WIN911 User Manual

Table of Contents

WIN-911

Welcome to WIN-911

WIN-911 is the most proven and advanced alarm notification software suite available for the automation industry. Capable of using a wide variety of notification methods, WIN-911 can reach you wherever you are. WIN-911 interfaces with SCADA/HMI data servers to monitor values and flag alarms. When an alarm is detected WIN-911 will notify remotely located users by dispatching electronic messages containing vital information and allowing the recipient to respond by replying to the message with acknowledgement instructions. In addition to simple notification, WIN-911 allows users to interact with your SCADA/HMI by accepting requests for both report data and current alarm conditions.

WIN-911 Enterprise Edition is a complete rewrite of our flagship product using current technology and standards. This release supports Email, Voice, SMS, and Mobile-911 messaging for remote notification delivery and subscribes as a client to any OPC DA server for data monitoring and alarm reporting. This release includes a suite of custom data source connections to iFIX, FactoryTalk A&E, InTouch, and Cimplicity.

Key differences from the WIN-911 Version 7 product are:

- The configuration tool is a browser-based GUI that configures the product live during runtime from any system on the network.
- Each module has two primary components, an Application Server running in Internet Information Services (IIS), and a runtime executable running in the system's services. Hence, Enterprise Edition is "always on" and does not require a restart to apply configuration changes; nor is it affected by Windows users logging in and off the host computer.

- The Email notification method for Enterprise Edition is capable of two-way communication. Thus a remote user will receive alarm notifications in near-real time, and be able to acknowledge alarms by responding with the proper credentials. The user can also request information from WIN-911 at his/her convenience.
- Dramatic enhancements to the Schedule interface allows the user to easily create complex schedules via an calendar presentation. Schedules use appointments that can revolve around blocks of time, days of the week, weeks of the months, etc..
- WIN-911 Enterprise Edition introduces a revolutionary concept in the design and deployment of complex notification tasking: Tactics and Strategies. Alarms are associated with a single Strategy. Each Strategy controls the execution of any number of Basic or Advanced Tactics which conduct remote notification procedures.

Release Highlights

- Improved InTouch Data Source
- Improved installer
- Localization Improvements

Getting Started with WIN-911

Tech Support

You can contact WIN-911 Tech Support at Support@WIN-911.com.

WIN-911 Installation

WIN-911 3.17.5 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.
- Microsoft Windows 7/8/8.1/10 Professional Edition or Microsoft Server
- 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 will be installed)
- 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

WIN911

- 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.

WIN-911 Client

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

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 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"

- WIN-911 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 your install WIN-911 and an 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"

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 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 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 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.

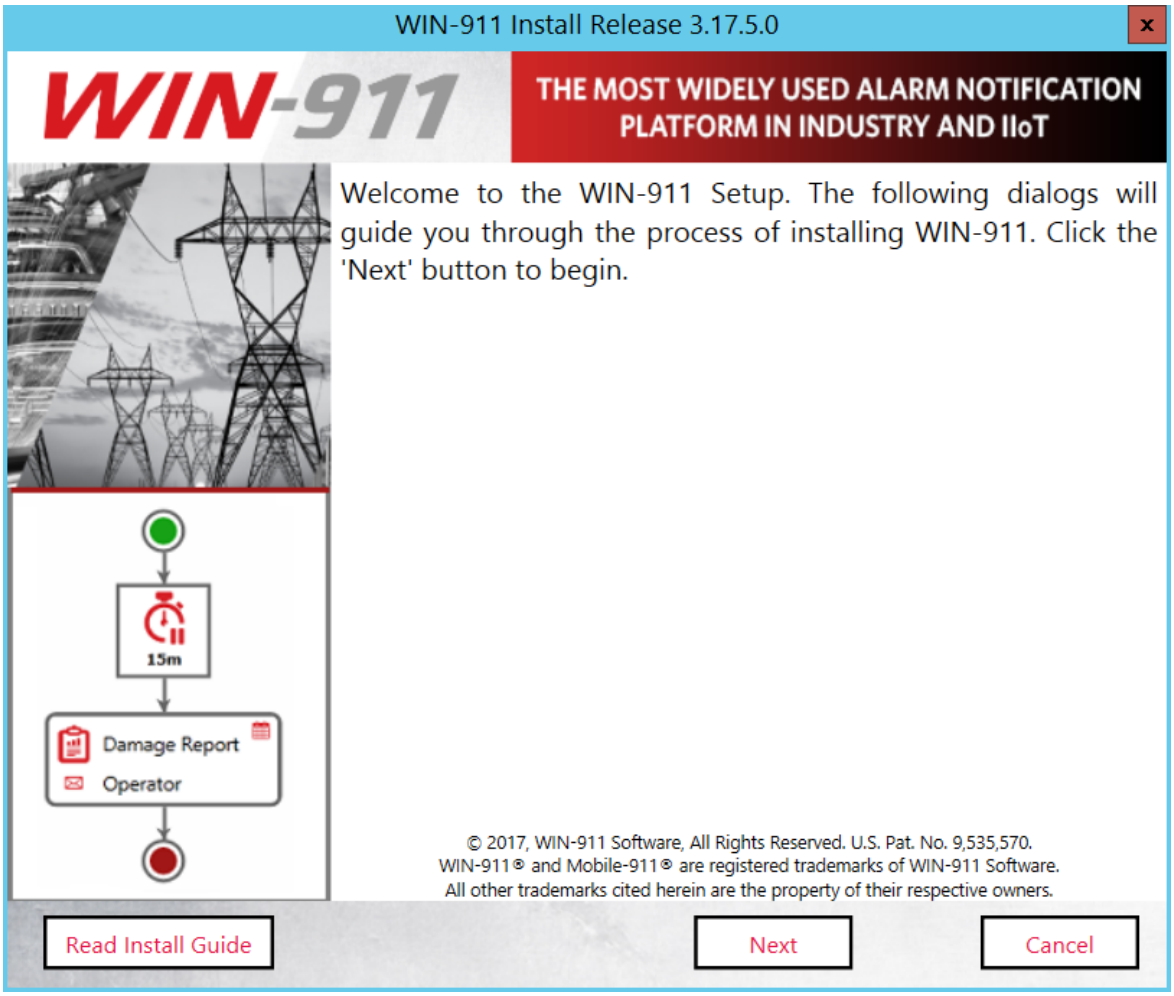
Installation Path

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 Setup

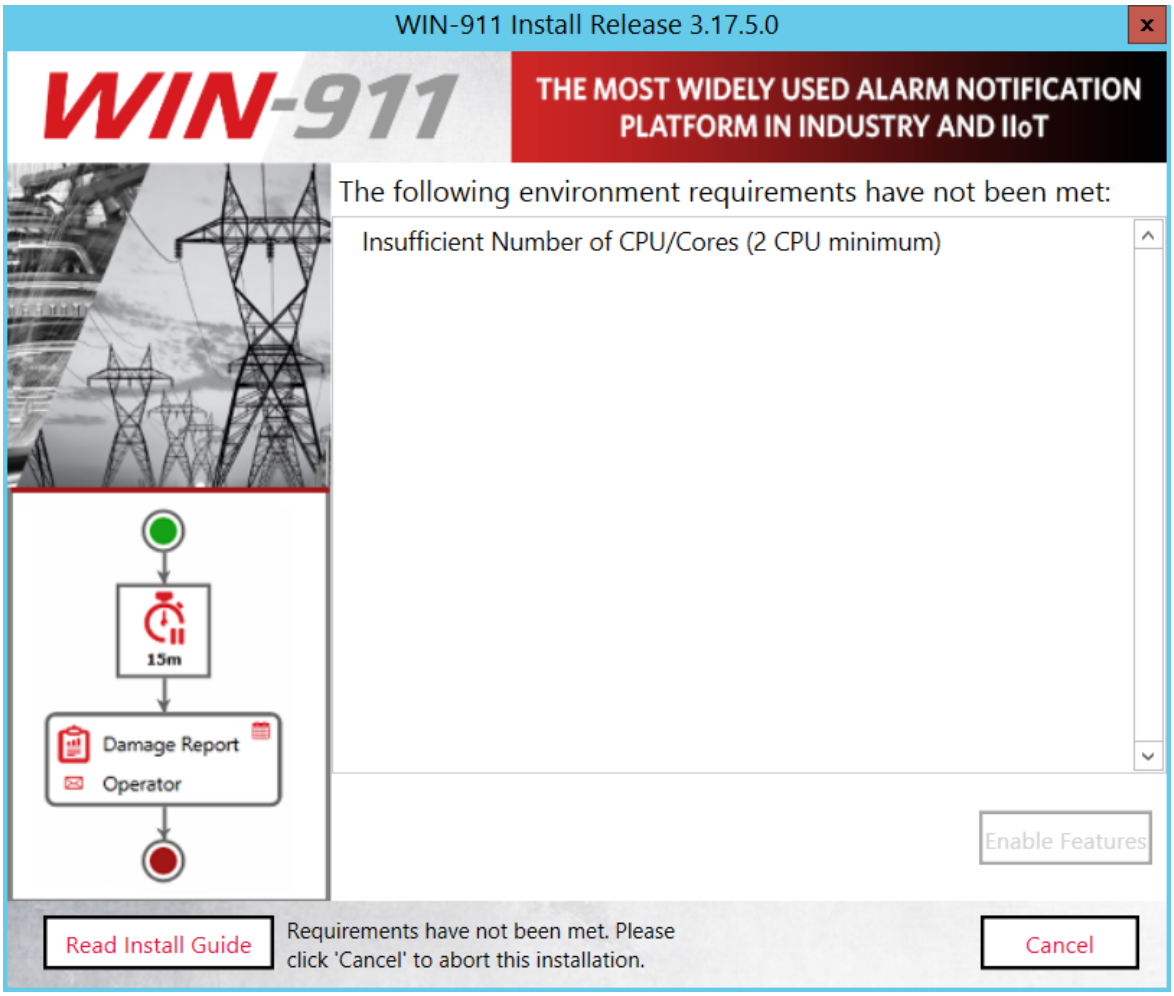
The WIN-911 Launcher requires .NET 4.0 (or higher). If the target machine lacks this framework, you will need to add the framework in order to commence. In Windows 8.x, this can be done through *Programs and Features> Turn Windows features on or off*. With Server operating systems use *Server Manager>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

