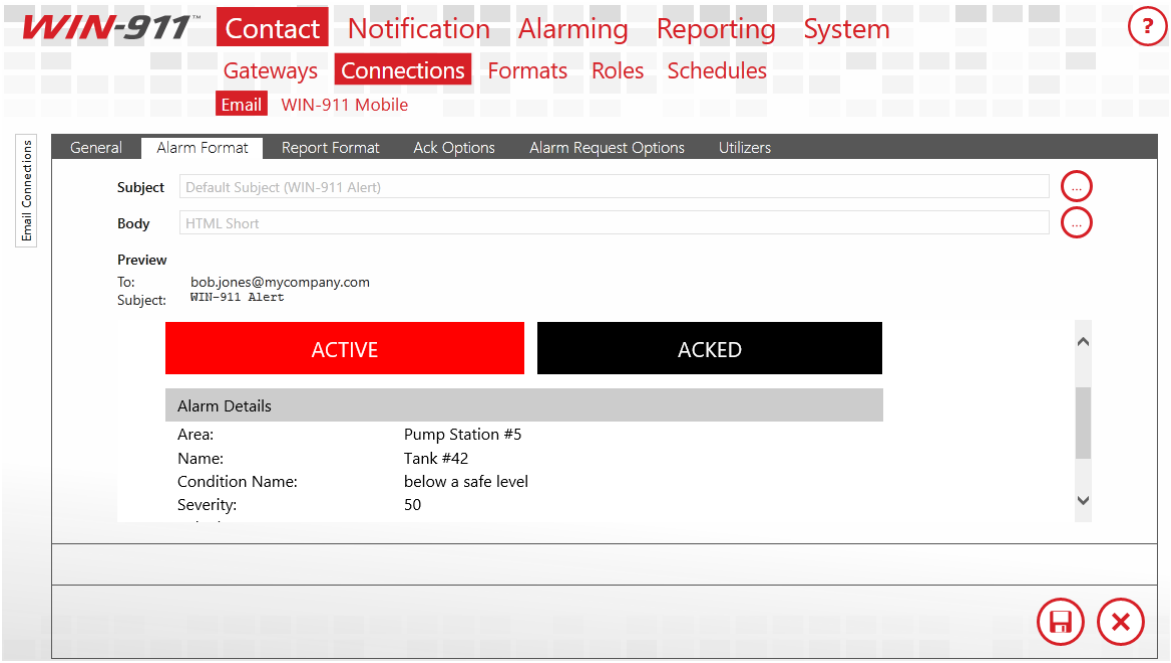
the fact that WIN-911 needs exclusive access to the mail account credentials you provide. WIN-911 will use this account to send and receive mail. It will also delete any mail sent to this address as it processes it, for this reason, you should not use this account for any other purpose. Secondly, you can disable incoming mail by unchecking the incoming mail option on your gateway. This means that users will not be able to acknowledge alarms, or make alarm and report requests. If you wish to allow some users to have incoming mail privileges and others not to, enable the feature here and configure the option on a per-user basis. We'll discuss this in the next section

Connections

A connection defines the specific endpoint WIN-911 will send a notification to. For the Email module, this is an Email address. In other modules, like SMS and Voice, this is a phone number. The connection also defines the format that should be applied to messages, for both alarms and reports. The connection also determines the hours during which a user should be notified, his personalized Schedule.

