

# **WIN-911 Enterprise Installation**

---

# Table of Contents

## Contents

<b>WIN-911 Enterprise Edition Installation</b> .....	4
WIN-911 Enterprise Edition 3.16.20 System Requirements .....	4
SQL Server Requirements .....	6
SQL Server not found on node: small configuration.....	6
SQL Server not found on node: medium and larger configurations (over 5000 data points) .....	6
Compatible version of SQL Server already installed .....	7
New version of SQL Server already installed.....	7
Incompatible version of SQL Server already installed.....	7
Install SQL Server Express on remote network computer.....	7
Installation Path .....	8
WIN-911 Enterprise Edition Setup .....	8
SQL Server Installation .....	9
Requisite Programs and Features .....	11
InstallShield Wizard .....	12
Modifying WIN-911 Enterprise Edition .....	23
Adding features to your existing WIN-911 installation .....	23
Removing features from your existing WIN-911 installation .....	24
<b>Uninstalling WIN-911 Enterprise Edition</b> .....	24
WIN-911 Endpoint Mapper .....	25
Licensing WIN-911 Enterprise Edition.....	26
Upgrading to WIN-911 Enterprise 3.16.9+ .....	30
Affected Versions.....	30
Re-licensing .....	31
Requesting a New License for WIN-911 Enterprise .....	33
Install Upgrade License.....	34
Getting Started with WIN-911.....	35

Configure a Notification Method .....	35
Gateways .....	35
Connections.....	37
Configure Escalation .....	40
Strategies.....	41
Configure a Data Sources Sources .....	42
<b>Alarms</b> .....	<b>44</b>

# WIN-911 Enterprise Edition Installation

## WIN-911 Enterprise Edition 3.16.20 System Requirements

### Enterprise Server

- Personal Computer with dual core processor. Quad core processor is recommended.
- 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:
  - Microsoft® Windows® 7/8/8.1/10 (64-bit only), Professional Edition (or higher). Since Windows 10 has continuous updates, you should run the Windows update feature to get the latest software.
  - Microsoft® Windows® Server 2008 R2, Service Pack 1, Standard Edition (or higher). Since Windows Server 2008 has continuous updates, you should run the Windows update feature to get the latest software.
  - Microsoft® Windows® Server 2012, Standard Edition (or higher). Since Windows Server 2012 has continuous updates, you should run the Windows update feature to get the latest software.
  - Microsoft® Windows® Server 2012 R2, Standard Edition (or higher). Since Windows Server 2012 has continuous updates, you should run the Windows update feature to get the latest software.
  - Microsoft SQL Server 2008 R2 through 2014 (Express, Standard, and Enterprise Editions) Note: SQL Server 2014 Express (included with WIN-911) requires Microsoft .NET 3.5 and will also require SP1 for Server 2008 R2.
  - Microsoft SQL Server 2014 Express LocalDB will be installed.
- Internet Information Services (IIS). Application Initialization will be installed for IIS 7.5 (Windows 7/2008 R2).
- Microsoft .NET 4.0 required for install (.NET 4.5.1 required to use WIN-911 Enterprise Edition)
- Optional Notification Hardware:
  - TAPI Voice calls

- TAPI voice modem
- Dedicated analog phone line

#### VoIP calls

SIP compatible VoIP internet account or PBX

#### Supported VoIP Providers:

Skype Connect	Callcentric
Axvoice	SureVoIP
Gafachi	VoIPtalk

#### Supported VoIP PBX Systems:

Ozeki Phone System XE	Trixbox
Cisco Unified CM	OpenSER
Cisco Call Manager Express	PBXnSIP
Asterisk	PBXpress
Asterisk Now	SipX ECS
3CX	Elastix
Kamailio	FreePBX
FreeSwitch	SwyxWare
OpenSIP	Aasta MX-One

#### Mobile-911

- Broadband always-on internet connection for Mobile-911 Server
- iOS, Android and Blackberry devices for the Mobile-911 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.

#### SMS

- MTC-G3 (GPRS), MTC-H5 (HSPA), and MTC-C3 (CDMA) with the AT&T and Verizon networks.
- MTR-G3 (GPRS), MTR-H5 (HSPA), and MTR-C2 (CDMA) with the AT&T and Verizon networks.
- MTCBA-G2 (GPRS) and MTCBA-C1 (CDMA). Note: These modems do not support Unicode.

## Enterprise Client

- Internet Explorer 8 through 11 for Windows
- Microsoft Silverlight 5.1

## SQL Server Requirements

WIN-911 Enterprise Edition uses a SQL Server database to store its configuration data. If a 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 Enterprise Launcher to install SQL Server Express 2014 for you, which is good for small to medium configurations (5, 000 data points or less).

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

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

## SQL Server not found on node: small configuration

If you install WIN-911 and a SQL Server instance named "WIN911" is not found, SQL Server 2014 Express can be installed as part of the installation process. This version of SQL Server is suited for small configurations, up to 5,000 data points, and is best suited for a single-node.

Note: Server 2008 R2 requires SP1 in order to install SQL Server 2014.

## SQL Server not found on node: medium and larger configurations (over 5000 data points)

For medium and larger systems, the following versions are supported:

- Recommended version: SQL Server 2012 SP1, Standard or Enterprise edition

- SQL Server 2014, Standard or Enterprise edition
- SQL Server 2012 SP2, Standard or Enterprise edition
- SQL Server 2008 R2, Standard or Enterprise edition

For more information about the comparative capabilities of different SQL Server editions, see "Features Supported by the Different Versions of SQL Server 2012" at the following URL:

["http://msdn.microsoft.com/en-us/library/cc645993\(v=SQL.110\).aspx"](http://msdn.microsoft.com/en-us/library/cc645993(v=SQL.110).aspx)

### Compatible version of SQL Server already installed

If a compatible version of SQL Server is already installed and an instance named "WIN911" is available on the network or locally, WIN-911 Enterprise Launcher installation will continue without interruption.

### New version of SQL Server already installed

If a new version of SQL Server is already installed that has not yet been fully tested with WIN-911 Enterprise products, a warning is displayed stating that the installed SQL version has not yet been tested. You can proceed with the installation, but we recommend that you contact WIN-911 customer support before proceeding to check if any issues have been found.

### Incompatible version of SQL Server already installed

If an older version of SQL Server is already installed that is not supported for use with WIN-911 Enterprise products, installation will stop and a warning will be displayed stating the SQL Server version is not compatible. You must exit the installation process and upgrade to a supported version of SQL Server before you can resume the installation.

### Install SQL Server Express on remote network computer

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.

## Installation Path

WIN-911 will install files in two locations on your system wwwroot and Program Files (x86). Both locations are special system directories that can be located on any physical or logical drive. The WIN-911 install will honor your OS settings for these directory locations. For most systems these are located at C:\inetpub\wwwroot and C:\Program Files (x86).

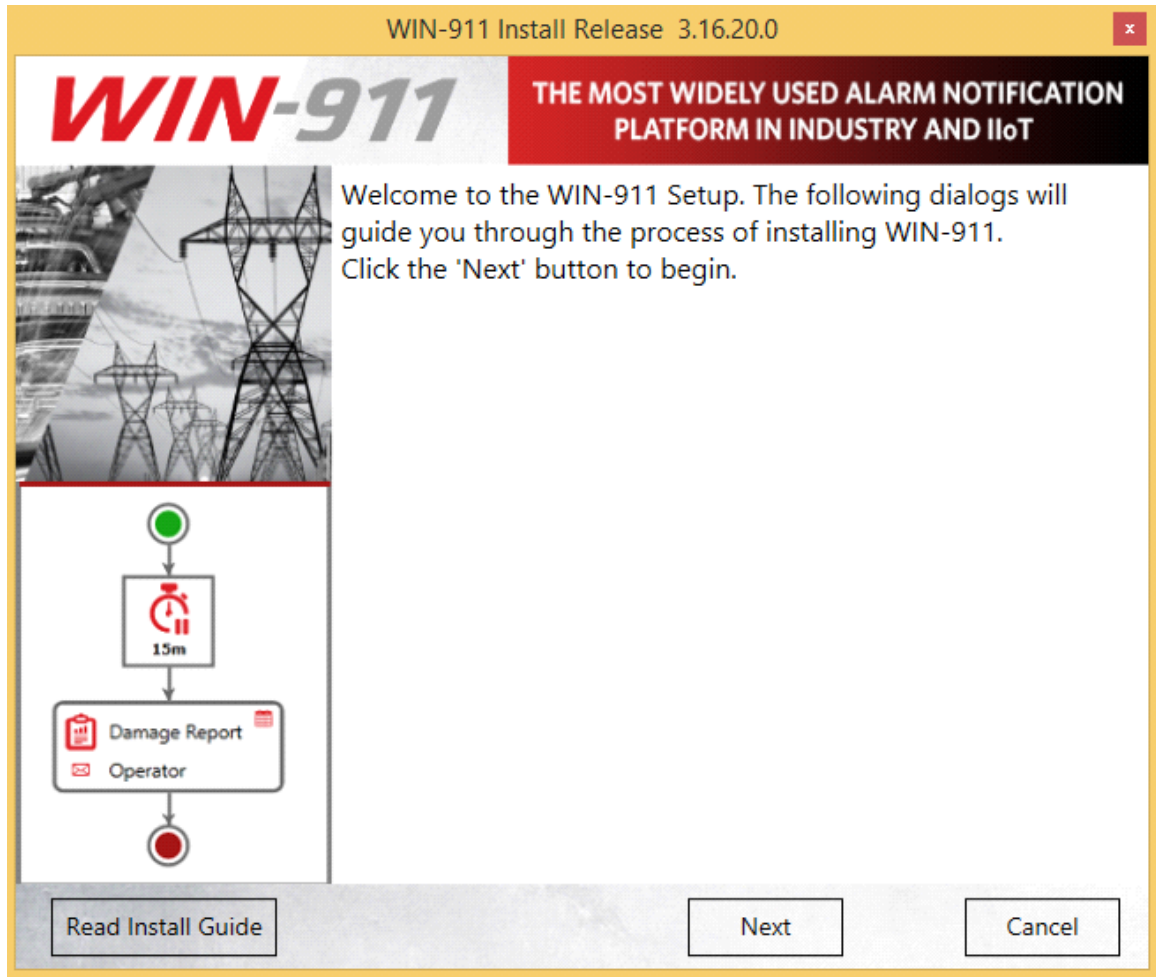
## WIN-911 Enterprise Edition Setup

The WIN-911 Enterprise 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 subfolder of the installation media or online.

To install WIN-911 Enterprise Edition

Insert the flash drive into your USB port. The install program automatically runs. If your network security policy does not permit autorun, browse to the root of your install drive and run *WIN-911 Enterprise launcher.exe*.





Click **“Next”** to begin WIN-911 Setup.

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

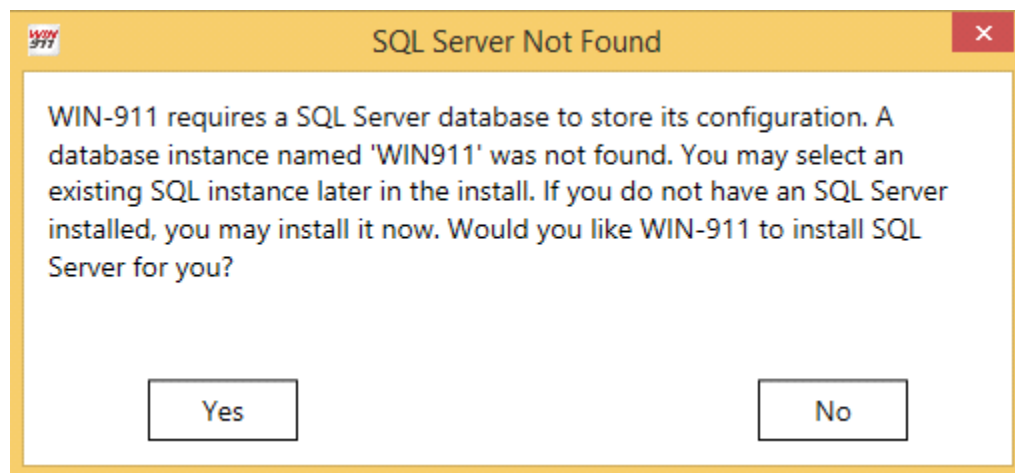
## SQL Server Installation

WIN-911 Enterprise Edition uses a SQL Server database to store its configuration data. The SQL Server requirements can be satisfied in one of the following ways:

- 1) A pre-existing local SQL Server.
- 2) A pre-existing remote SQL Server located on the WIN-911 network (Active Directory only).

3) Have the WIN-911 Enterprise Launcher install SQL Server 2014 Express on the host computer.

The install script will check the WIN-911 host for a SQL Server instance named "WIN911". If one is not found on the host, the install will next browse the network. In order for the SQL browser to search for a suitable server the SQL Server Browser service must be enabled and started (Server OS's have this disabled by default). You will also need Network Discovery enabled. If there is no suitable SQL Server visible 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.

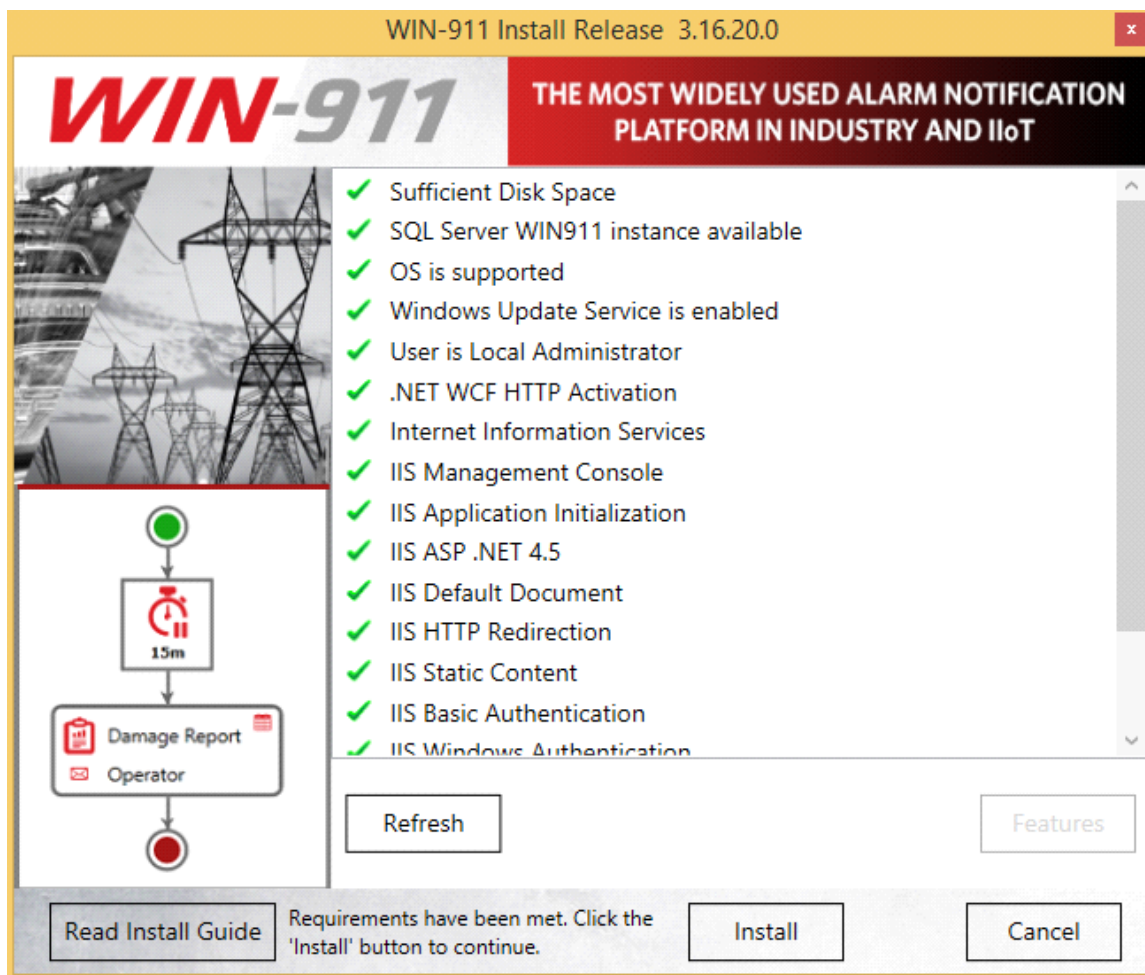
*Note: if you are upgrading, you should select "No" to keep your existing data.*

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

If the install script finds a suitable SQL Server the above message will not appear.