To install WIN-911



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

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



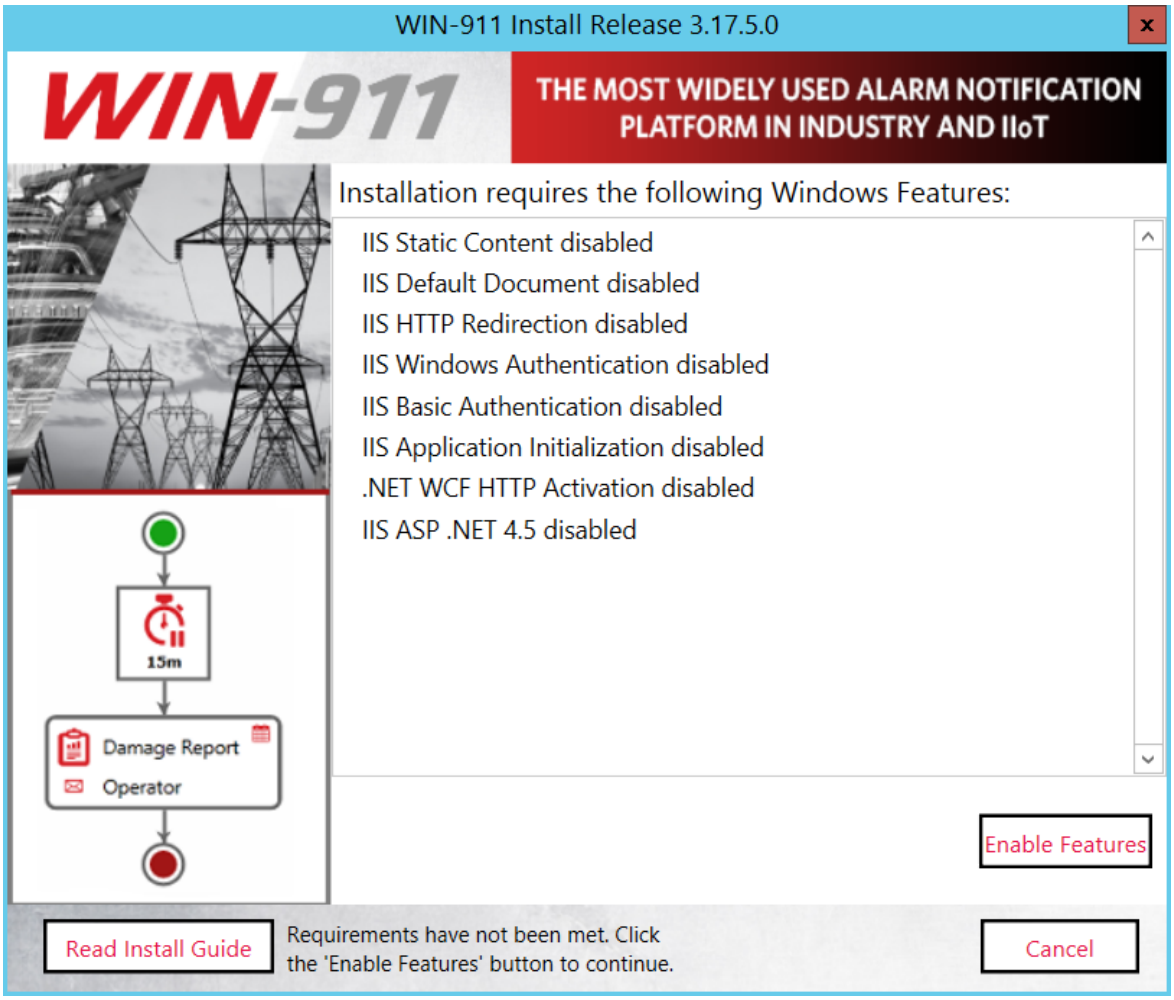
Such environment requirements include:

- 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 3.17.5 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 4.5
- Windows Edition and Feature Set Detection
- WIBU CodeMeter Control Center
- 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.

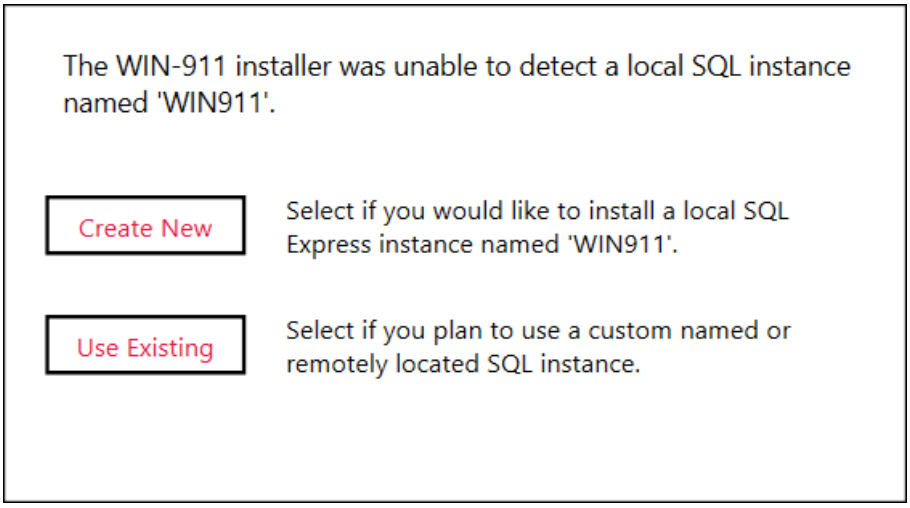
Note: If these requirements are met, this page will not appear.

SQL Server Installation

WIN-911 uses an 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 Launcher install SQL Server 2014 Express on the host computer.