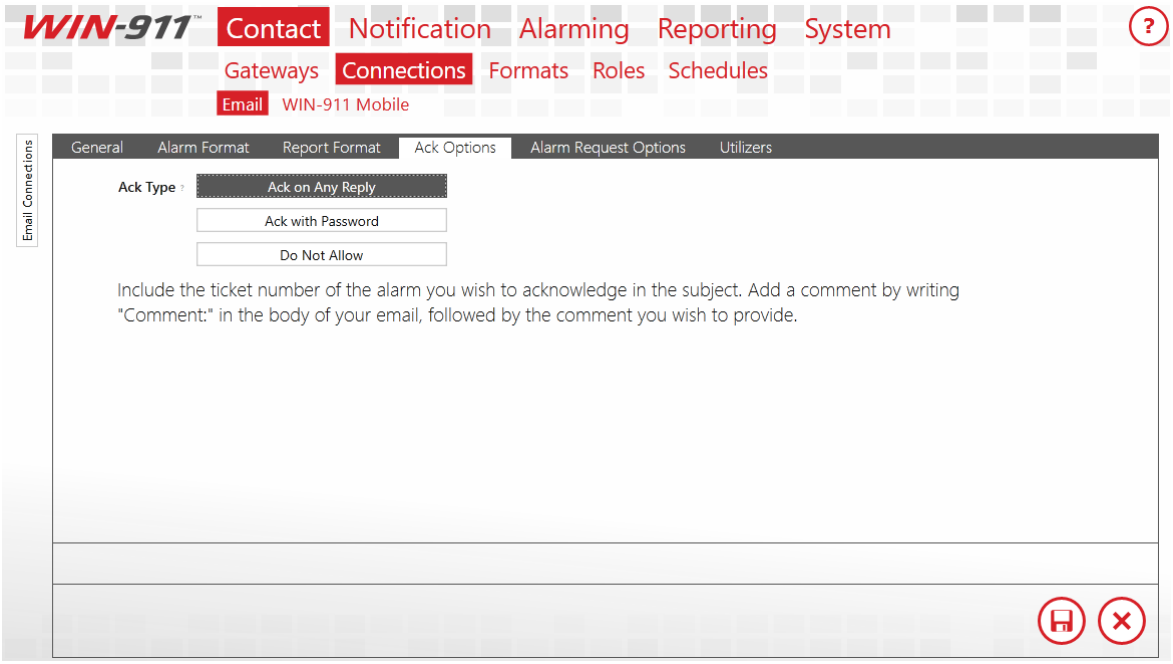


Enter a unique name for the connection and an Email address. Pick a Schedule from the list of default Schedules available to you, or if none of these meet your needs, click the arrow next to the list of Schedules to be taken to a workspace where you may define a new one. Schedules are configured using a calendar control much like any scheduling application. Use the GUI to configure when a connection is on or off duty. When you're done, use your browser's back button to finish configuring your connection. You may also attach a Role to a Connection. Roles are used to organize connections. We'll talk about Roles more when we discuss alarm escalation. There are a few predefined Roles already configured. Use the arrow button to create a new one, if you would like to. An arrow next to any field will take you to a workspace where you may configure that setting. You'll find this pattern repeated throughout the WIN-911 user interface.



Select an Alarm Format that best suits your needs. You may format the subject and body in any way you wish. WIN-911's message formats are stored as XSLTs. XSL is a powerful programming language used for transforming XML documents. WIN-911 uses XSLTs to transform

alarms into Email messages, voice calls, text messages, etc. Editing XSL is quite a complex task and is well outside the scope of this document. For more information on creating XSLTs, consult with W3Schools or contact WIN-911's support department. We'll be glad to help you design a Format that best suits your needs.



The Ack Option tab defines how alarms should be acknowledged by this connection, or if this connection should be allowed to acknowledge alarms at all. Select "Ack on Any Reply" and when WIN-911 receives a reply from this connection about an alarm, WIN-911 will acknowledge the alarm. Select "Ack with Password" to require a specific phrase be present in the reply message.