## Requisite Programs and Features



The install will conduct an inspection of your operating system and demand the presence of all required programs and features before proceeding. Any missing features will be delineated in the list above. You can proceed with the install if the SQL Server instance is not satisfied if you wish to use a custom SQL instance (not named "WIN911"). All other features must be satisfied before proceeding.

Note: Upgrading users will require an updated license before installing. See below: "Upgrading to WIN-911 Enterprise 3.16.9+"

System requirements include the following:

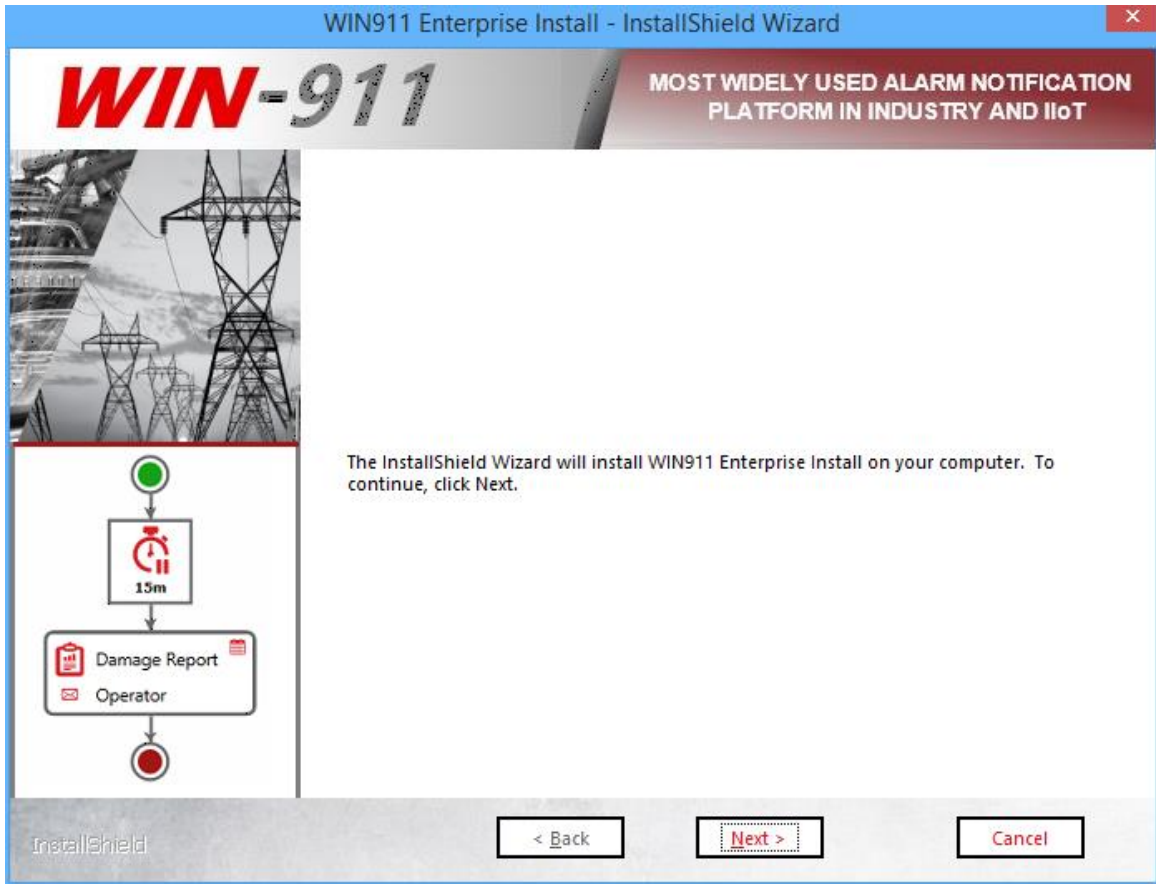
- Microsoft .NET 4.5
- Windows Edition and Feature Set Detection
- WIBU CodeMeter Control Center
- SQL Server
- IIS Features: Application Initialization, Basic Authentication, Windows Authentication, HTTP Redirection and ASP.NET 4.5, HTTP Activation

Use the **"Features"** button to launch the **"Windows Features and Roles"** configuration workspace to add any missing components. Then use the **"Refresh"** button to re-scan for missing features.

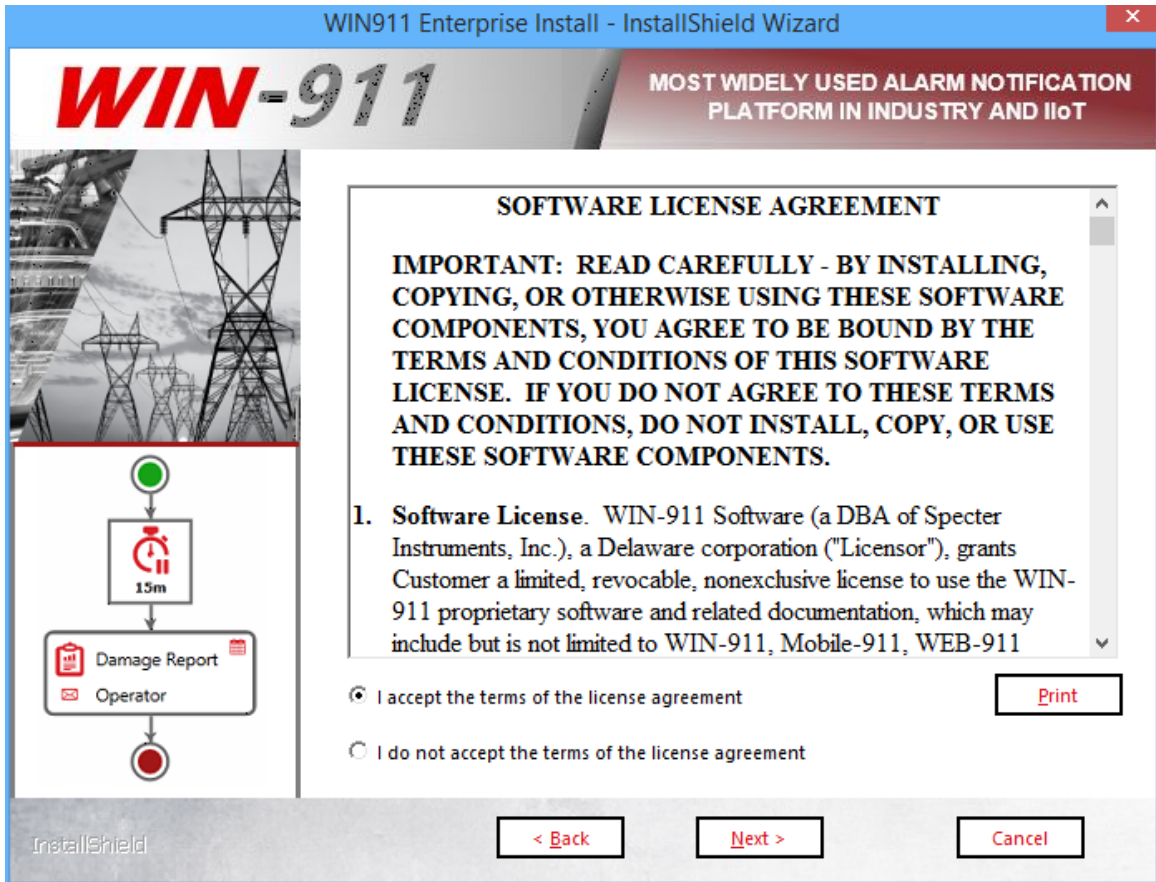
Once all requirements are satisfied, click **"Install"** to continue.

## InstallShield Wizard

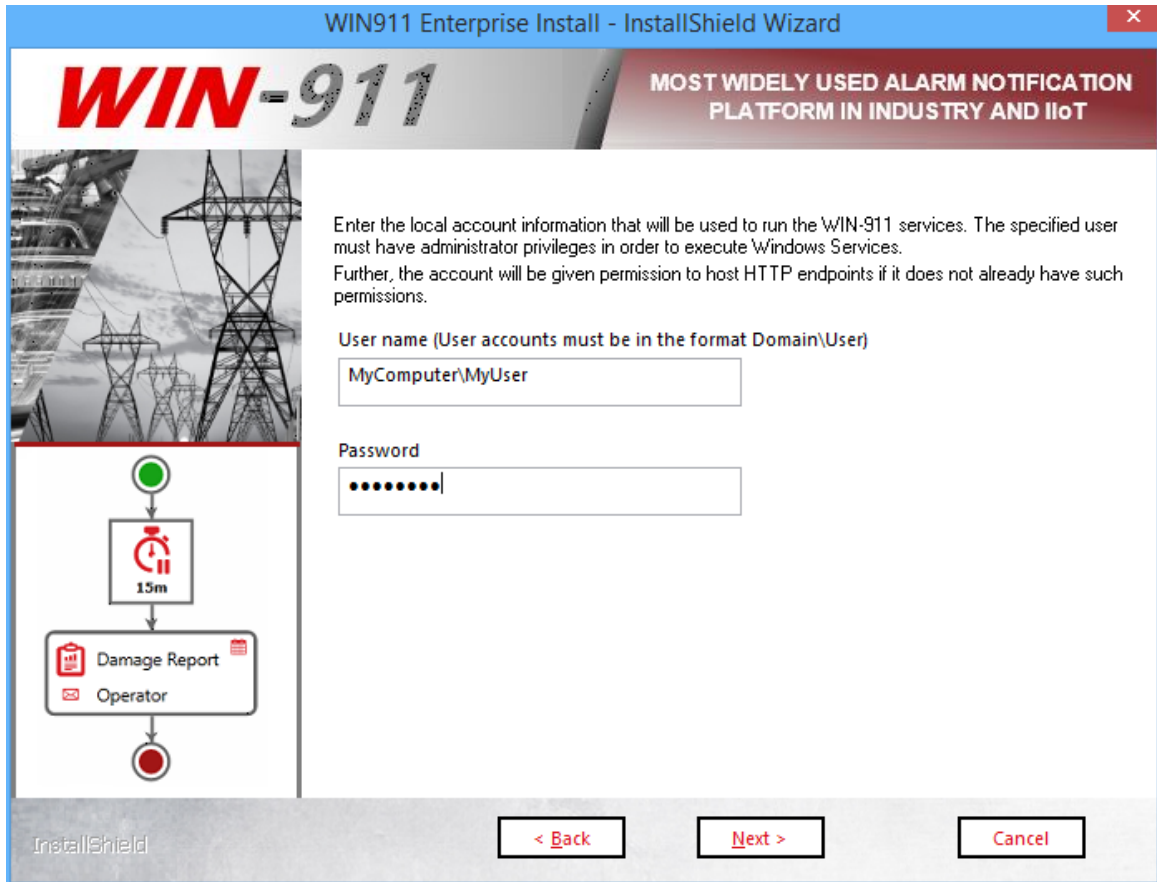
*Note: In order to upgrade WIN-911 Enterprise from a version prior to 2.16.1, you must first upgrade your license and have your support number ready to enter before proceeding with the install. Please contact WIN-911 Software at 1-800-331-8740.*



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

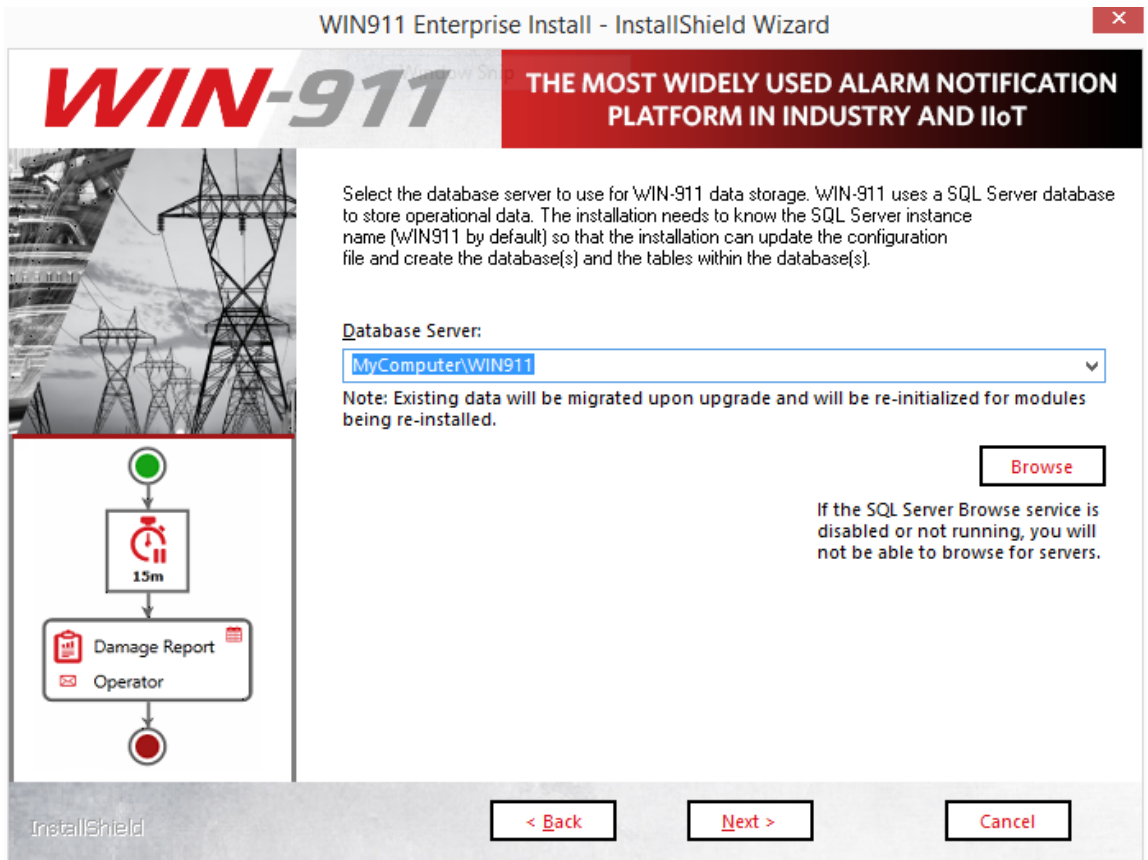


Accept the terms of the Software License Agreement by clicking the top radio button and then select "Next" to advance.