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:



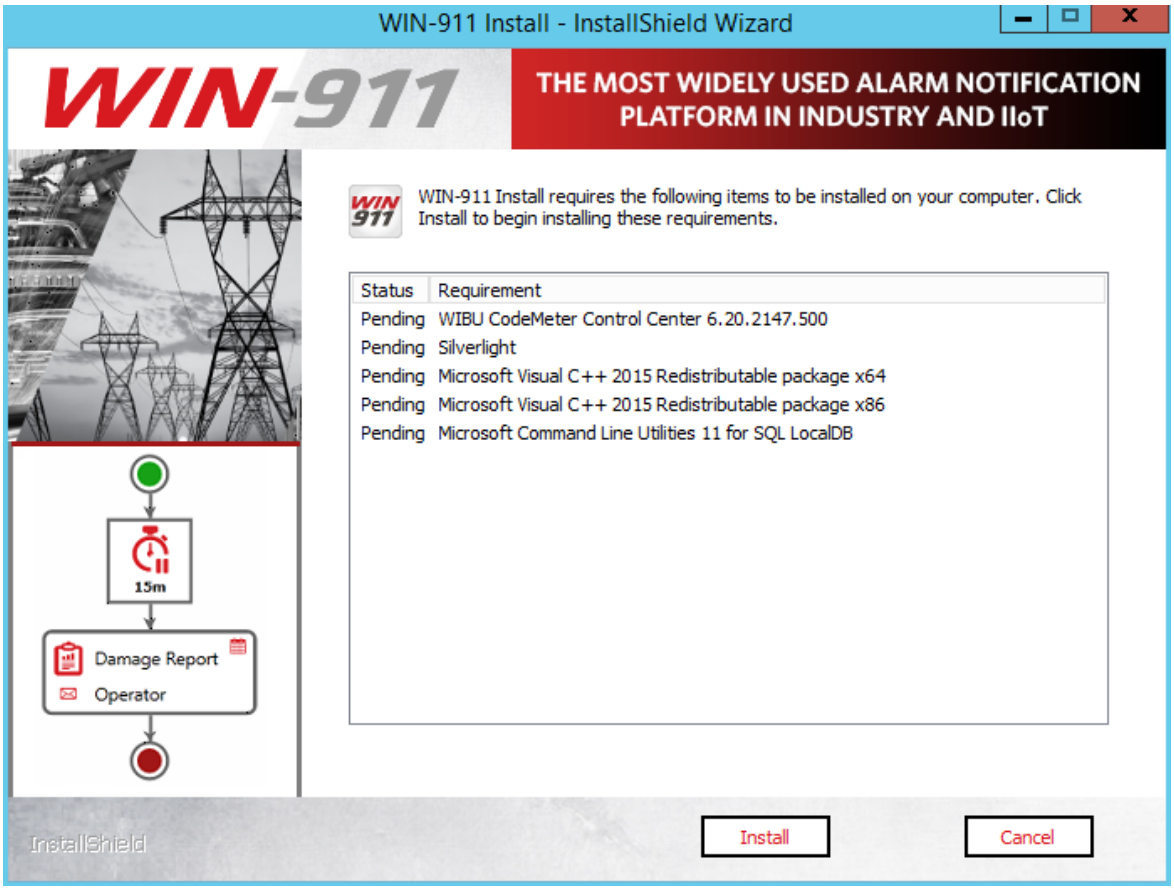
This is an optional step and is not required in order to continue with the installation, but WIN-911 cannot be used until the SQL Server requirement is satisfied.

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

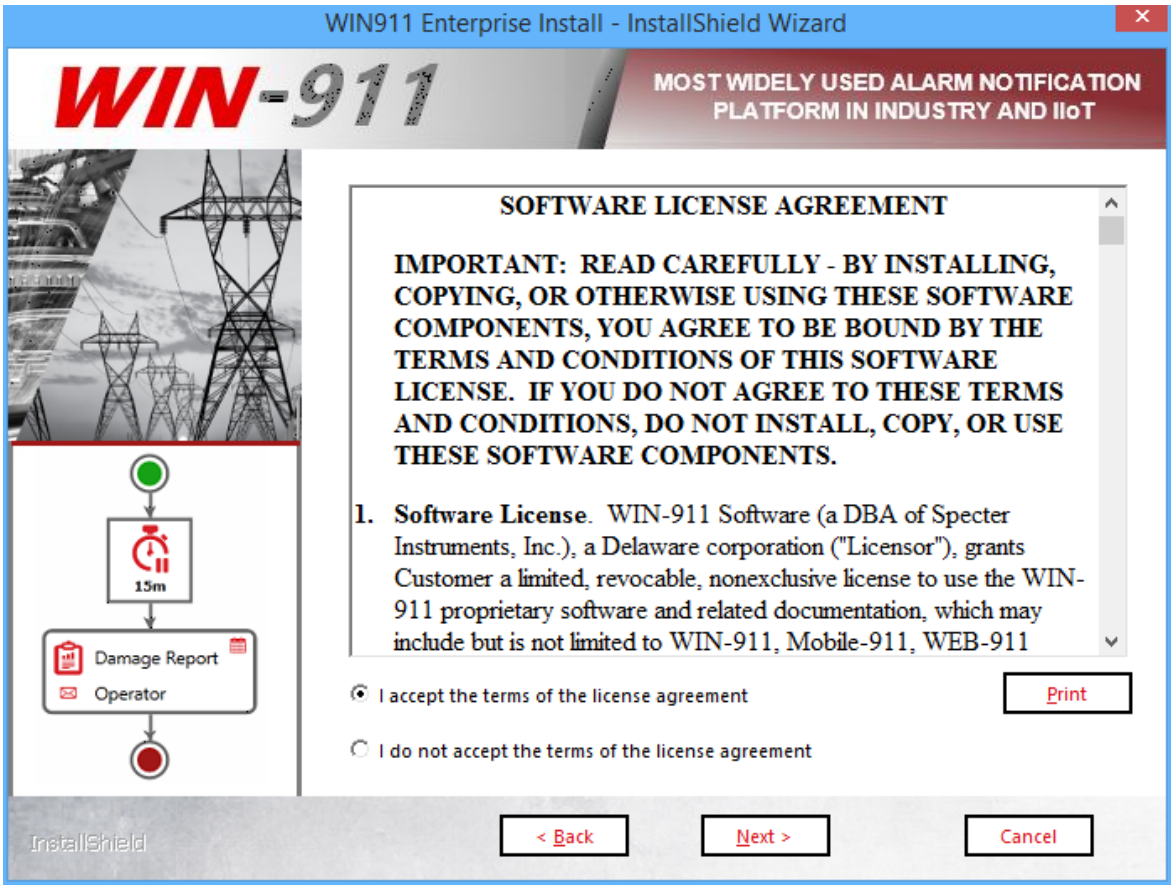
For more information about specific requirements for SQL Server installation and configuration, see Microsoft documentation available online.