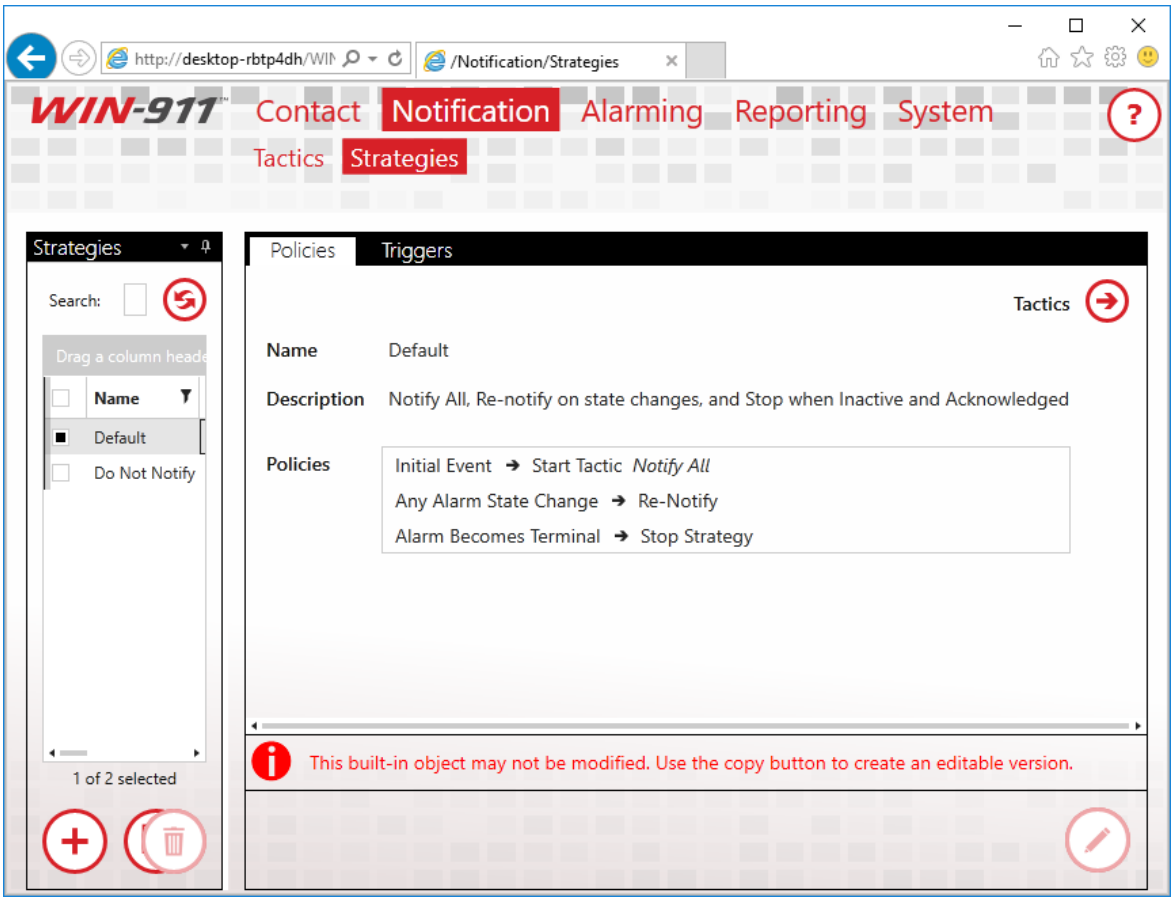
There are a few more settings available for you to configure, but they are not necessary. For the full documentation regarding Email Connections, see the WIN-911 Email manual. Save the Connection and we'll move on to configuring your escalation rules.

Configuring Escalation

The Dispatcher module is responsible for accepting alarms from data sources, running your escalation rules to determine who should receive those alarm messages and when. It sends these messages out to the appropriate notification module, which will, in turn, send them to their final destinations.

Strategies

Strategies are simply a list of events and how WIN-911 should respond to those events.



The Default Strategy will send every alarm to every connection configured in your WIN-911 system and send every update about every alarm to every user who previously received a message about the alarm. It will stop sending messages after the alarm is Terminal. An

alarm is considered Terminal when it is inactive and acknowledged. The Strategy only has three rules, formally called Policies, which define this behavior.

Initial Event -> Start Tactic “Notify All”
Any Alarm State Change -> Re-Notify
Alarm Becomes Terminal -> Stop Strategy

The first rule means that when the initial alarm is received, WIN-911 should start a Tactic called “Notify All.” The Tactic determines who should actually be notified for an event. The “Notify All” Tactic tells WIN-911 to notify every connection configured in the system about the alarm. When it does so, it takes into account the Schedule defined for the connection. If the connection is on-duty, the alarm will be sent, if it is off-duty, the connection will be passed over. We’ll talk more about Tactics later.