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. 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.**

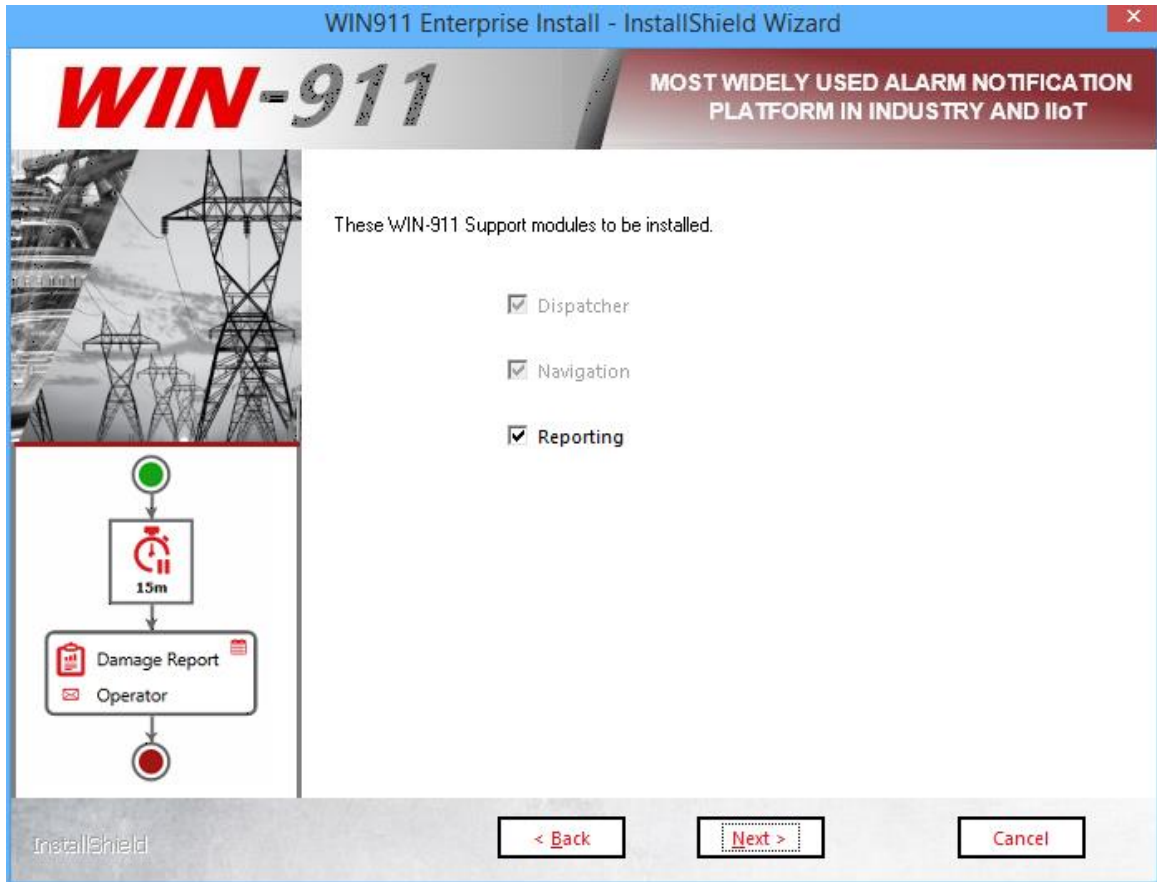
*Note: You must be logged in and executing this installation as an owner and administrator of the SQL instance. Additionally, the selected user here (if different) must be a member of the Windows local or domain administrator group with administrative privileges on the SQL instance.*



In this step the installation looks for a SQL Server instance called "WIN911". It is important to note that the instance does not have to be on the WIN-911 host. If you wish to use a non-local server instance you will have to specify the correct host name. 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 text entry field.

Click "Next" to advance.

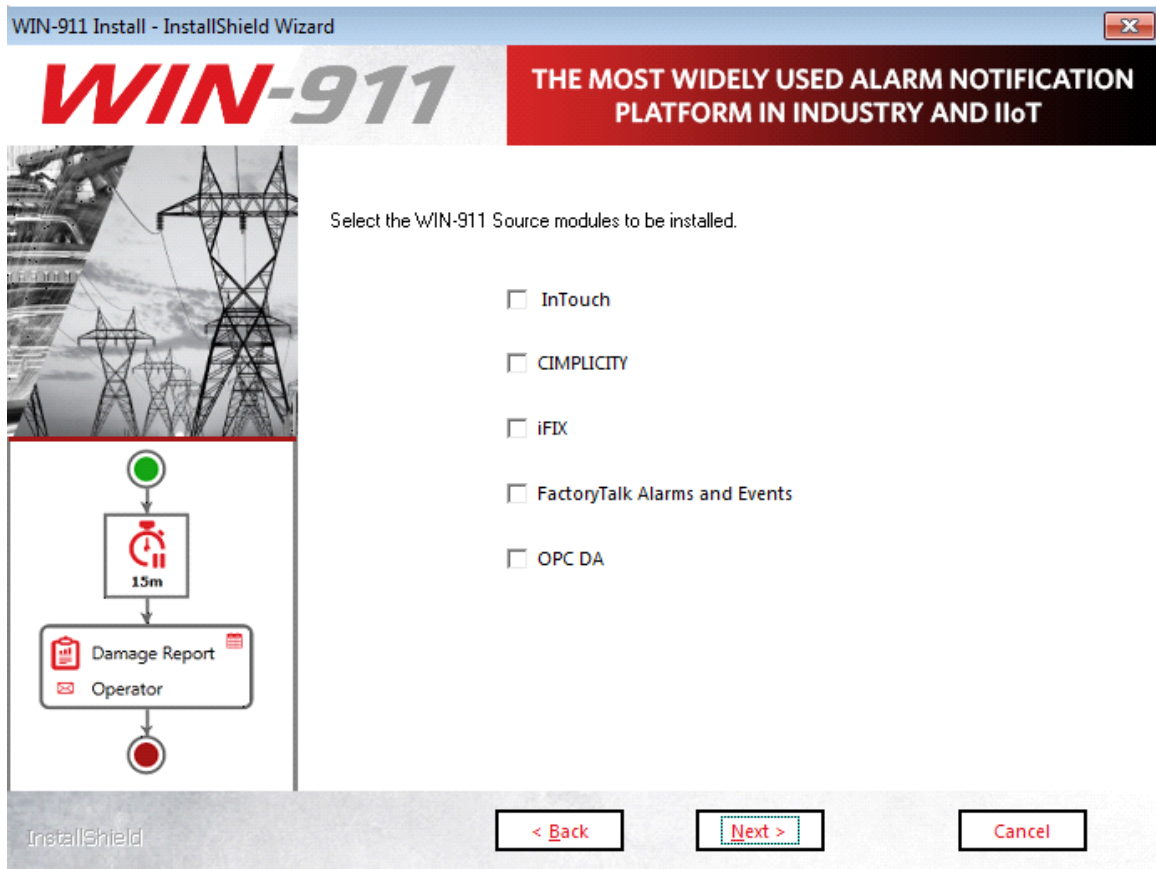




The support module selection menu allows you to choose which components of WIN-911 Enterprise Edition you install. As a general rule, all support features should be installed.

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

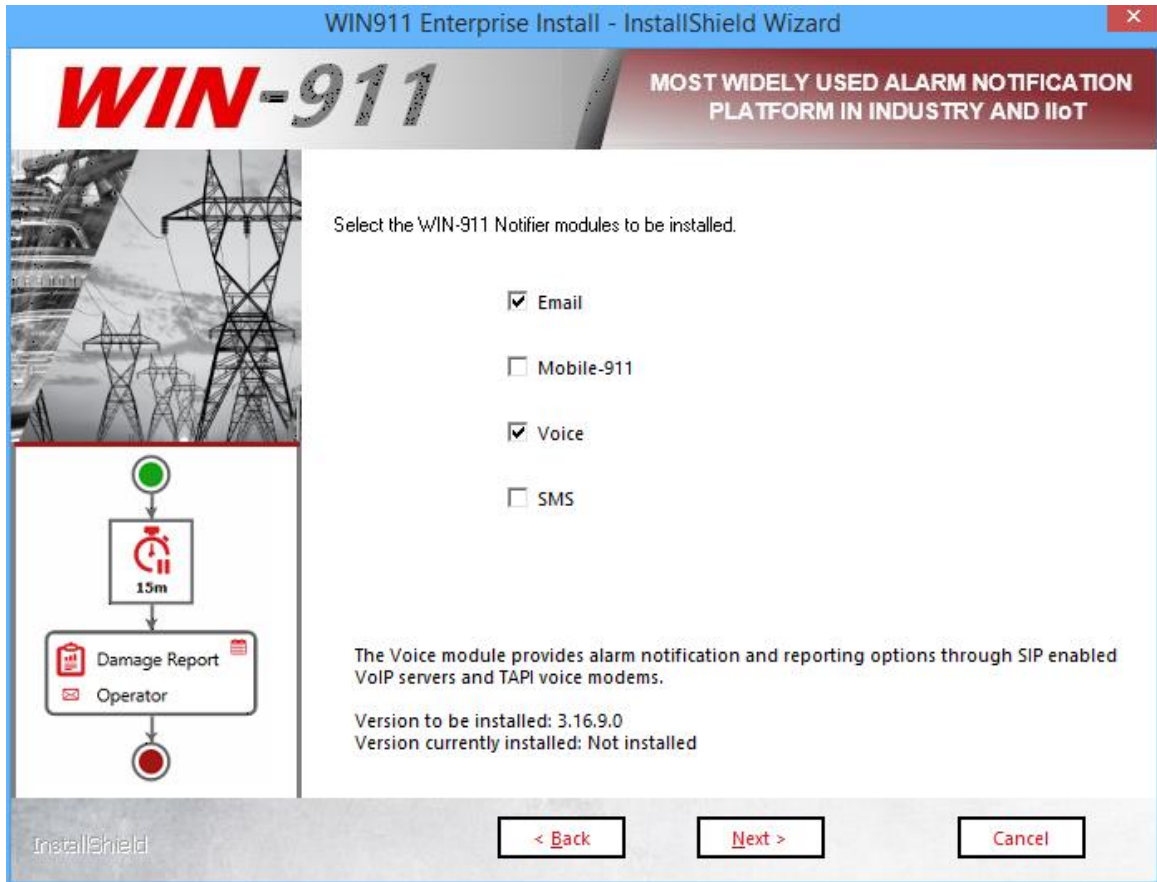
Click "Next" to advance.



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 Enterprise Edition you install. In order to avoid nuisance alarms you should install only the source modules you intend to use. You can always add features later that are not originally installed by re-running the setup.

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

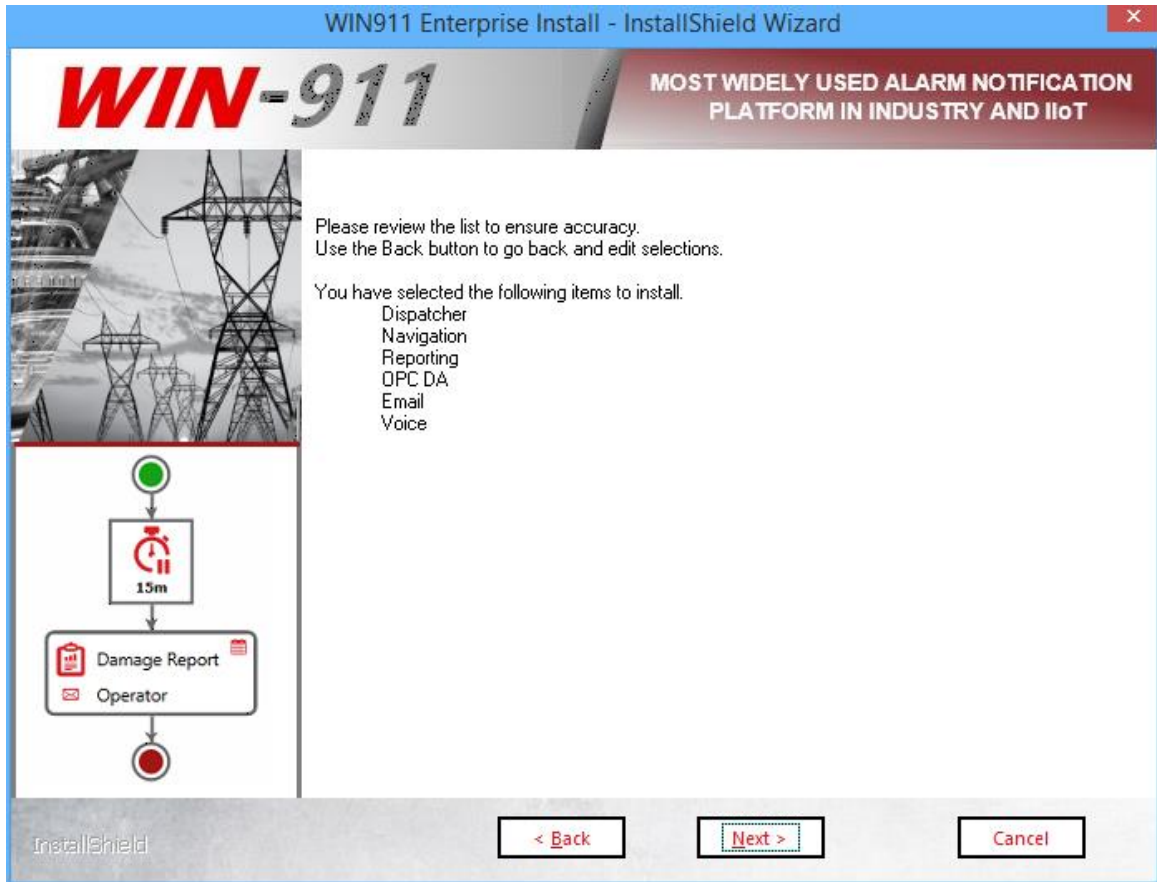
Click "Next" to advance.