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

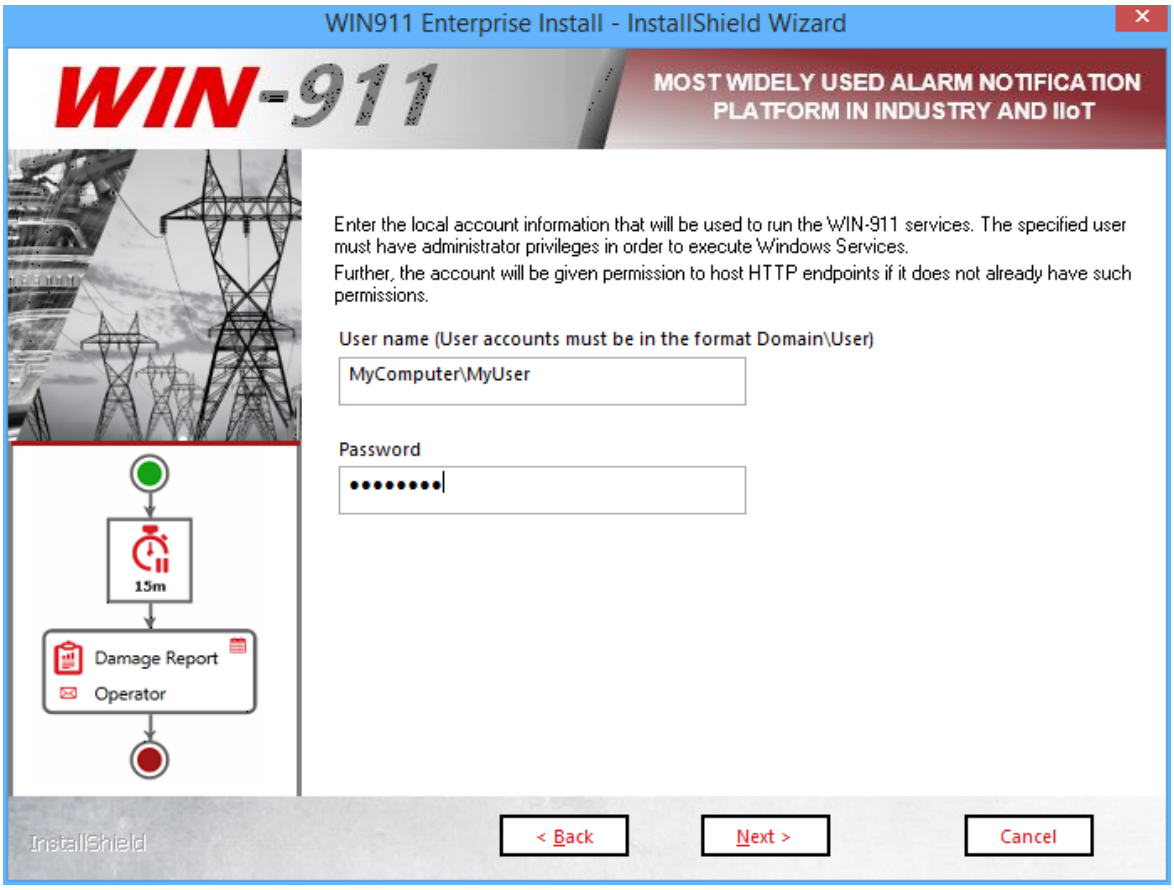
InstallShield Wizard



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

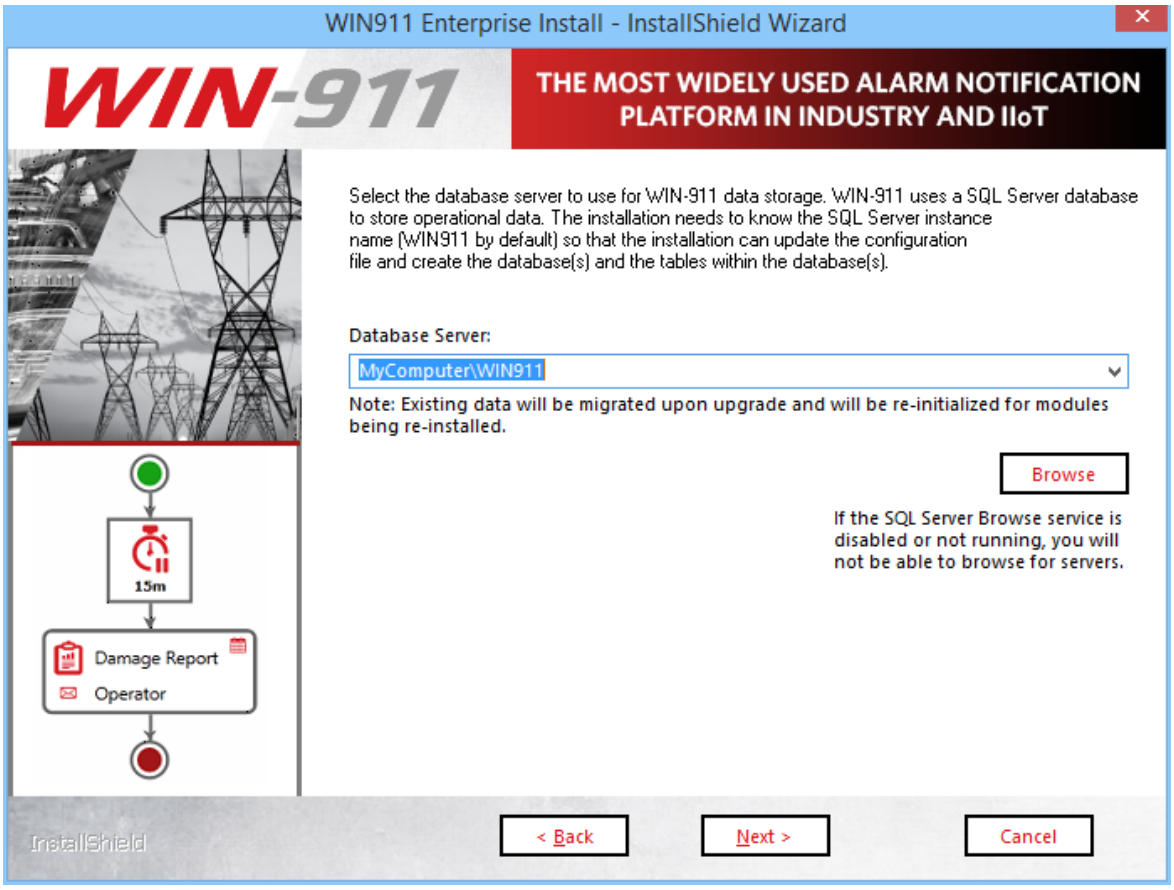


Accept the terms of the Software License Agreement by clicking the top radio button and then select **"Next"** to advance.



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.**

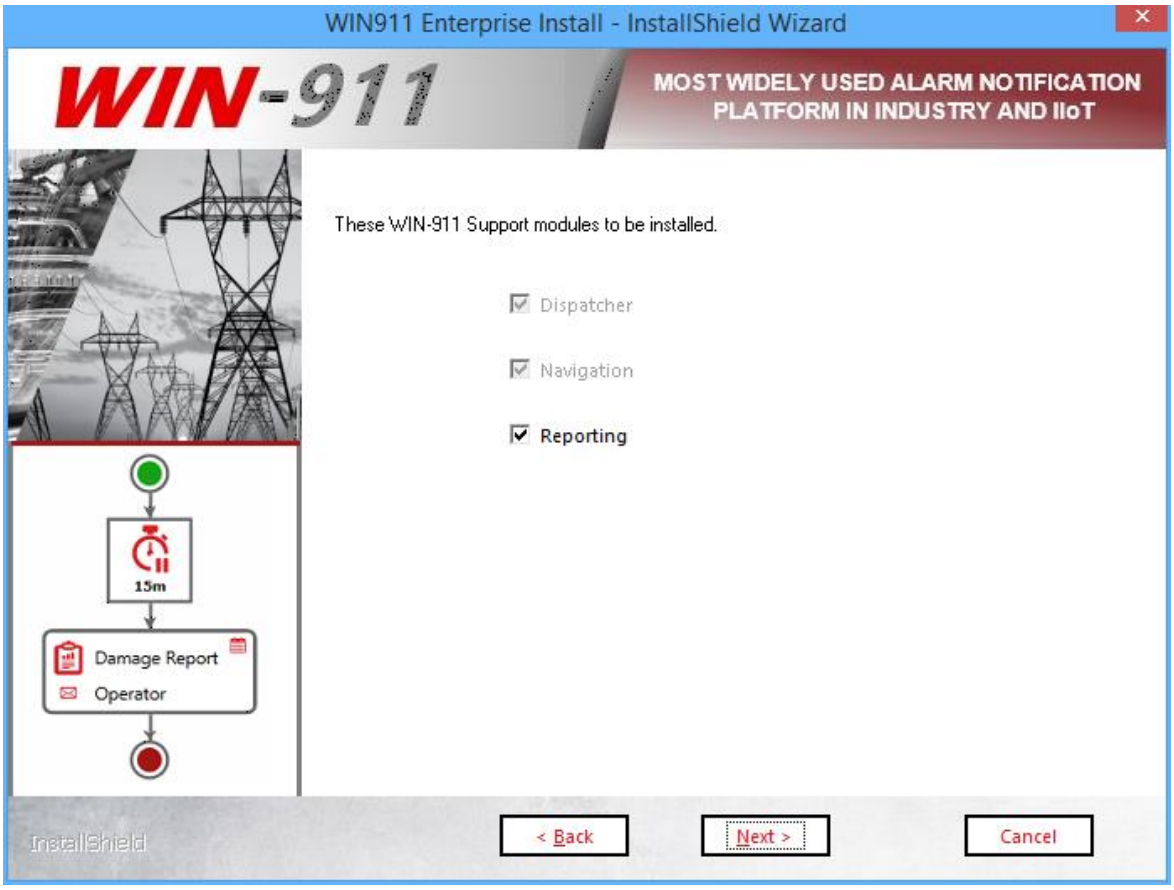
Note: You must be logged in and executing this installation as an owner and administrator of the SQL instance. Additionally, the selected user here (if different) must be a member of the Windows local or domain administrator group with administrative privileges on the SQL instance.



In this step, the installation looks for an 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.