The second rule says that when any state change is received for the alarm, WIN-911 should send a message to anyone who previously received a message regarding the alarm. An alarm is considered to have changed state when either the active or acknowledged state changes.

The last rule says that when the alarm is both active and acknowledged, it should stop processing the strategy rules for the alarm. This ends the life-cycle of the alarm.

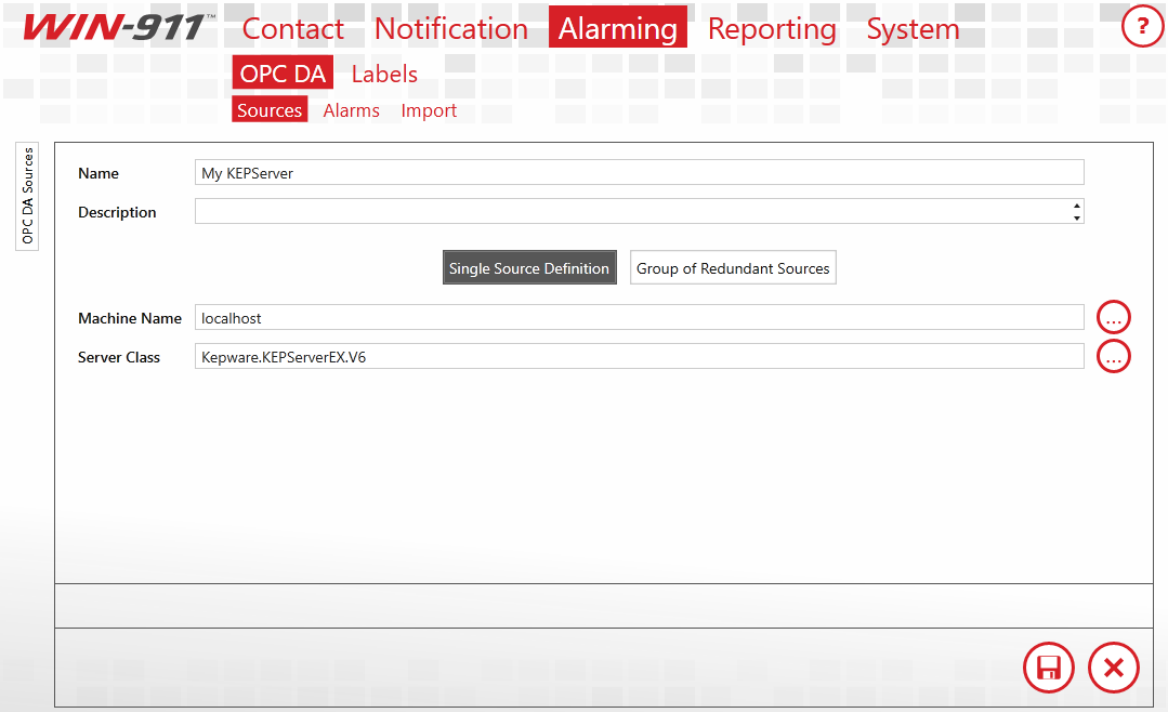
There are two types of Tactics, Basic and Advanced. Basic Tactics are simply a list of connections. When a Basic Tactic is started, everyone on the list is notified. Basic Tactics are easy to configure, and correspondingly, offer less flexibility regarding notification. That said, they meet the majority of users’ needs and have the added benefit of being quite easy to maintain.

Advanced Tactics are essentially flow charts which determine who should hear about an alarm. Each block in the chart represent either an action to be taken or a decision to be made. These actions are generally Notification Blocks. Notification Blocks send messages to the connections specified in the block. You may also place a Role in a Notification Block. When you do this, any connection which has that Role attached, will be notified. Decision Blocks allow the chart to branch, decisions may be made based on properties of the alarm or the amount of time the tactic has been executing. Advanced Tactics are quite powerful and quite nuanced. A full discussion on them can be found in the Dispatcher manual. You may have noticed that we haven't configured anything on the Dispatcher yet. We'll go ahead and stick with the Default Strategy for now, and move the discussion along to the OPC module.