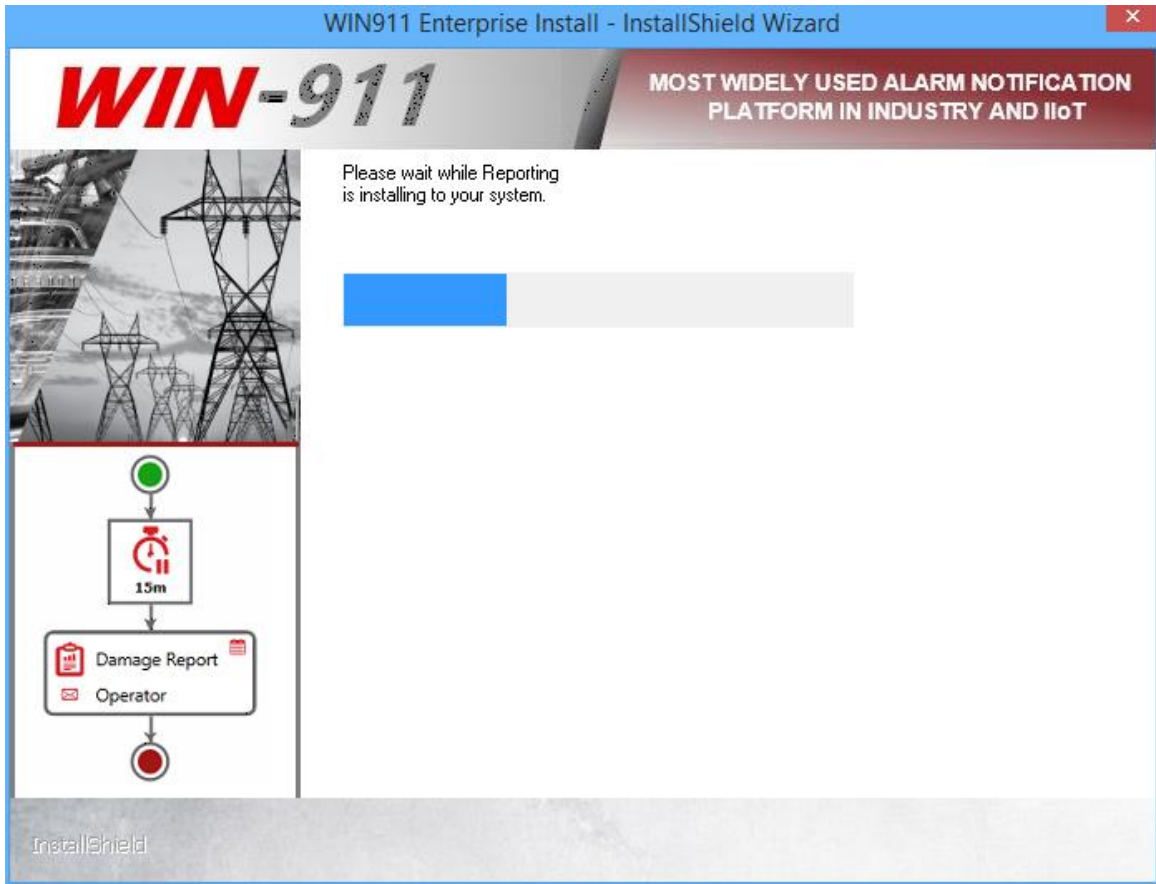
WIN-911 provides several methods of remote notification to the users, including Email, Mobile-911, Voice, and SMS. The notifier module selection menu allows you to choose which components of WIN-911 Enterprise you install. Again, you should install only the notifier modules you intend to avoid errors. You can re-run the setup program to add features that are not originally installed.

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

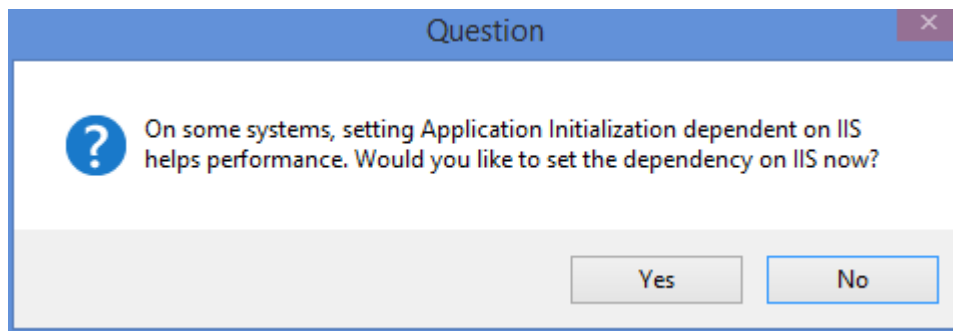
Click "Next" to advance.



This page presents the manifest of selected modules to be installed. Please review and click the *Back* button to change the list or *Next* to begin the installation and initialization phase of the setup.



This portion of the install may take several minutes, especially for the dispatcher module.




If you are installing on a system that does not have application initialization pre-loaded (Windows 7 and Server 2008 R2 do not), click Yes.

WIN911 Enterprise Install - InstallShield Wizard

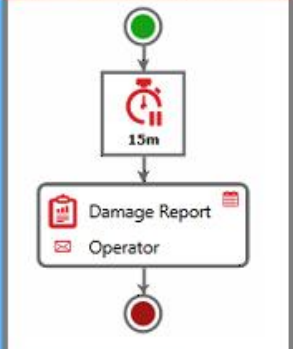
# WIN-911

MOST WIDELY USED ALARM NOTIFICATION PLATFORM IN INDUSTRY AND IIoT



**Setup Complete**

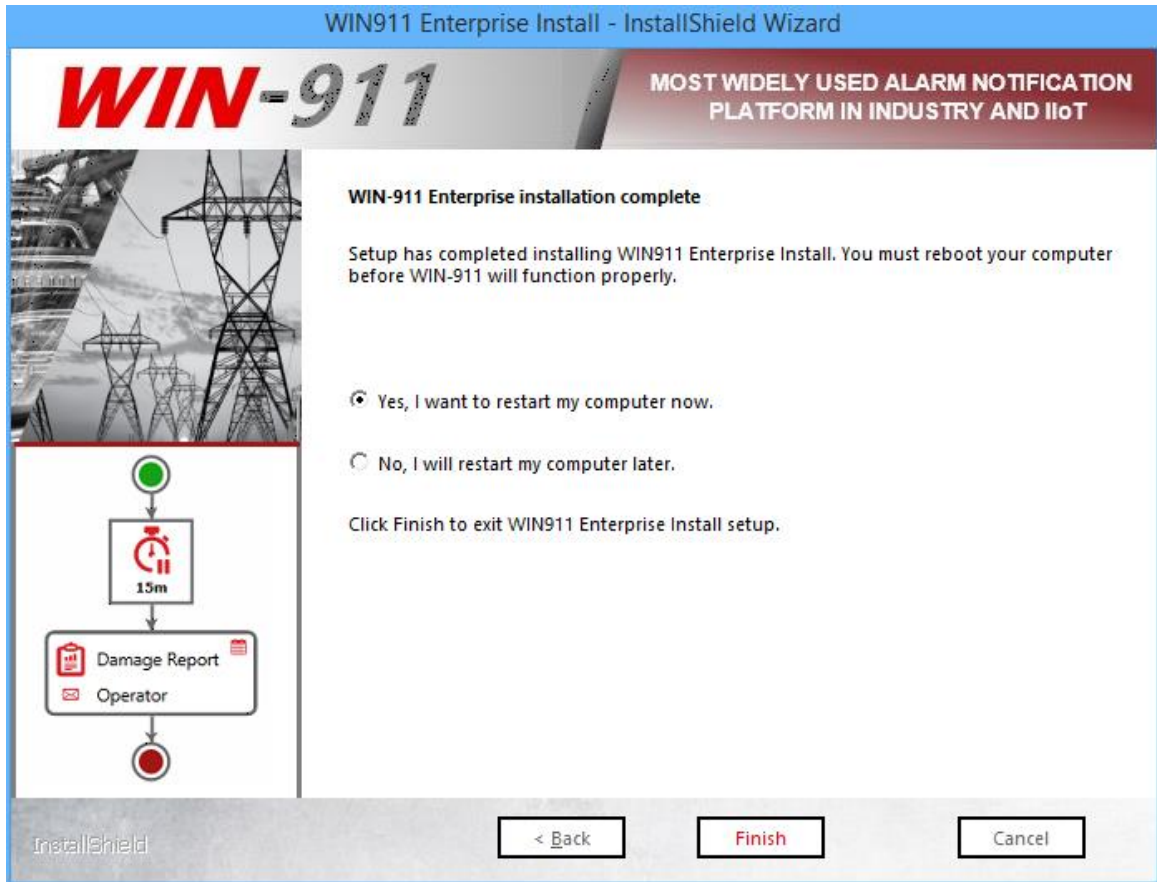
Setup has successfully installed WIN911 Enterprise Install. Click Finish to exit.



InstallShield

< Back    Finish    Cancel

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 Enterprise Edition

### Adding features to your existing WIN-911 installation

Run the WIN-911 Enterprise 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. Tick 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 module 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.

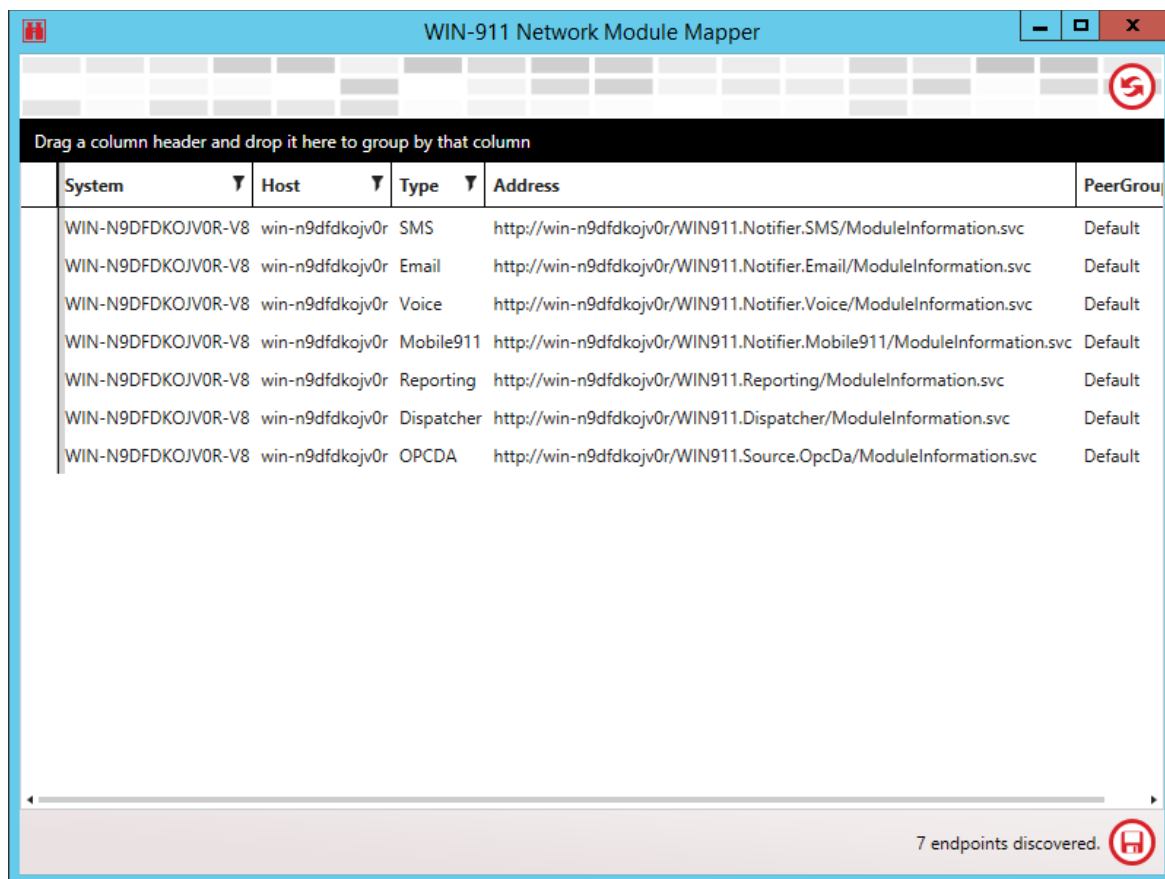
See the WIN-911 Endpoint Mapper below for more information on this step.

## Uninstalling WIN-911 Enterprise Edition

WIN-911 can be uninstalled via *Control Panel\Programs and Features*. Each module will have to be uninstalled individually. Right-click the WIN-911 module and select Uninstall. Repeat this process until all WIN-911 modules have been removed.



## WIN-911 Endpoint Mapper



System	Host	Type	Address	PeerGroup
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	SMS	http://win-n9dfdkojv0r/WIN911.Notifier.SMS/ModuleInformation.svc	Default
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	Email	http://win-n9dfdkojv0r/WIN911.Notifier.Email/ModuleInformation.svc	Default
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	Voice	http://win-n9dfdkojv0r/WIN911.Notifier.Voice/ModuleInformation.svc	Default
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	Mobile911	http://win-n9dfdkojv0r/WIN911.Notifier.Mobile911/ModuleInformation.svc	Default
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	Reporting	http://win-n9dfdkojv0r/WIN911.Reporting/ModuleInformation.svc	Default
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	Dispatcher	http://win-n9dfdkojv0r/WIN911.Dispatcher/ModuleInformation.svc	Default
WIN-N9DFDKOJV0R-V8	win-n9dfdkojv0r	OPCDA	http://win-n9dfdkojv0r/WIN911.Source.OpcDa/ModuleInformation.svc	Default

Whenever you modify your WIN-911 system by uninstalling software modules you will need to run the endpoint mapper. The mapping process might take several minutes to appear and may need to be refreshed if the proper number of endpoints are not listed. This is normal so allow for extra time during the post modification reboot.