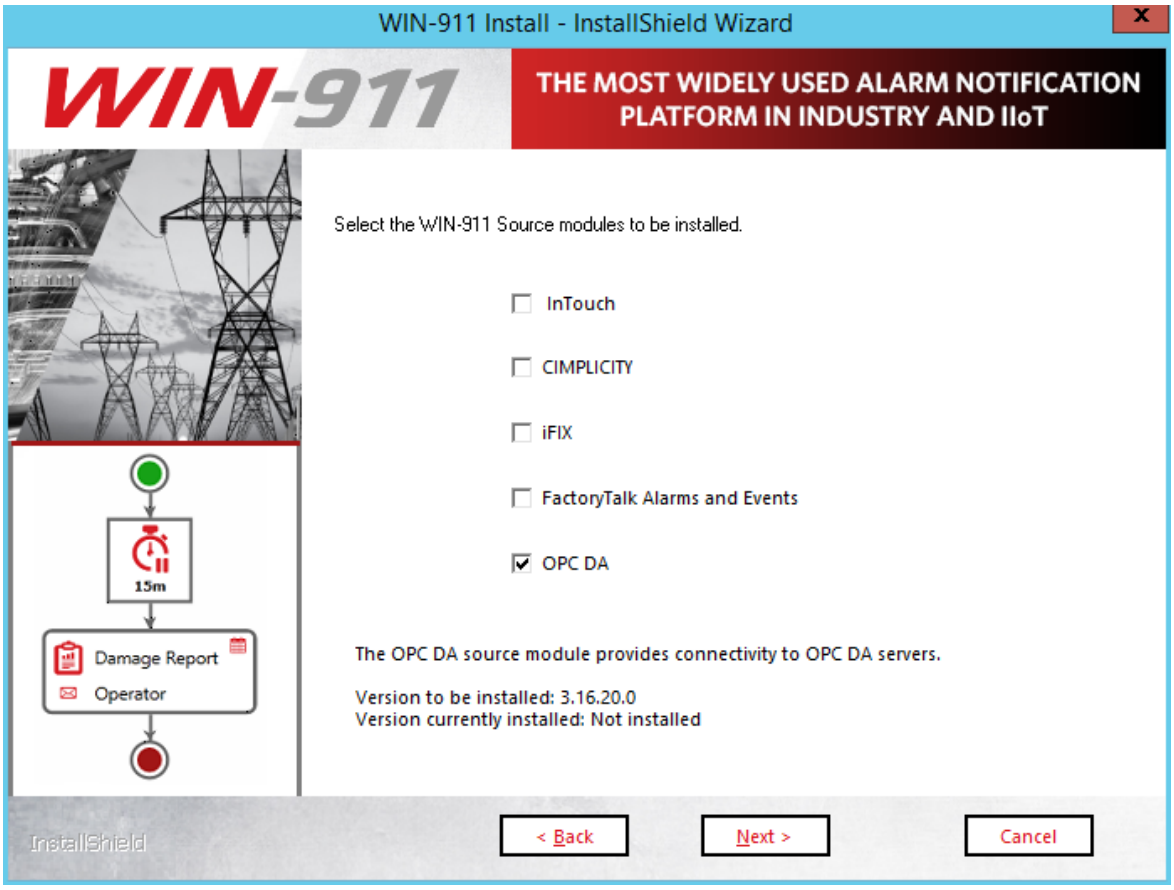
Click **"Next"** to advance.



The support module selection menu allows you to choose which components of WIN-911 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.

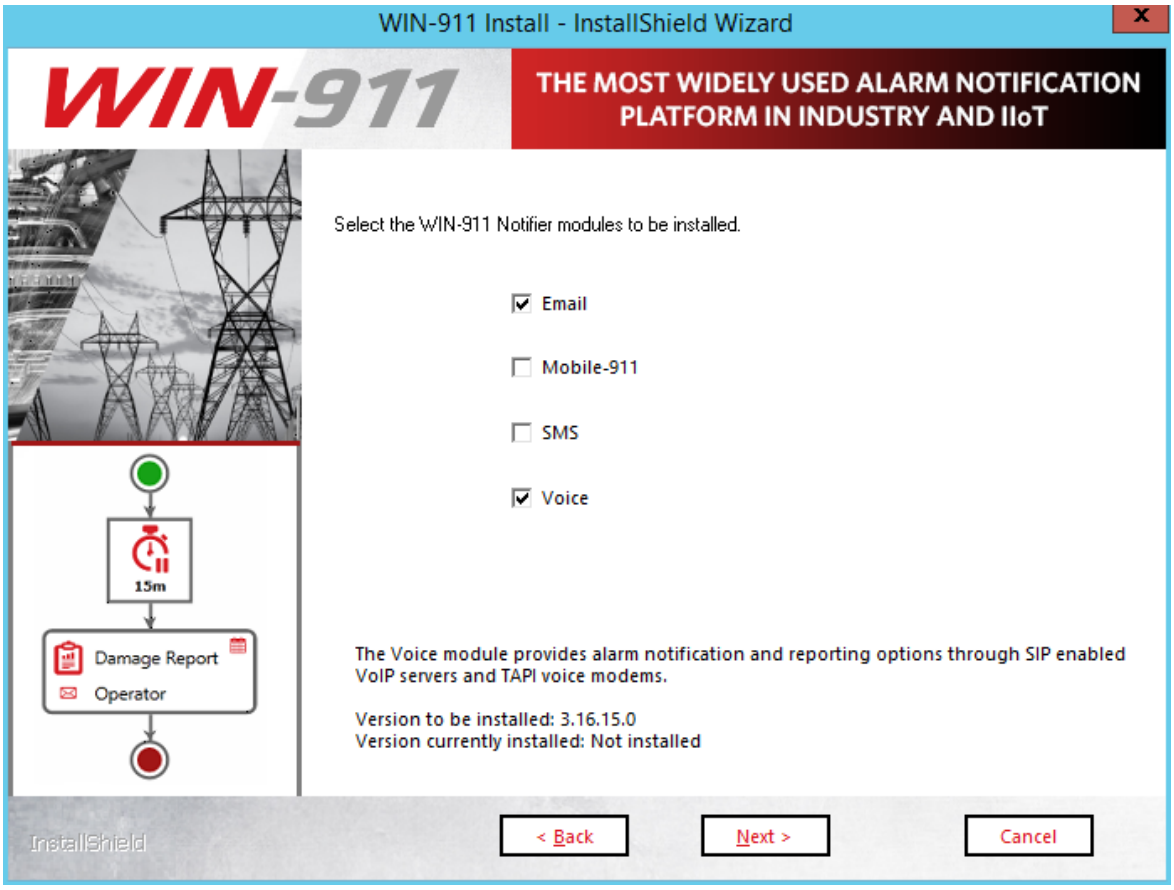
Click **"Next"** to advance.



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. 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.

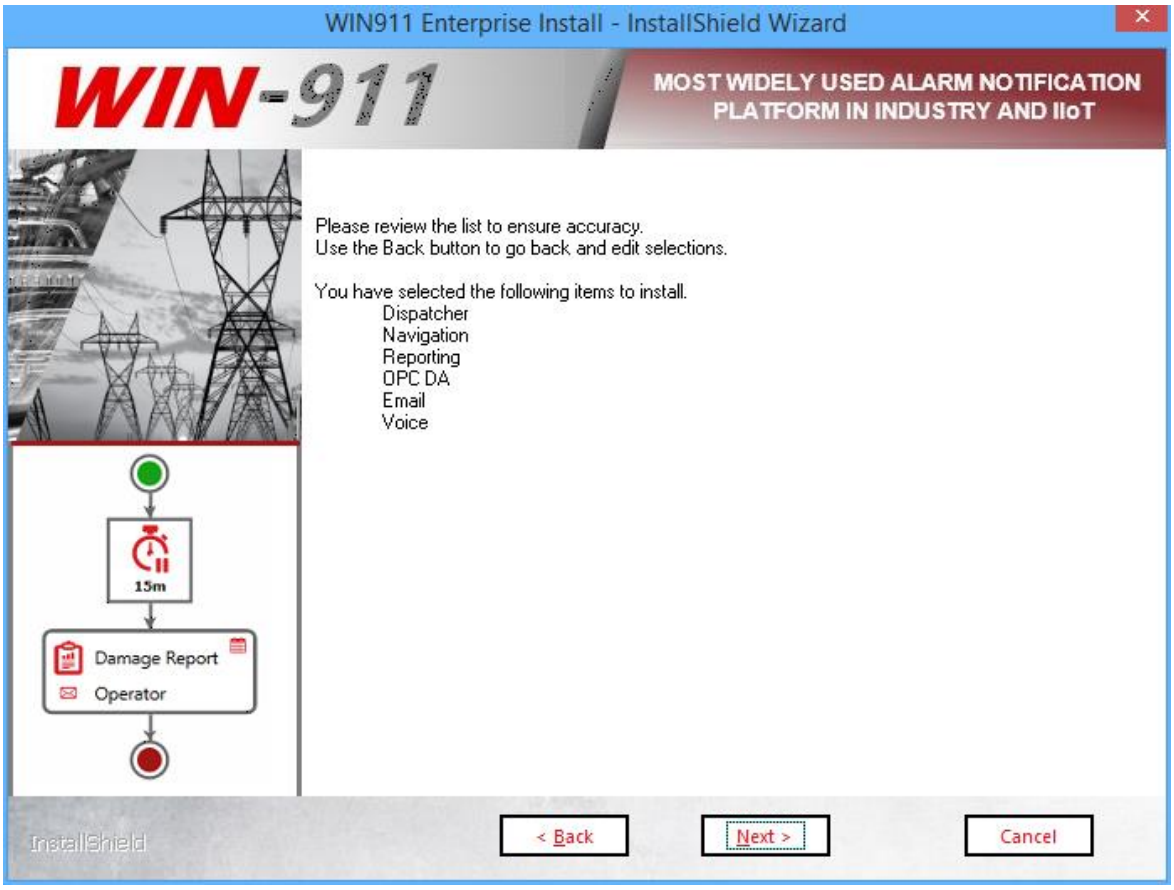
Click **"Next"** to advance.