Configure Data Sources

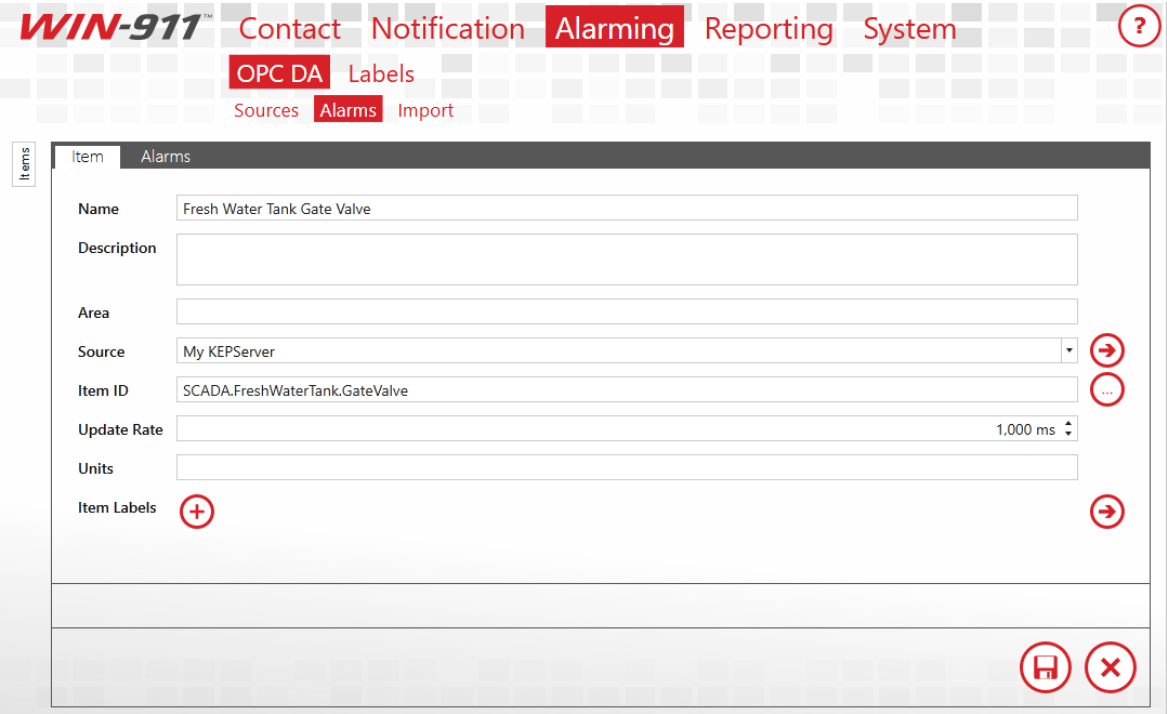
Sources

WIN-911 needs to know where to look for your alarms, or in the case of OPC DA, where to access your data so it can generate alarms based on the information it's provided. This point is an important one, so I'll state it plainly. Alarms are configured in WIN-911 for OPC DA data sources and WIN-911 determines when a specific alarm condition exists. Other Data Sources, like iFIX, CIMPLICITY and FactoryTalk determine when an alarm condition exists and pass that information onto WIN-911. This means that, with the exception of OPC DA, all of your alarm maintenance remains in your SCADA where it belongs. The remainder of this guide will assume that you have a locally installed OPC DA server and at least one digital point configured in that server.



Start configuring your OPC DA module by connecting WIN-911 to your OPC server. In the OPC DA menu, create a new Source. Once again, the Name field is user defined and does not relate to any setting on your server, so be as descriptive as possible. The Machine Name is the hostname or IP address of the computer that your OPC DA server is installed to. If the server is running on the same machine as WIN-911, set this to "localhost." The server name is the name of your actual OPC DA server. Leave the radio button set to "Single Source." Redundant OPC DA is outside the scope of this document. Save the Source and click the Alarms link in the navigation menu to create an OPC DA alarm.