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

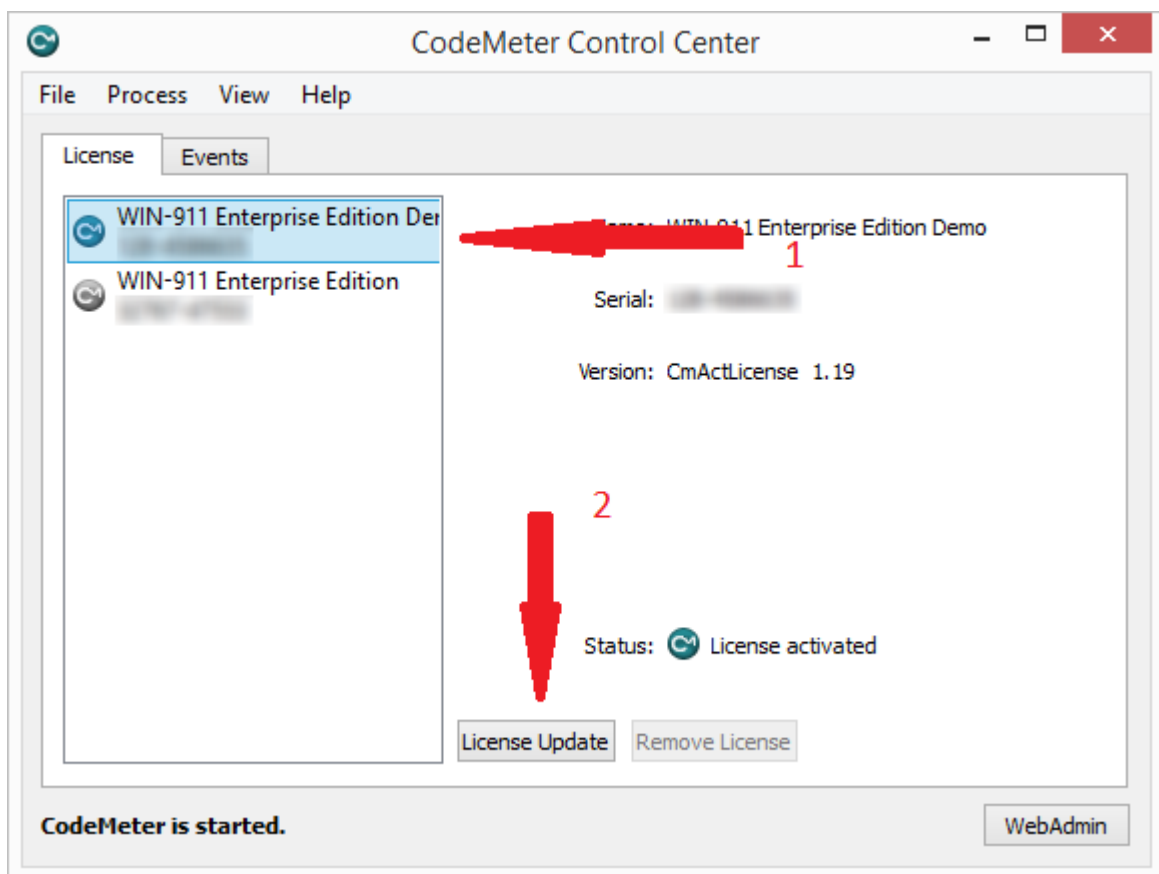
Once the proper number endpoints are listed in the mapper click the save button. This will conclude this portion of the install. **You should not need to run the WIN-911 Endpoint Mapper again** unless you remove certain features included in the initial install.

## Licensing WIN-911 Enterprise Edition

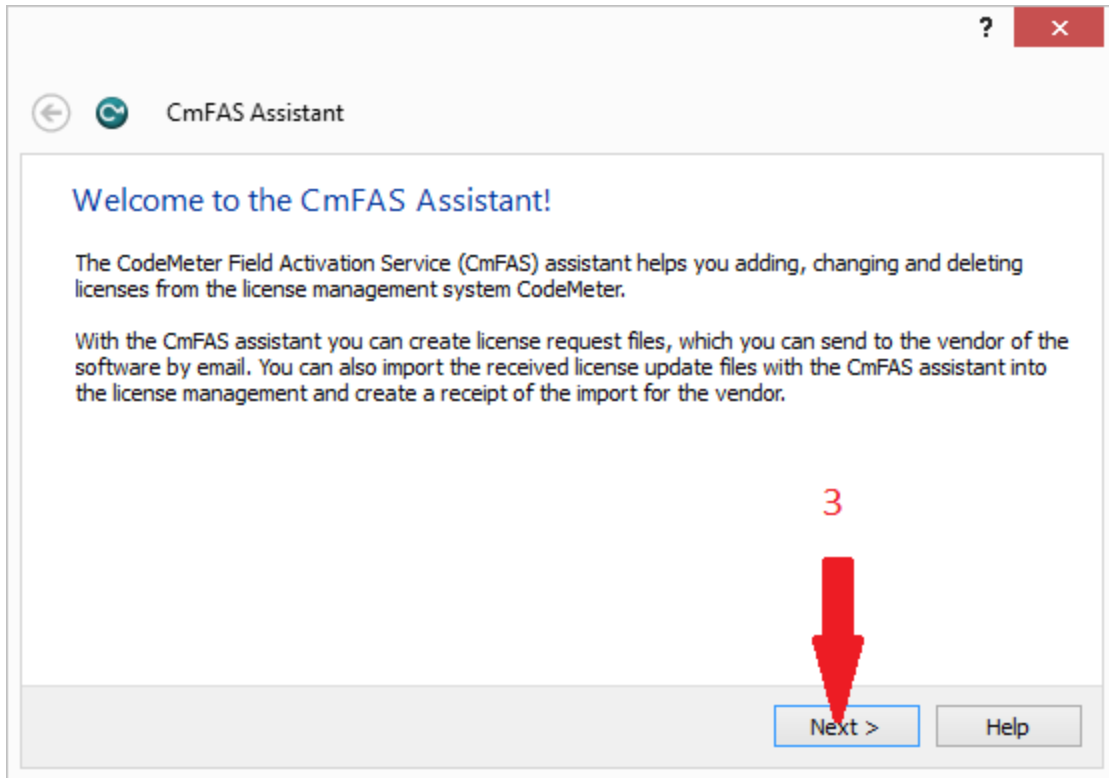
*Note: After an initial installation WIN-911 Enterprise will be configured with a demo license that will run 30 days without restriction.*

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

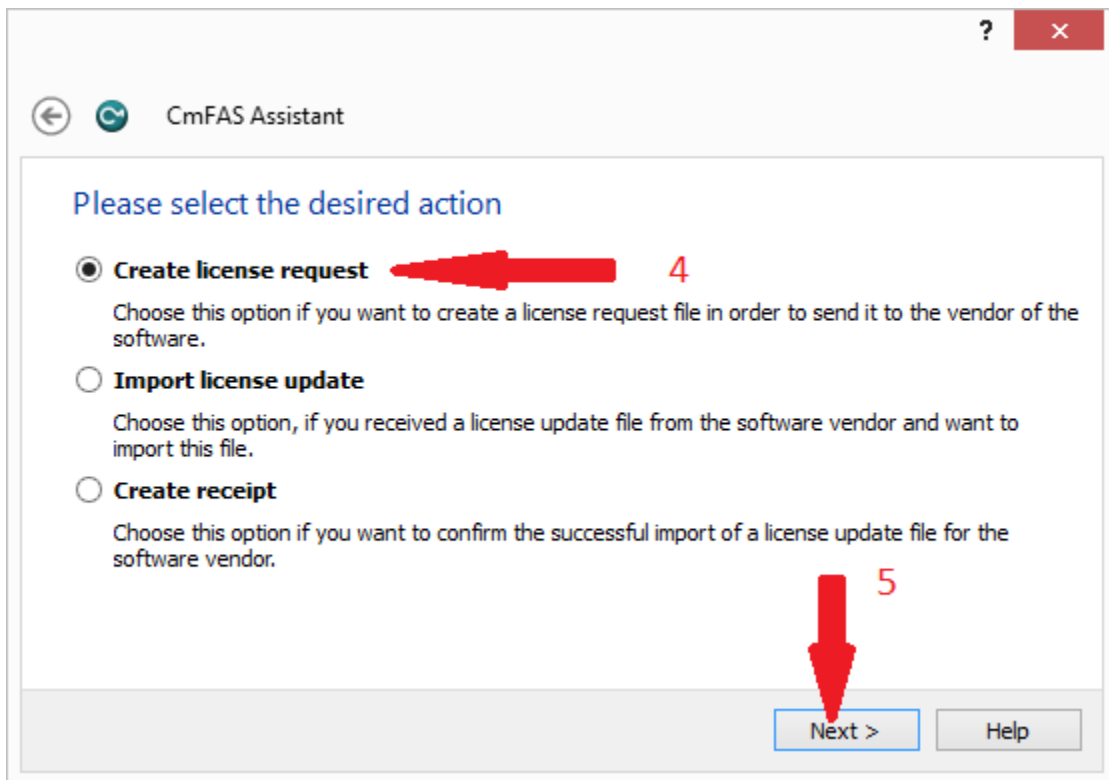
Click the "License Update" button and follow the wizard to generate a license request file.



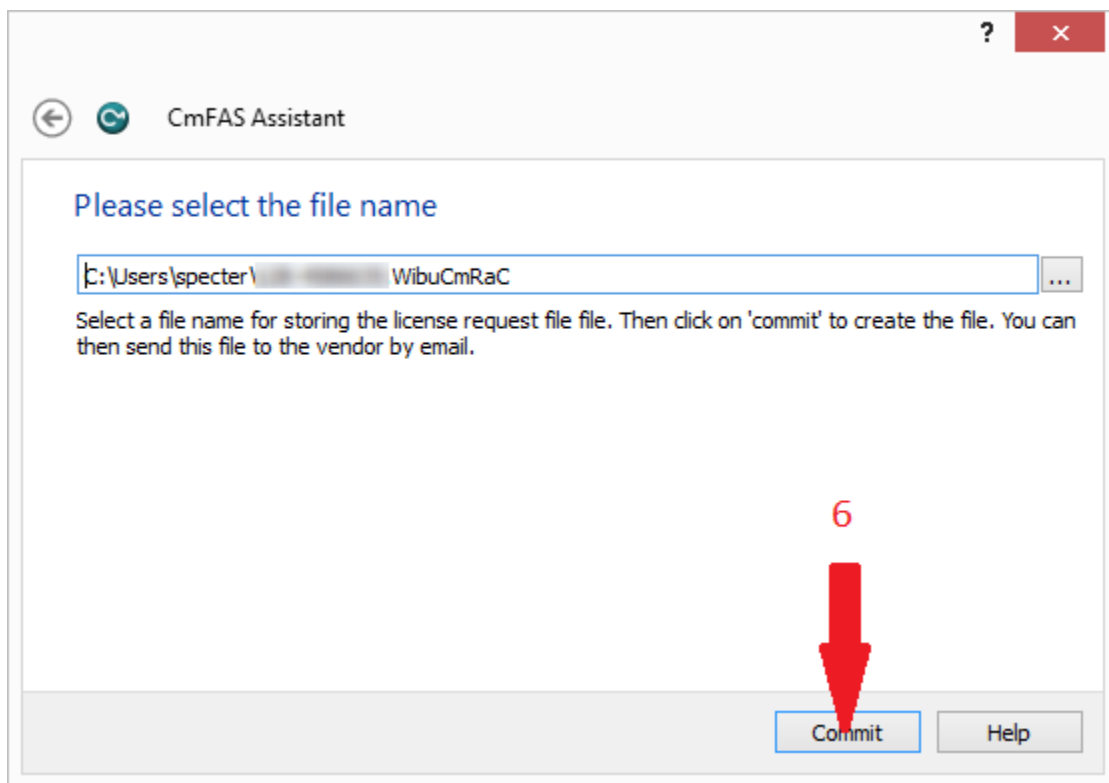
Select the container with the active license (1). The Status indication will verify "License activated". Then click License Update (2).



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



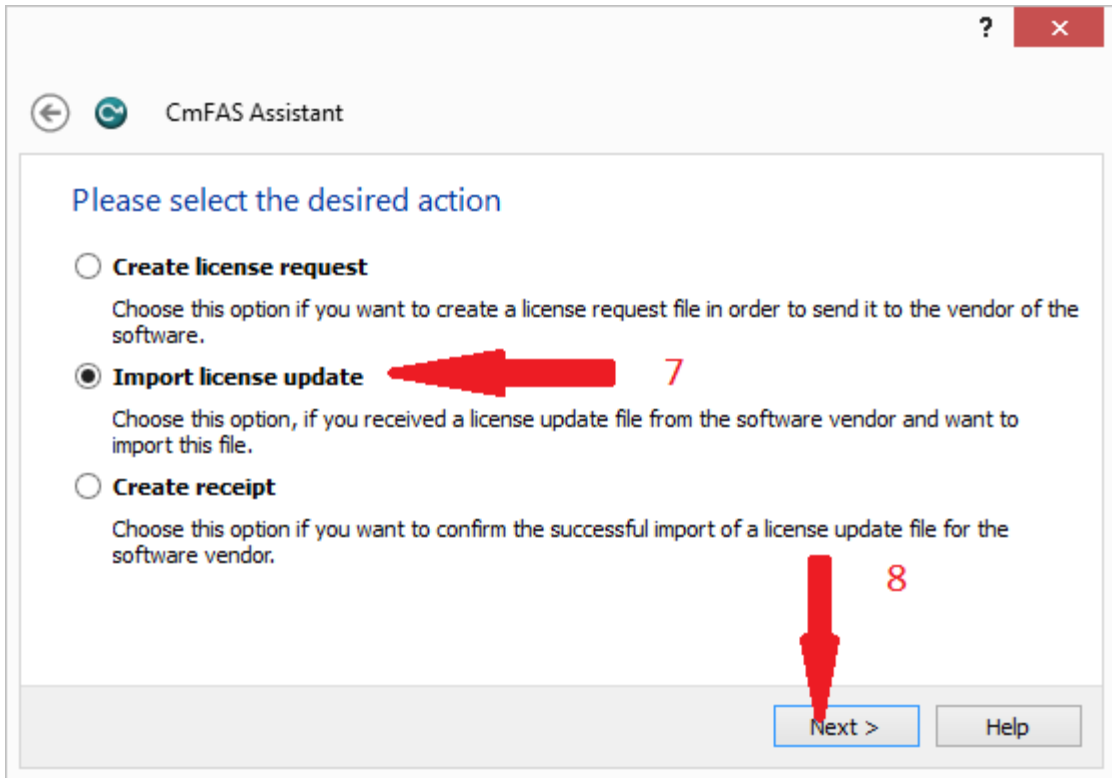
Select the Create license request (4) option and then click Next > (5)...



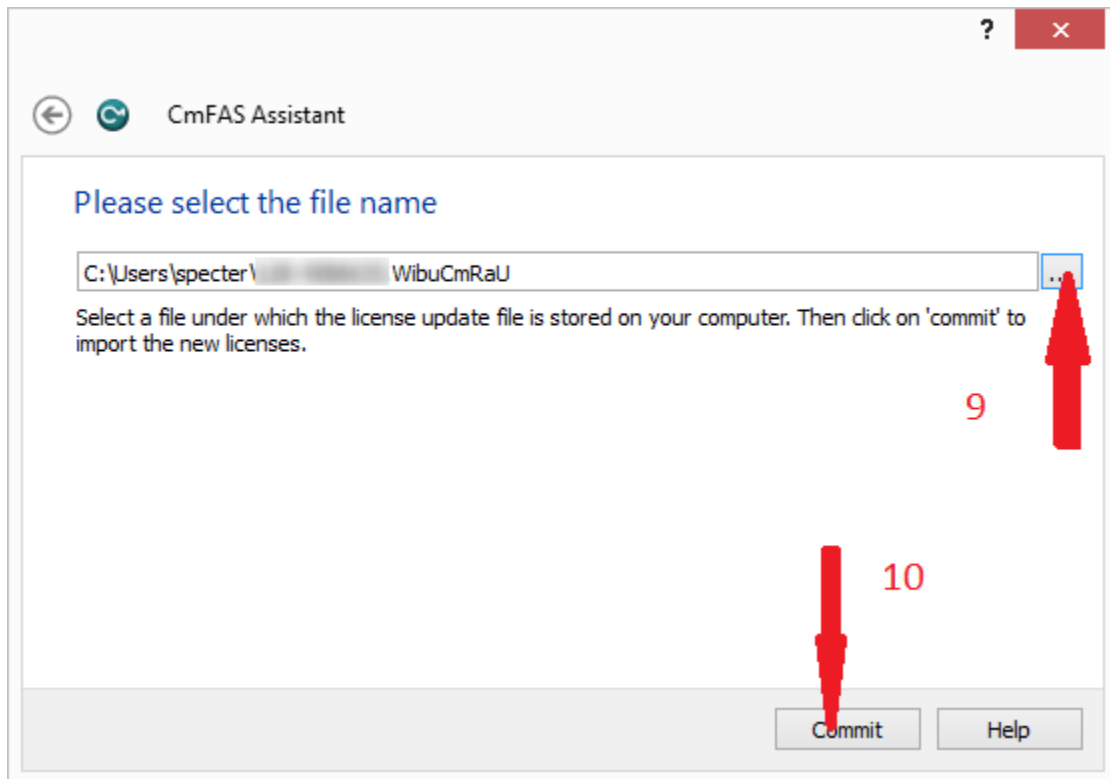
Note the location of the license request and then click Commit (6).