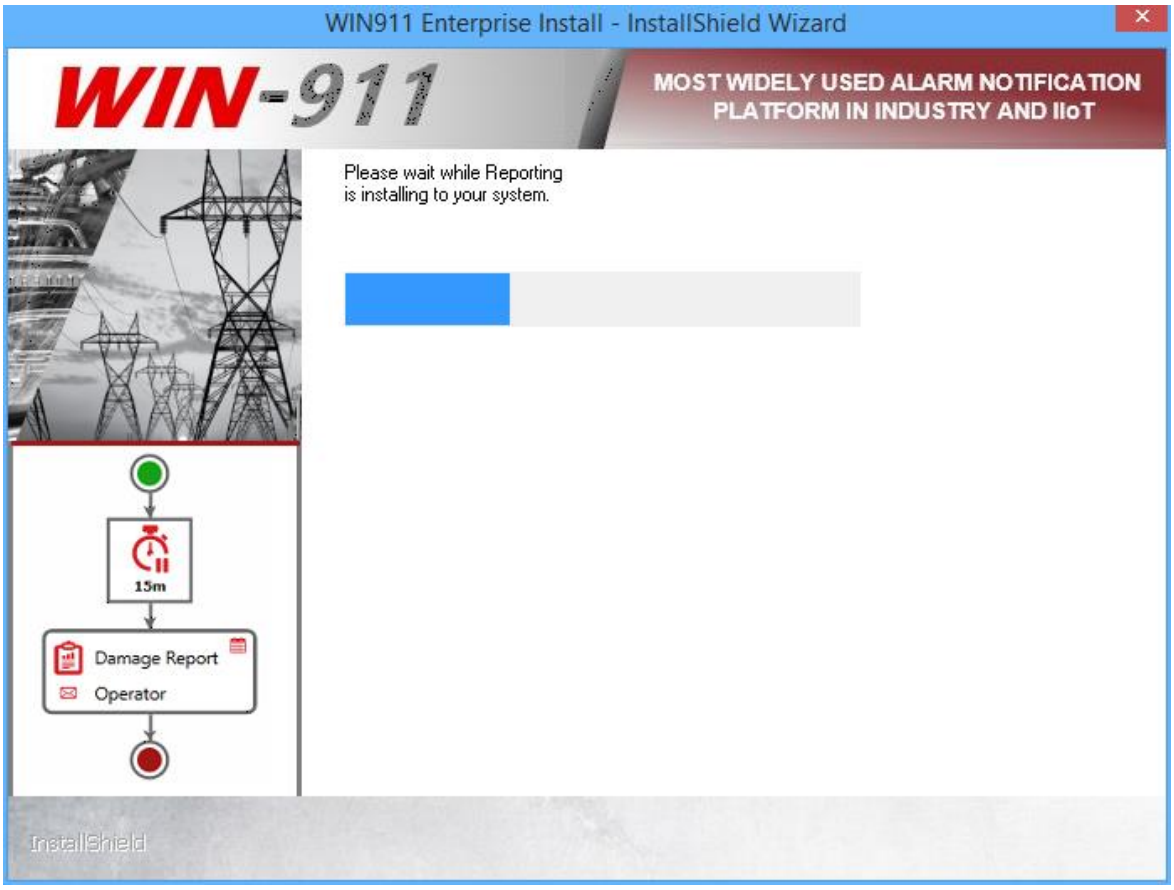
WIN-911 provides several methods of remote notification to the users, including Email, Mobile-911, Voice, and SMS. The notifier module selection menu allows you to choose which components of WIN-911 you install. Again, you should install only the notifier modules you intend to avoid errors. You can re-run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

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

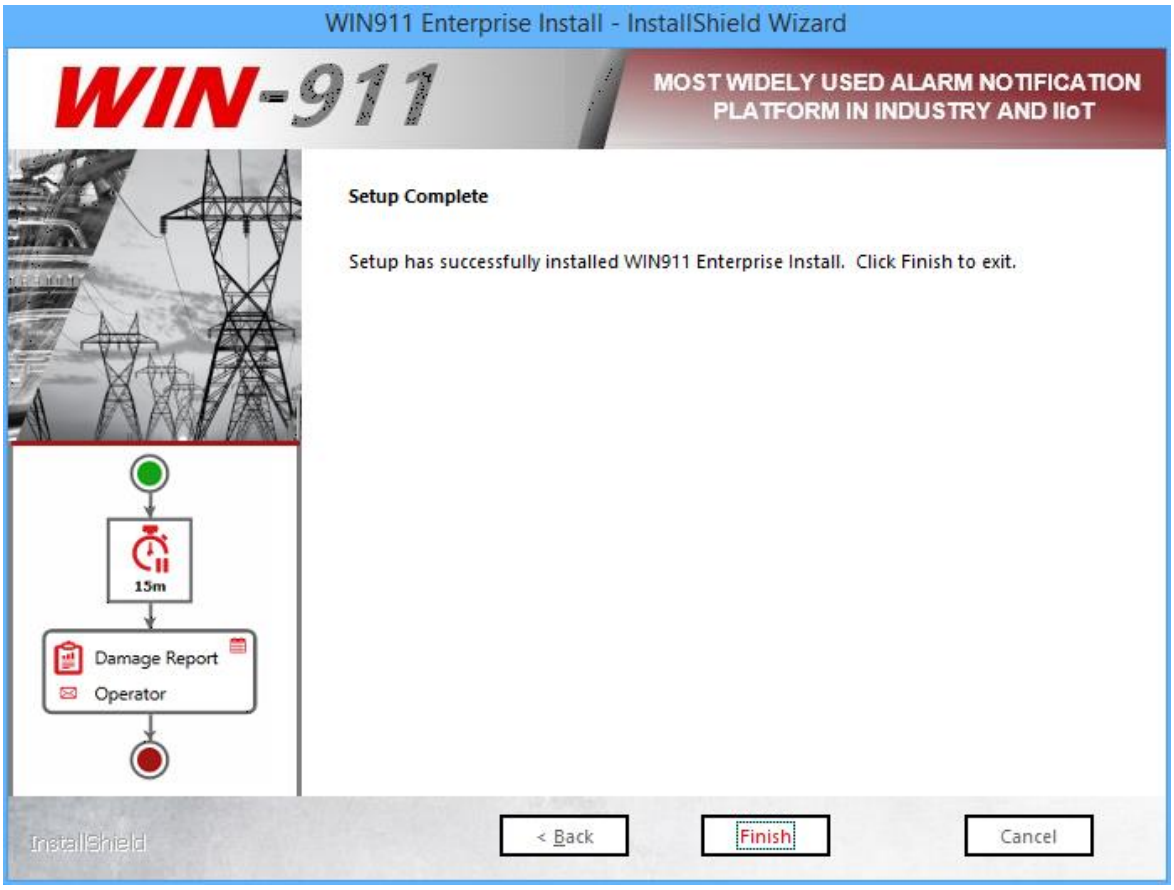
Click **"Next"** to advance.