Alarms

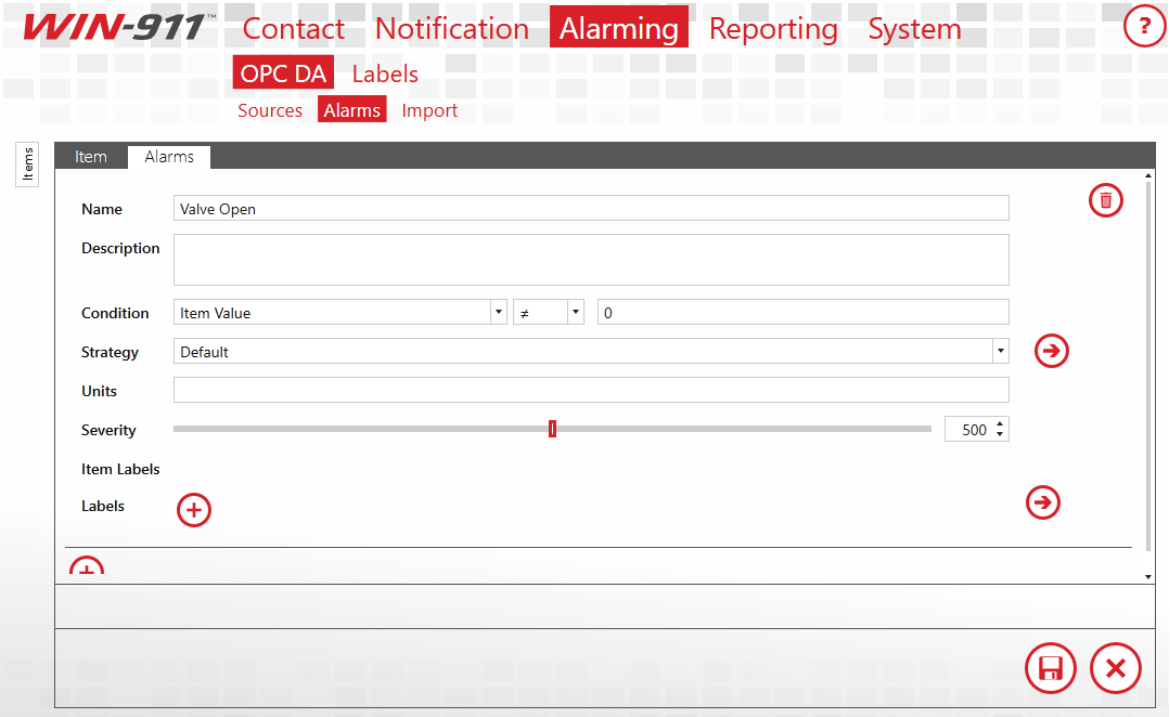


There are two components to any OPC DA alarm, the data on which the alarm is based, and alarm definition itself. Create a new item and enter a descriptive name for it. Again, the Name field is user-defined and does not relate to any setting on your OPC DA server. Select the OPC DA Source you configured previously. Type the Item ID of your OPC DA item in the Item ID field, or click the browse button to browse your server directly. Units are optional and are always a good idea, if you're dealing with an Analog Item. Since our point is Digital, we'll skip it.

Labels

Labels are another organization feature of WIN-911, much like Roles. Tactics can treat Alarms with specific labels differently that other alarms. For instance, if you label alarms by building or assembly line, you can use a Label Decision Block to notify one set of your personnel about alarms on assembly line 1 and another set for alarms on assembly line 5. We'll skip labels for our Digital Alarm for now, but this

is a powerful feature that you'll want to revisit once you create your production configuration.