Email the license request file to <mailto:license@win911.com> or submit via website.

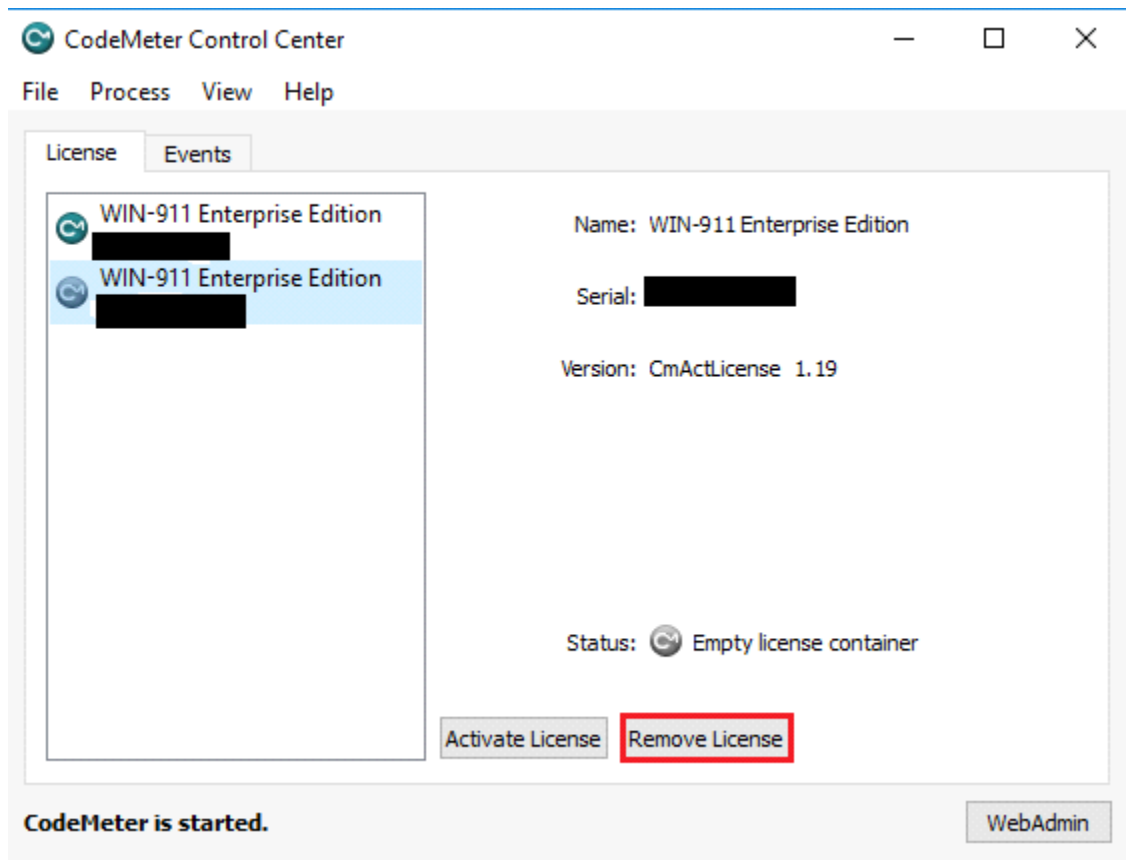
Upon receipt of the license file save to desktop. Return to the CmFAS Assistant and select Import license update (7) and then click Next > (8)...



Browse to the license file (9) and select Commit (10).



Remove the Demo license by highlighting it and clicking "Remove License".  
Click "Activate License" to complete the process.



## Upgrading to WIN-911 Enterprise 3.16.9+

WIN-911 Enterprise v.3.16.9 introduces a new licensing schema that is incompatible with licenses issued for previous versions. If you have installed and licensed a previous version of WIN-911, you will need to request a new license before you can install 3.16.20 and subsequent releases.

## Affected Versions


WIN-911 Enterprise v.1.14.2, v.1.14.5, v.2.15.1, and v.2.15.6

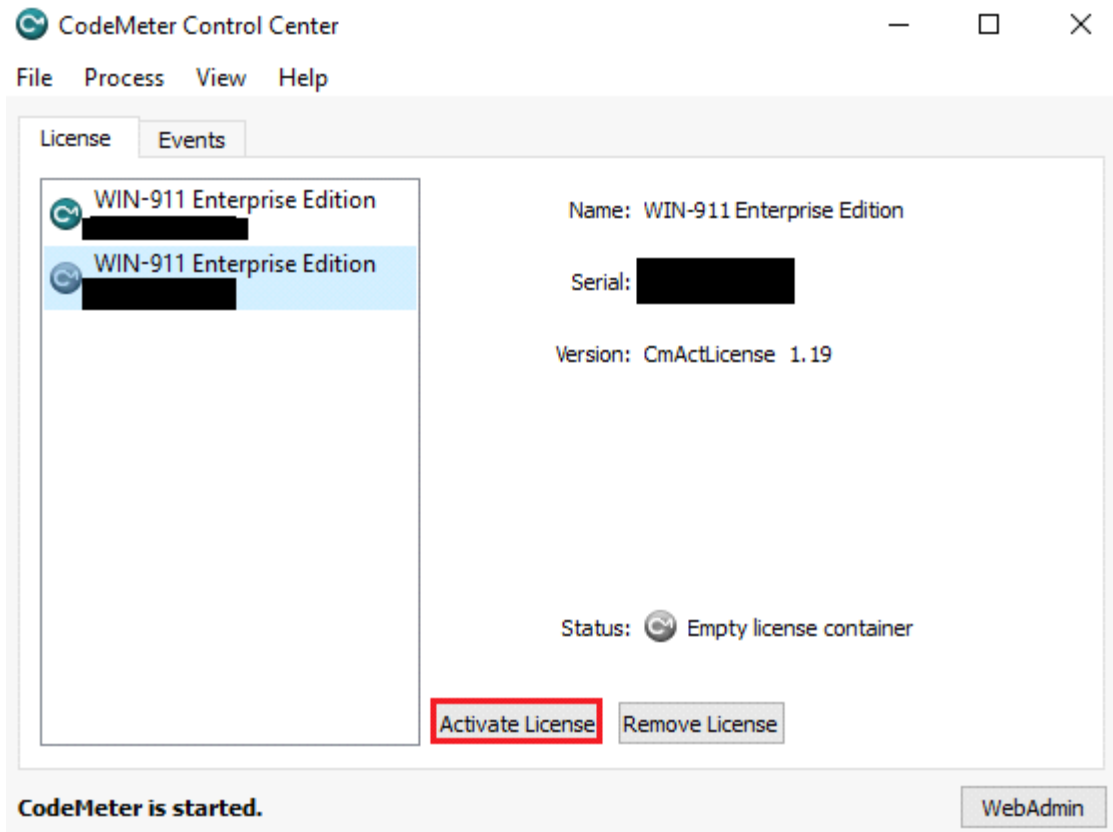
## Re-licensing

### Requesting a New License for WIN-911 Enterprise w/ FactoryTalk Alarms and Events

**ONLY** follow these directions if you have purchased WIN-911 with the FactoryTalk Alarms and Events connection. If you're unsure whether your license contains FactoryTalk, please contact our Sales department via phone at **1-800-331-8740** or email at [sales@win911.com](mailto:sales@win911.com). If you did not purchase WIN-911 Enterprise with the FactoryTalk Alarms and Events connection, jump to **Requesting a New License for WIN-911 Enterprise**.

**\*\*NOTE\*\*** WIN-911 Software will only respond to license request during normal business hours, Monday - Friday 8 AM - 5 PM Central Time Zone (UTC-06:00). If you remove your license in order to upgrade WIN-911 Enterprise w/ FTAE, WIN-911 will not be functional until you receive a new license.

1. Open CodeMeter by double clicking on the  icon on your system tray.
2. Select your demo license container on the left side of the CodeMeter Control Center window and then select **Remove License**.
3. We now need to generate a new license file, to do this you must download a tool which will generate the license for you, you can download the tool from here. [\[Download License Tool\]](#)
4. Extract the ZIP file on your computer and run Generate License.bat. This will generate a new license file in CodeMeter.
5. Go back to CodeMeter and select your new license container on the left side of the CodeMeter Control Center window and the select **Activate License**.




- The CmFAS Assistant wizard will appear. Select **Next >**
- Select **Create license request** and select **Next >**
- Choose where you would like to save the license request file and select **Commit**.
- Your license request file will be generated. Select **Finish** to close the wizard.
- Upload your license request file to [our licensing page](#). You will need to enter your WIN-911 Enterprise Serial Number so have it ready.
- Once we receive your license request we will create a new license and send it back to you as soon as possible. We can only respond to license requests Monday - Friday 8 AM - 5 PM CST.

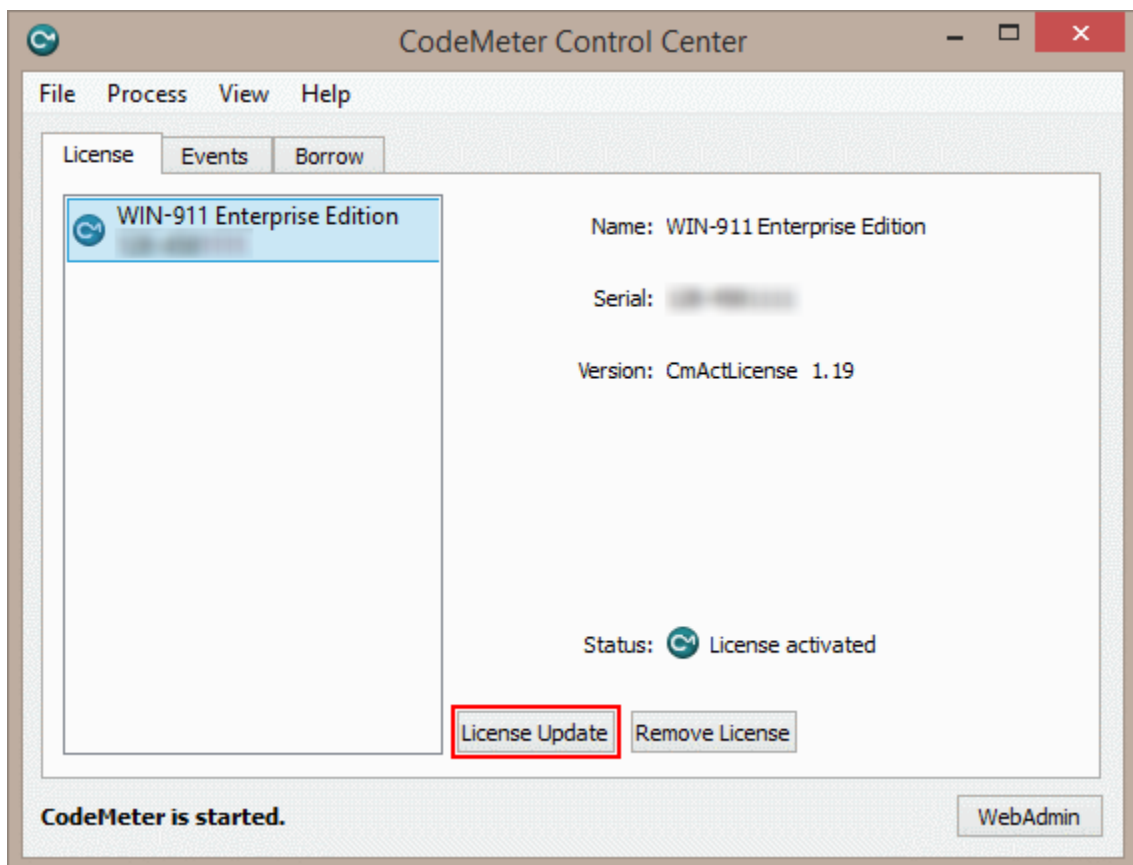


## Requesting a New License for WIN-911 Enterprise

**Only** follow these directions if you have purchased WIN-911 WITHOUT the FactoryTalk Alarm and Events connection.

**Note:** If you have installed a version of WIN-911 Enterprise previous to and it was never licensed, you will need to contact us to request a new demo license before installing v.3.16.20.

- Open CodeMeter by double clicking on the  icon on your system tray.
- Select your license container on the left side of the CodeMeter Control Center window and then select License Update.

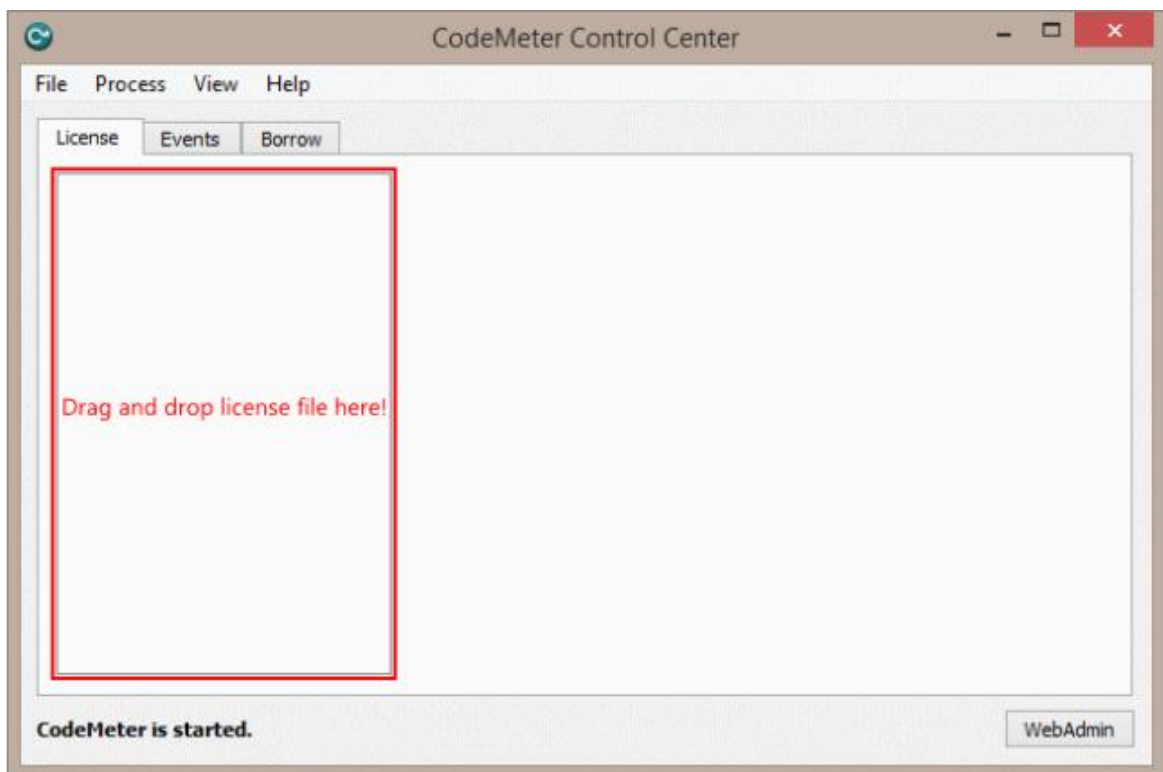


- The CmFAS Assistant wizard will appear. Select Next >
- Select Create license request and select Next >.