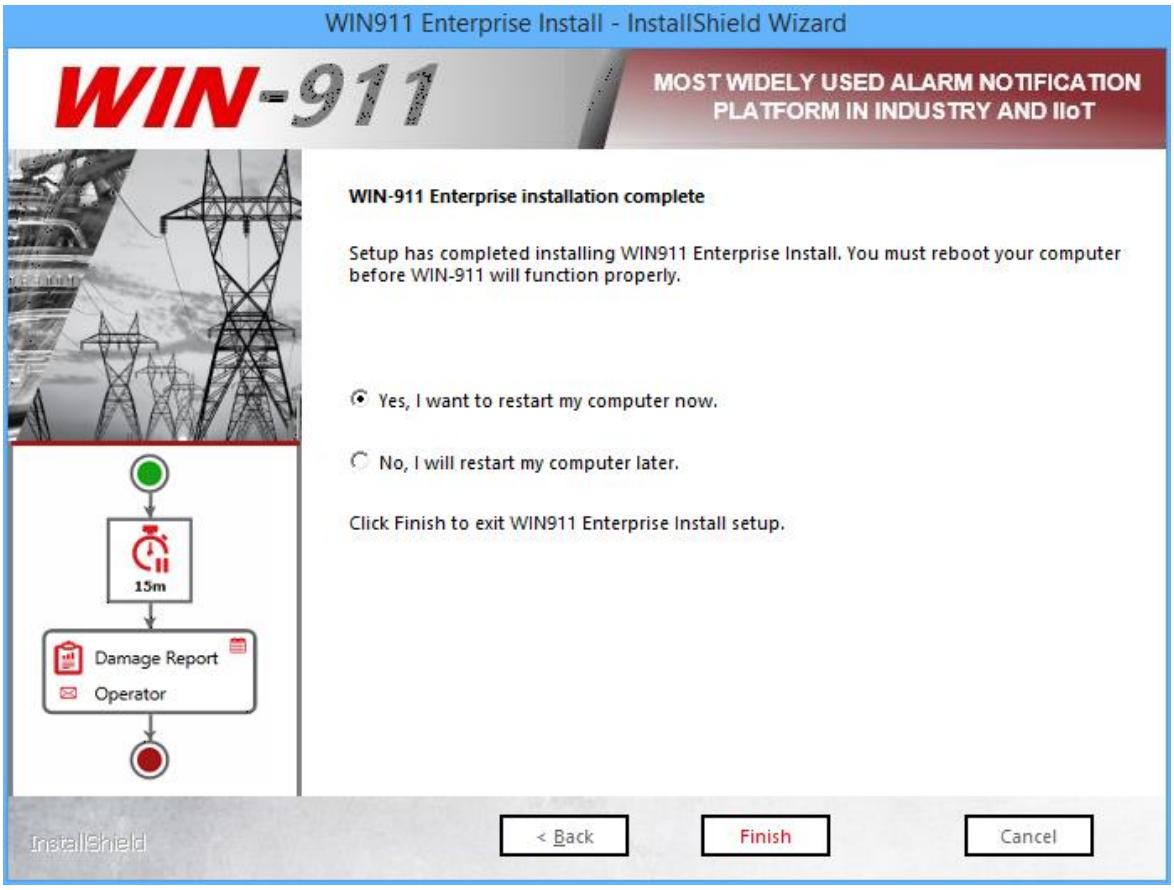
This page presents the manifest of selected modules to be installed. Please review and click the *Back* button to change the list or *Next* to begin the installation and initialization phase of the setup.



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



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. 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

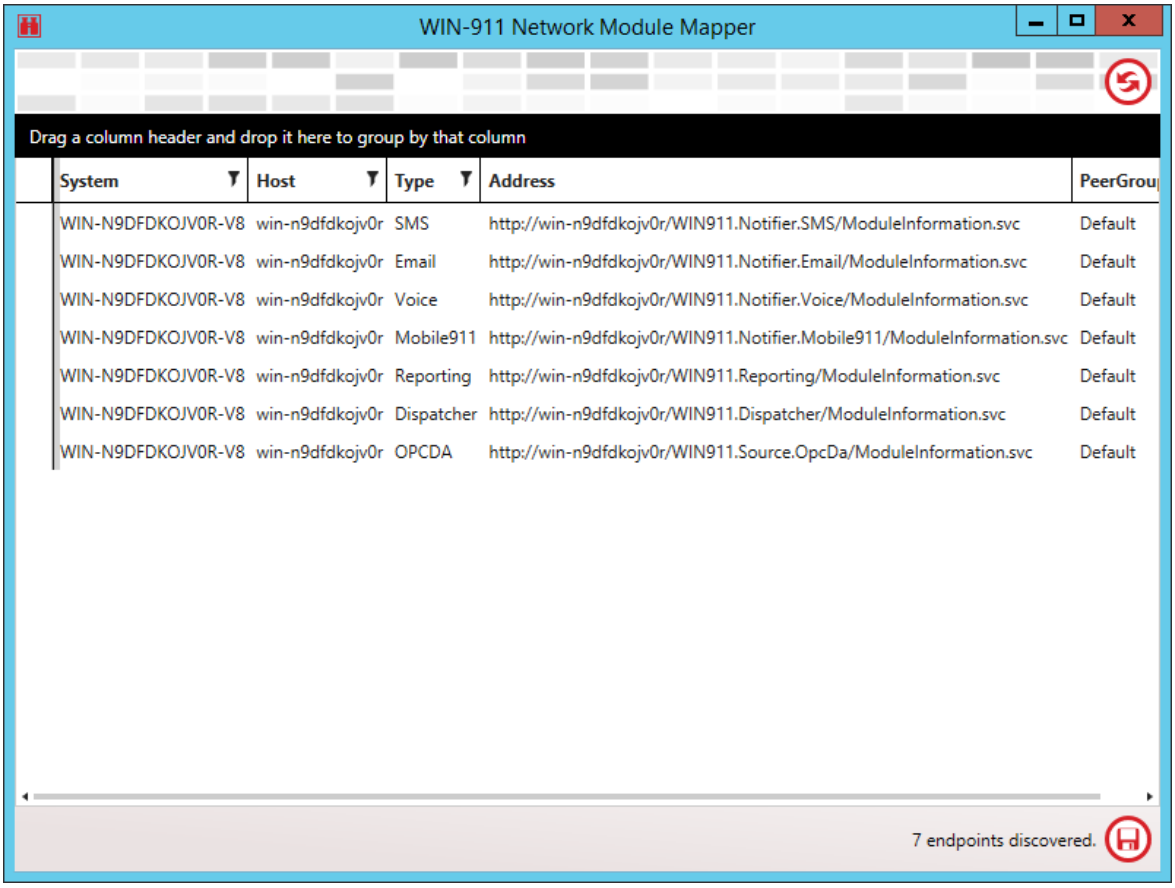
WIN-911 features can be uninstalled via *Control Panel\Programs and Features*. Each module will have to be uninstalled individually. Right-click the WIN-911 module and select Uninstall. Repeat this process until all undesired features have been removed. You will then need to run the WIN-911 Endpoint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