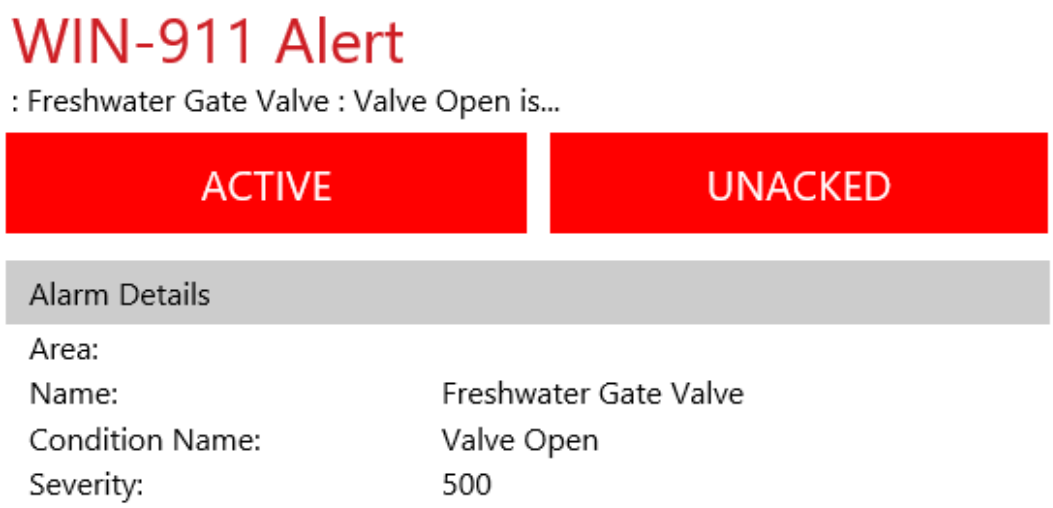
Click the Alarm tab to define the condition under which this OPC DA Item will generate an alarm. Our alarm will be triggered when the value is not zero. Enter a descriptive name for the Alarm and set the Condition so that when the Item Value is not equal to zero, our alarm is triggered. Set the Strategy to the Default Strategy, which we discussed earlier. The Strategy selection you make here is how WIN-911 associates alarms with specific Strategies. We're telling WIN-911 that when this alarm condition is met, it should execute the Strategy defined here. The Strategy then executes the Policies configured within it.

Before we save our Alarm, it's worth mentioning that WIN-911's configuration is live. As soon as you make changes to your configuration, they're executed. If you need to do maintenance on your WIN-911 system, and wish to avoid sending nuisance alarms to your users, you should place WIN-911 into Standby Mode. You'll find

this option in the navigation menu under "System > Standby/Activate."

Once you're satisfied with the changes you've made to your configuration, simply place WIN-911 back into Active Mode.

Let's save our alarm and toggle the OPC DA item in our OPC DA server to "1." You should receive an alarm message at the Email address you configured at the beginning of this guide. It should look something like this:



Congratulations on configuring you first WIN-911 System.

What just happened? You triggered the alarm by toggling it to a non-zero value. This is the Initial Event that the Default Strategy mentioned. Because the initial event was received, WIN-911 started the Notify All Tactic, which sent the alarm message out to everyone in your WIN-911 system. Everyone includes our one and only Email connection, so we received the alarm message.

Toggle the OPC DA item back to zero and the alarm state will become inactive. Because this represents a state change, the Default Strategy will execute the Policy for Any State Change., which tells WIN-911 to renotify everyone who was sent the alarm message again. You should get an Email indicating that the alarm is now inactive.

If you set your connection up with the "Ack on Any Reply" setting, reply to this message. Leave the subject alone, it contains a ticket number, which WIN-911 uses to identify which alarm you would like to acknowledge. You can leave the body of the Email blank, or leave it filled with the history of your thread. If you set WIN-911 to require a password to acknowledge the alarm, enter that password anywhere in the body of your Email.

After WIN-911 acknowledges the alarm, you'll receive another message, because of your renotification policy, which will indicate that the alarm has indeed been acknowledged. Because the alarm in now Inactive and Acknowledged, WIN-911 will stop the executing Strategy and the lifetime of the alarm is now completed.