- Choose where you would like to save the license request file and select Commit.
- Your license request file will be generated. Select **Finish** to close the wizard.
- Upload your license request file to [our licensing page](#). You will need to enter your WIN-911 Enterprise Serial Number so have it ready.
- Once we receive your license request we will create a new license and send it back to you as soon as possible. We can only respond to license requests Monday - Friday 8 AM - 5 PM CST.

## Install Upgrade License

- Once you receive your new license file you can import it into CodeMeter.
- Open CodeMeter Control Center. Find your new license file and drag it onto the box on the left side of the **License tab**



Your new license is installed and you can now install WIN-911 Enterprise 3.16.20 and newer versions

# 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.

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 must be notified about. Let's walk through each of these items.

## Configure a Notification Method

### Gateways

It is considered a best practice to configure any new installation by starting on the Notifier 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. It is titled 'WIN-911 Configuration'. 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.

WIN-911™ **Contact** Notification Alarming Reporting System ?  
Email Mobile-911 SMS Voice Roles Schedules  
Gateway Connections Formats

Outgoing Server Incoming Server

Type SMTP

Host smtp.mycompany.com

Use TLS/SSL



Port 587

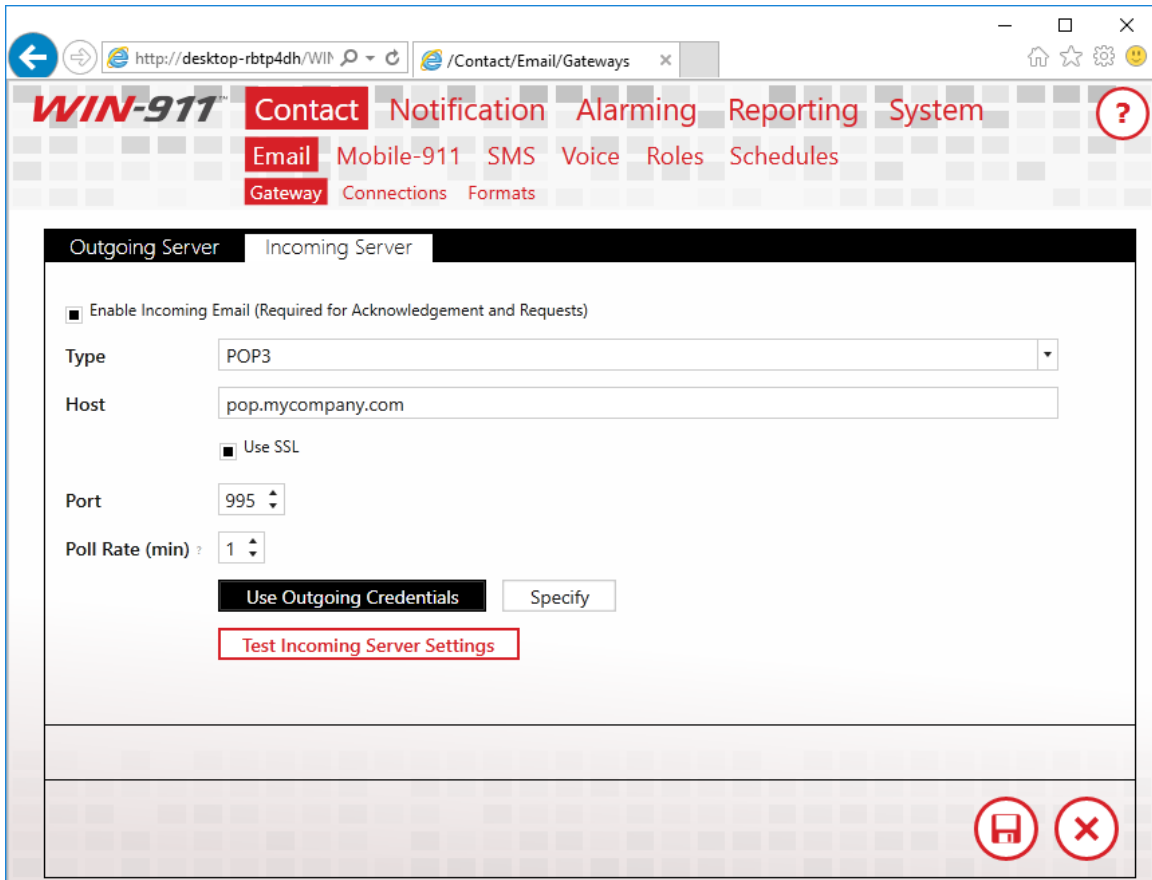
Email Address ? win911@mycompany.com

Username win911@mycompany.com

Password ●●●●●●●●

**Test Outgoing Server Settings**

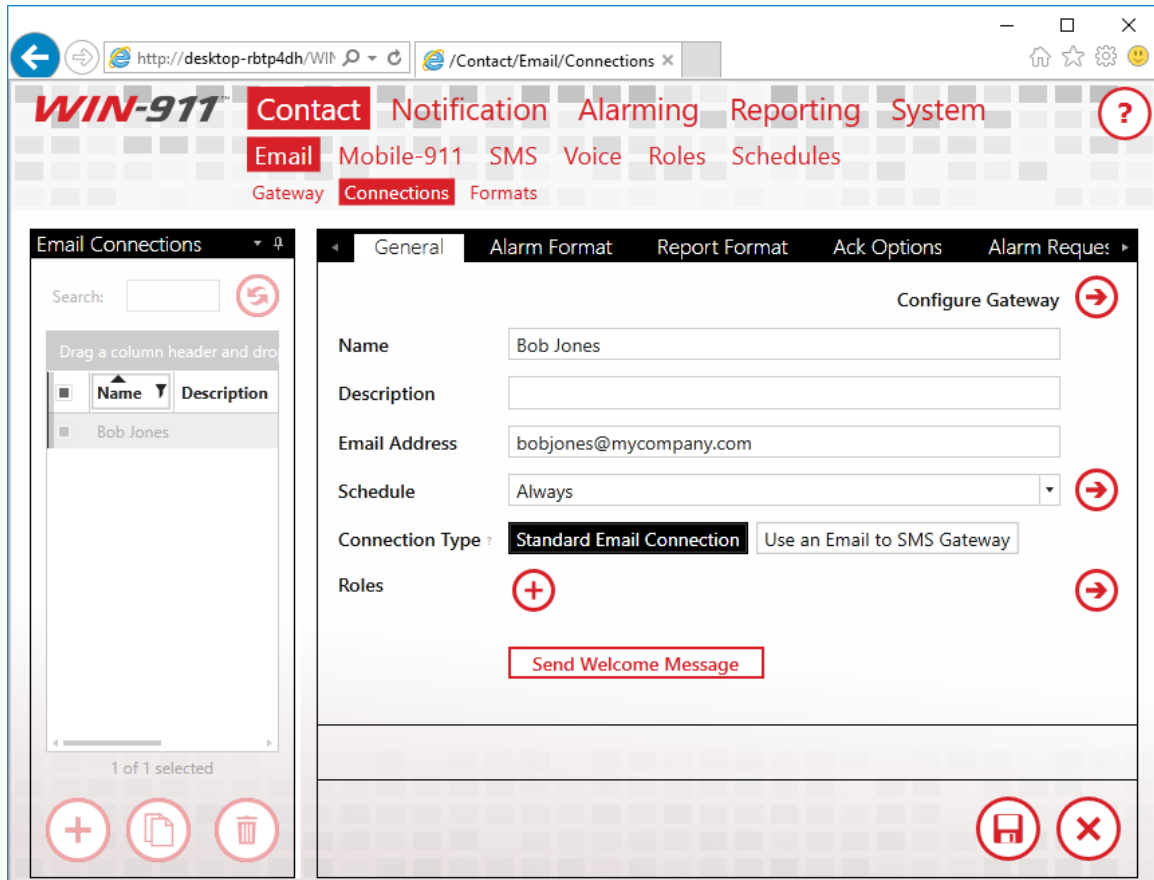
 



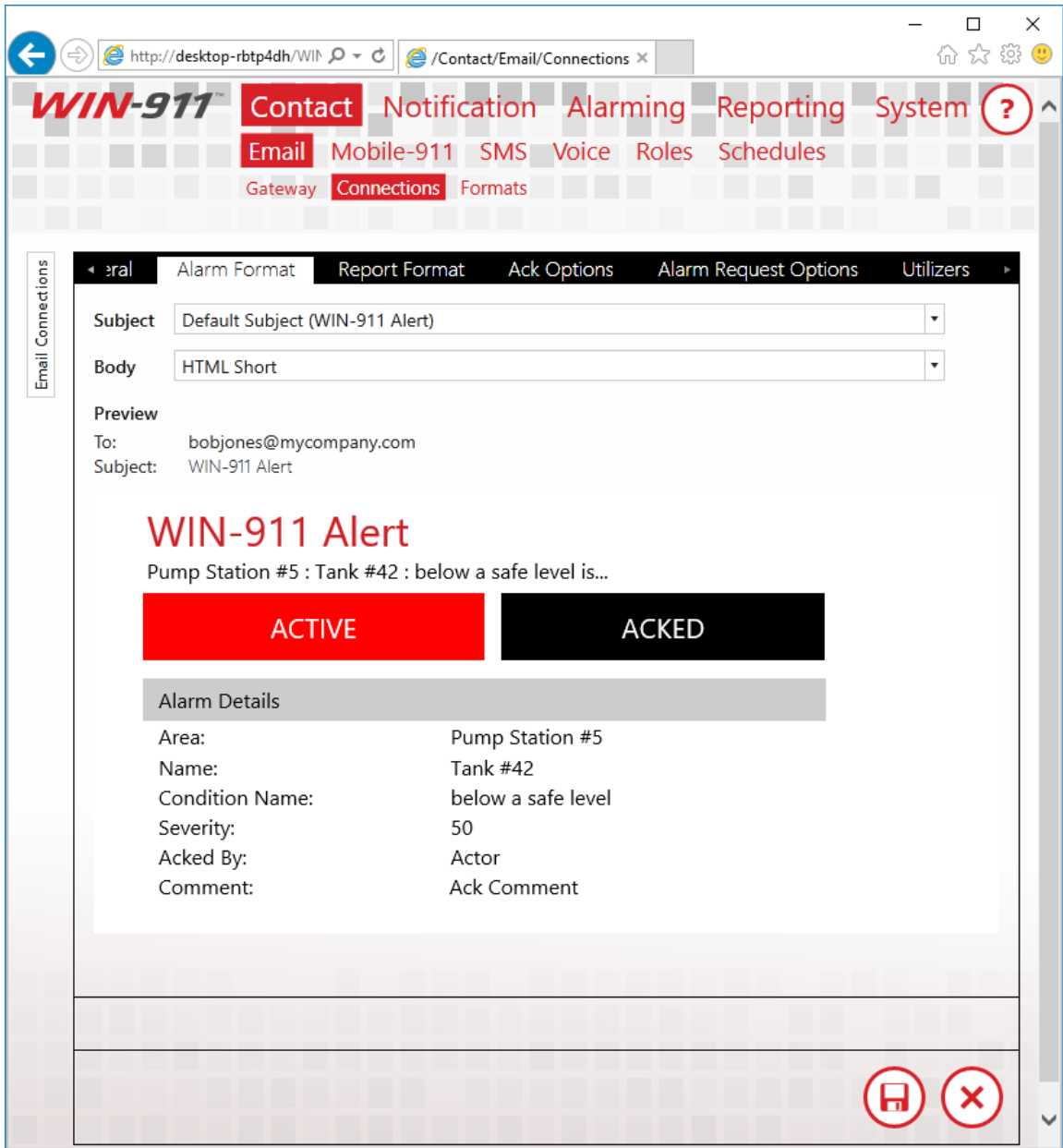
There are two configuration items worth bringing to light here. The first is, in order to connect to your mail server, you must acknowledge the fact that WIN-911 needs exclusive access to the mail account credentials you provide. WIN-911 will use this account to send and receive mail. It will also delete 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

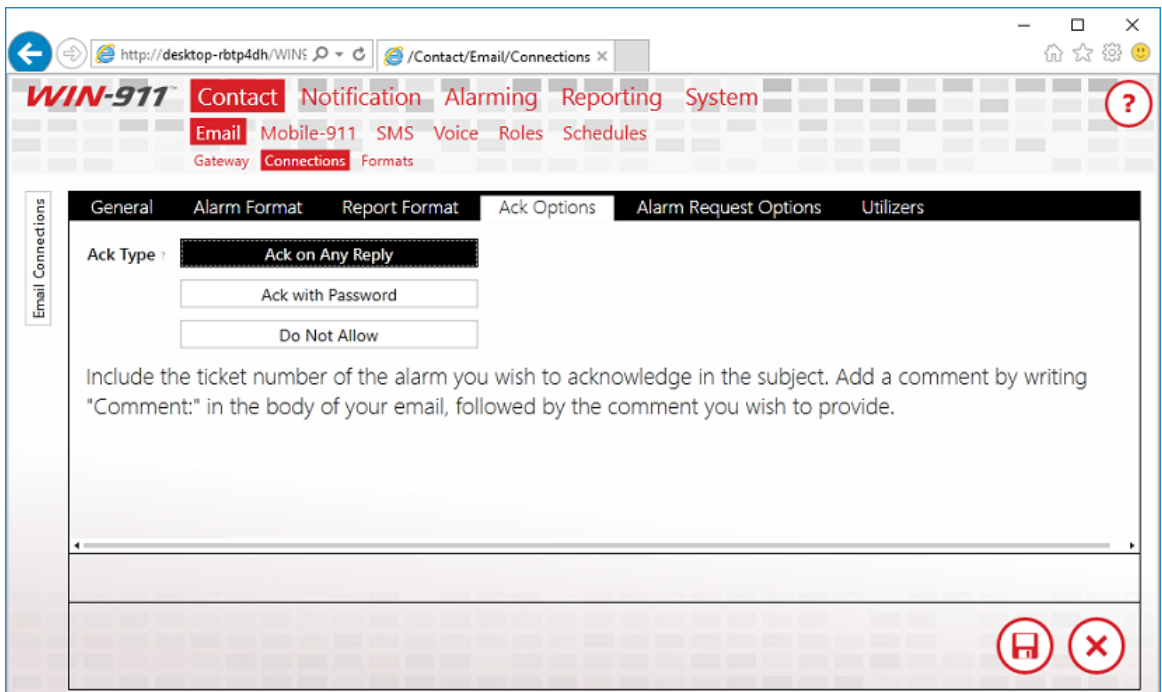
A connection defines the specific endpoint WIN-911 will send a notification to. For the email module, this is an email address. In other modules, like SMS and Voice, this is a phone number. The connection also defines the format that should be applied to messages, for both alarms and reports. The connection 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.

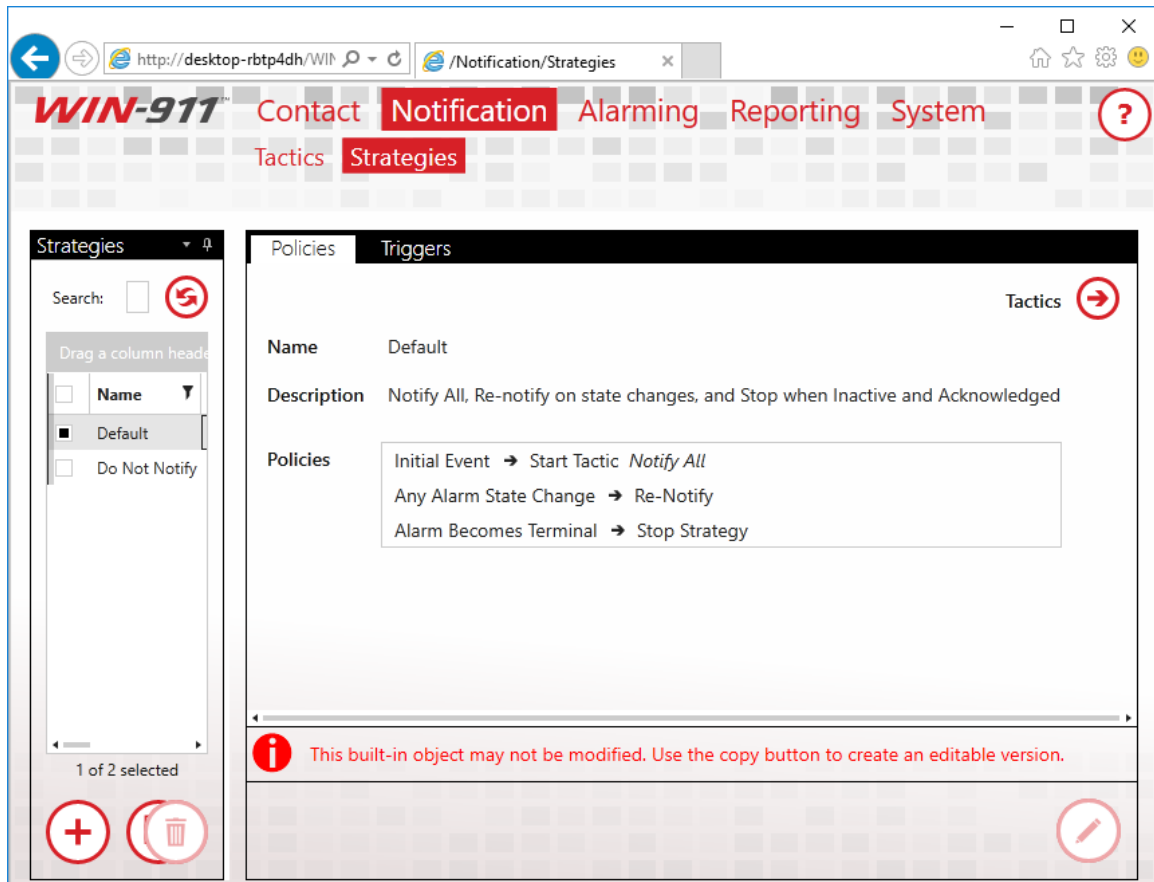
## Configure Escalation

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 lifecycle 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.

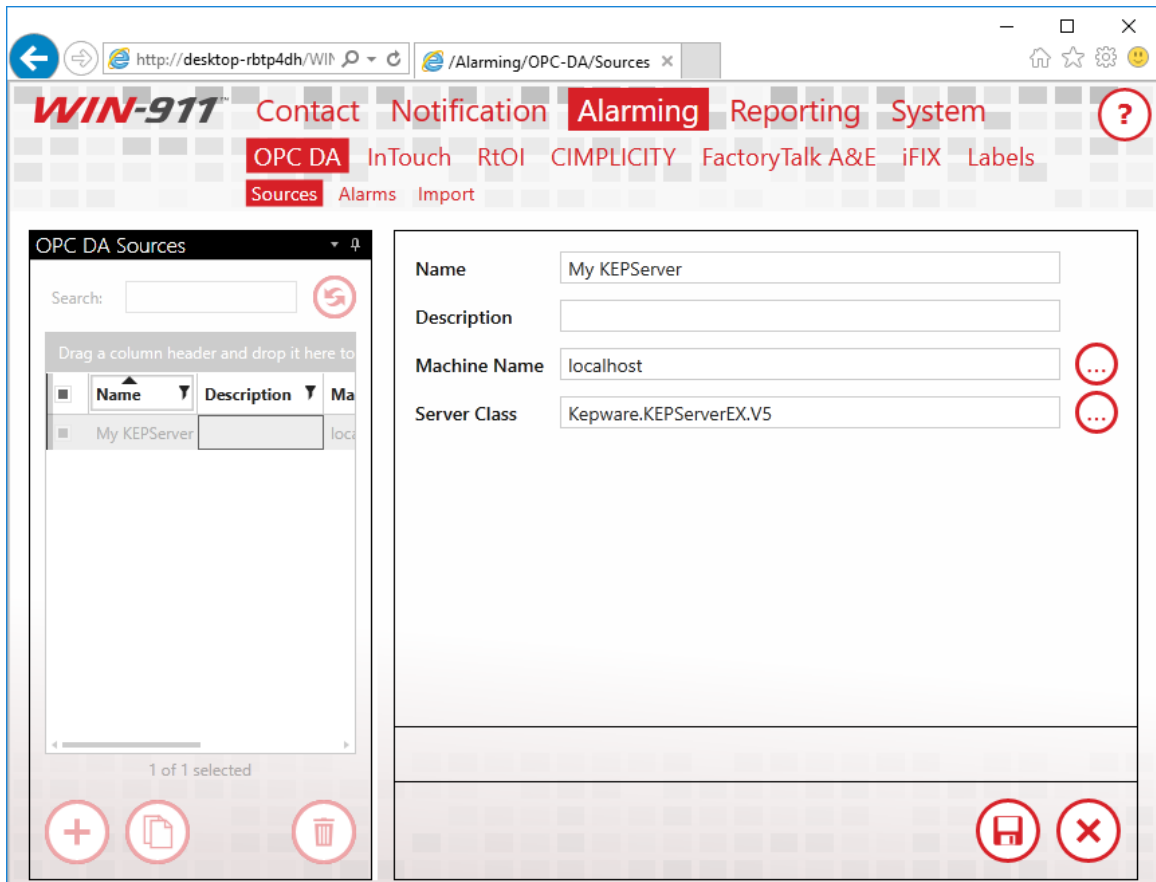
Advanced Tactics are essentially flow charts which determine who should hear about an alarm. Each block in the chart represent either an action to be taken or a decision to be made. These actions are generally Notification Blocks. Notification Blocks send messages to the connections specified in the 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 a 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

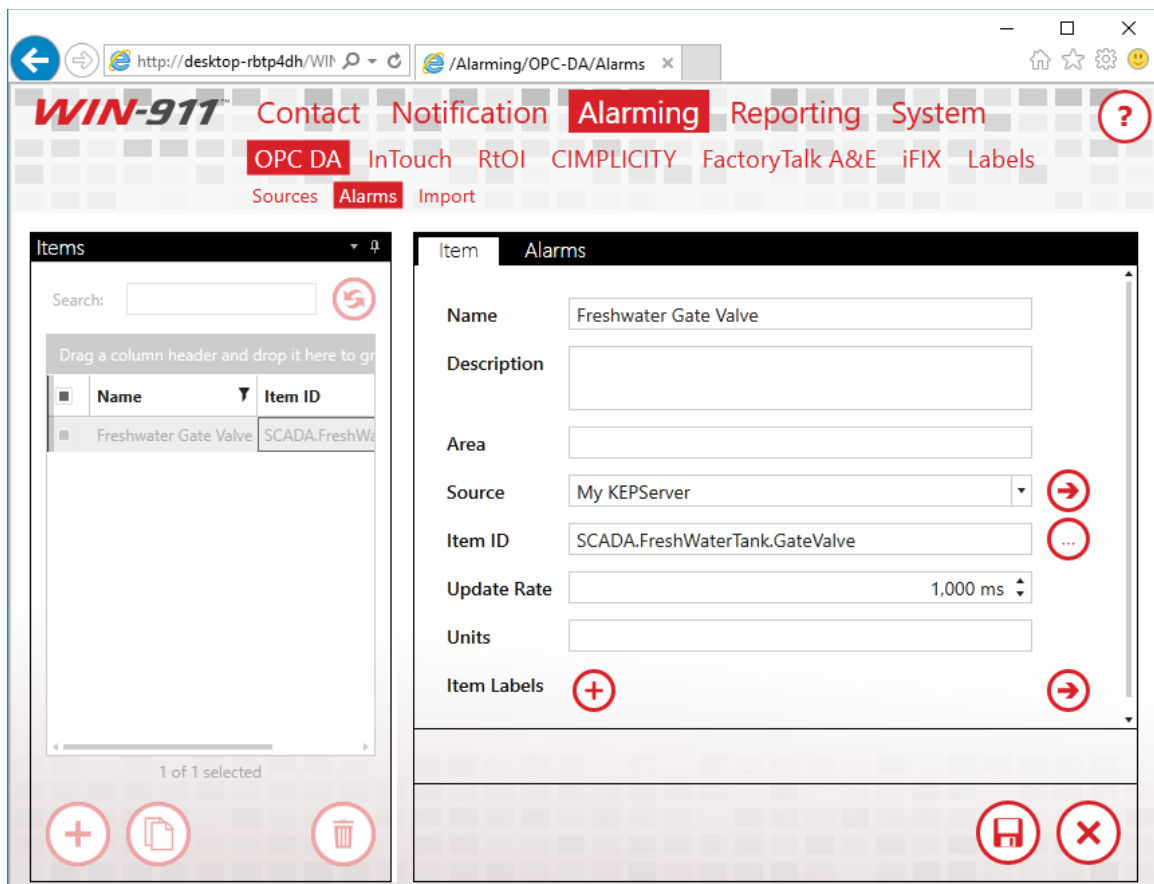
SCADA where it belongs. The remainder of this guide will assume that you have a locally installed OPC DA server and at least one digital point configured in that server.



*An example of a locally installed connection to KEPServerEX*

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.

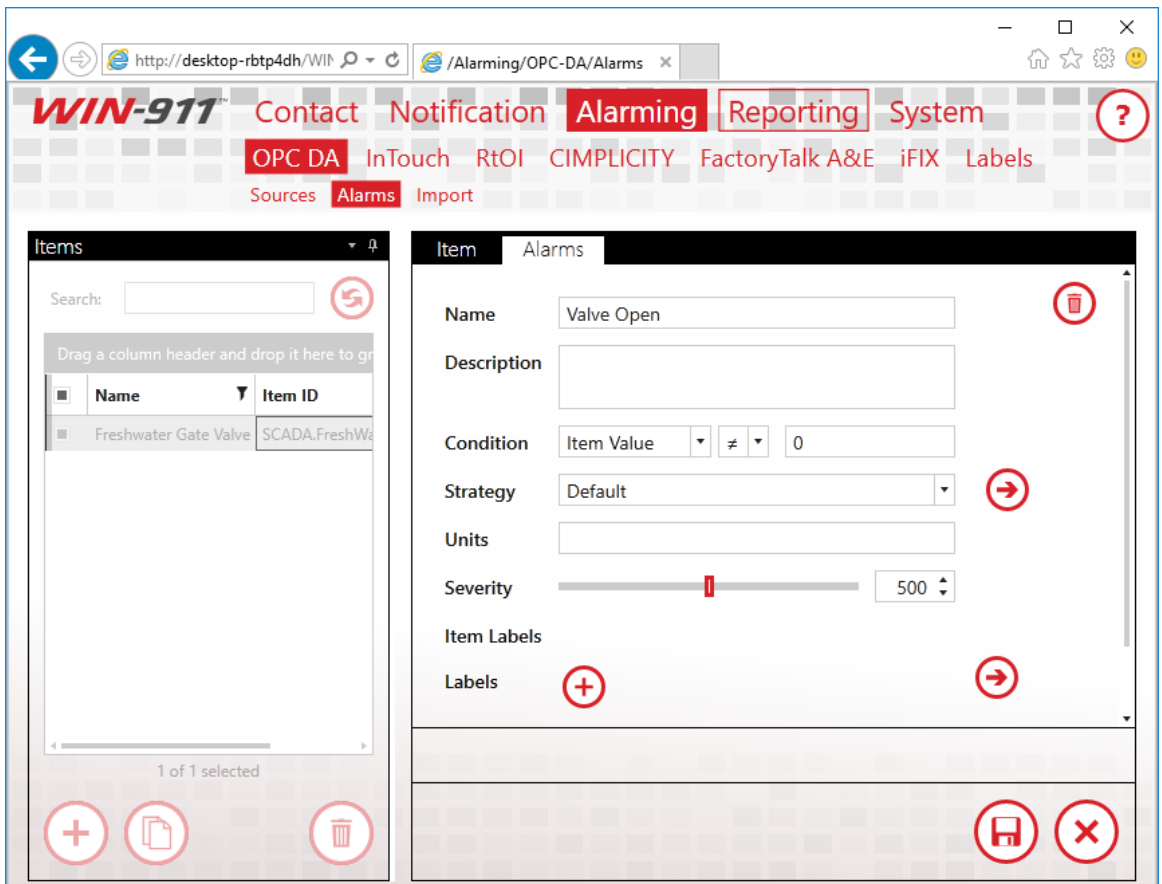
## Alarms



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 than 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.

## WIN-911 Alert

: Freshwater Gate Valve : Valve Open is...

ACTIVE

UNACKED

### Alarm Details

Area:

Name: Freshwater Gate Valve

Condition Name: Valve Open

Severity: 500

Congratulations on configuring your 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 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 email 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 is now Inactive and Acknowledged, WIN-911 will stop the executing Strategy and the lifetime of the alarm is completed.