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



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**

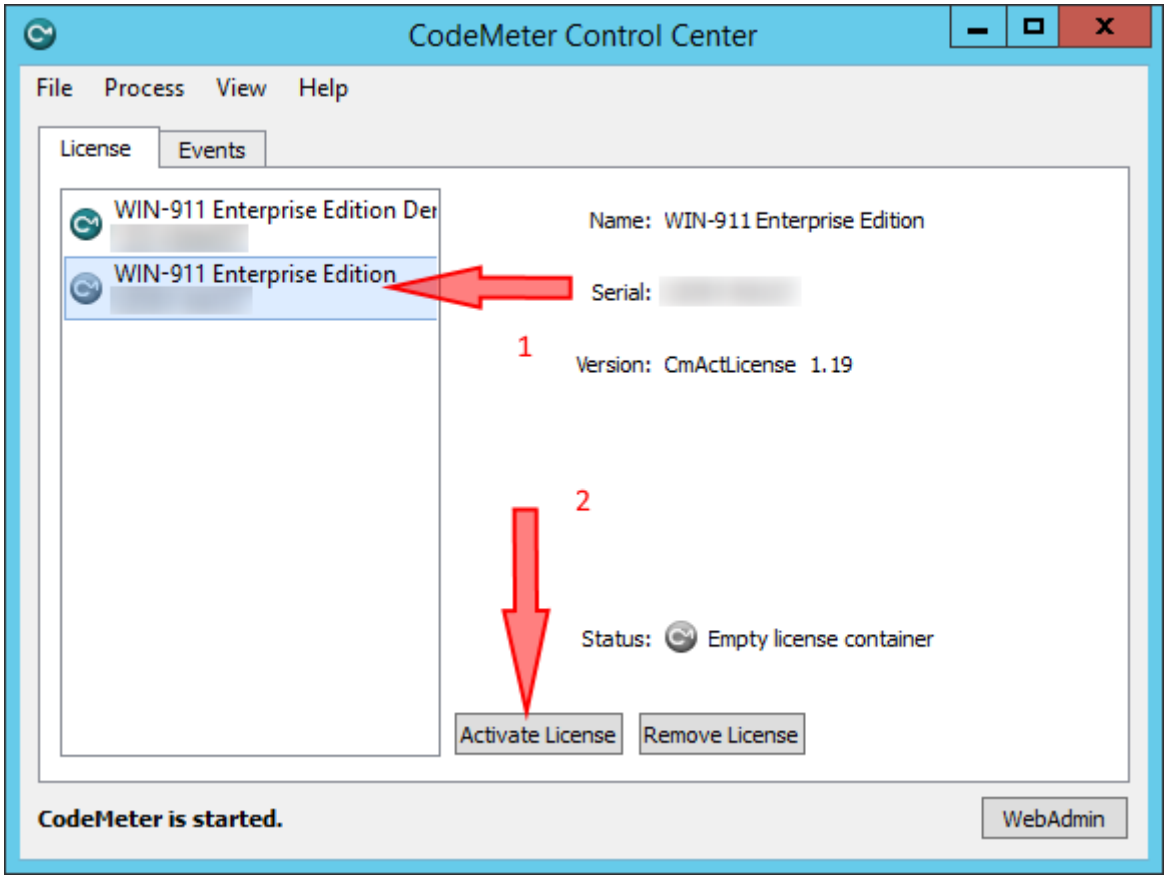
not need to run the WIN-911 Endpoint Mapper again unless you remove certain features included in the initial install.

Licensing WIN-911

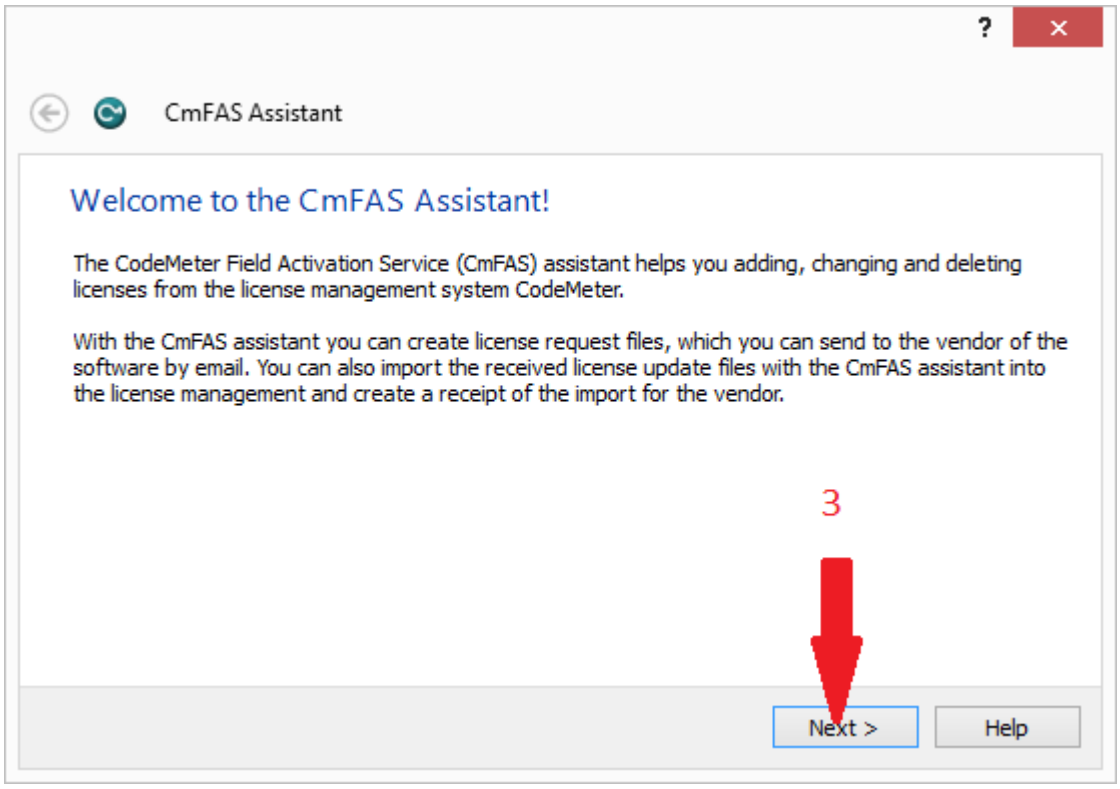
Note: After an initial installation WIN-911 will be configured with a demo license that will run 30 days without restriction.

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

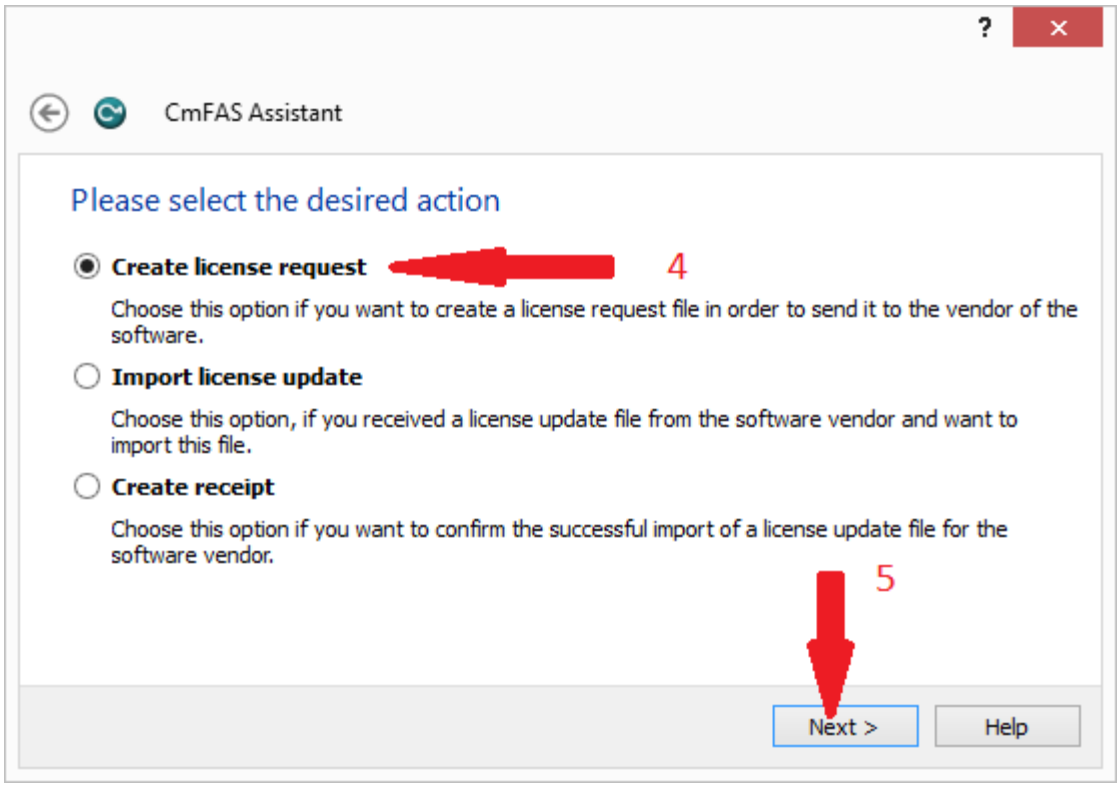
Click the "License Update" button and follow the wizard to generate a license request file.



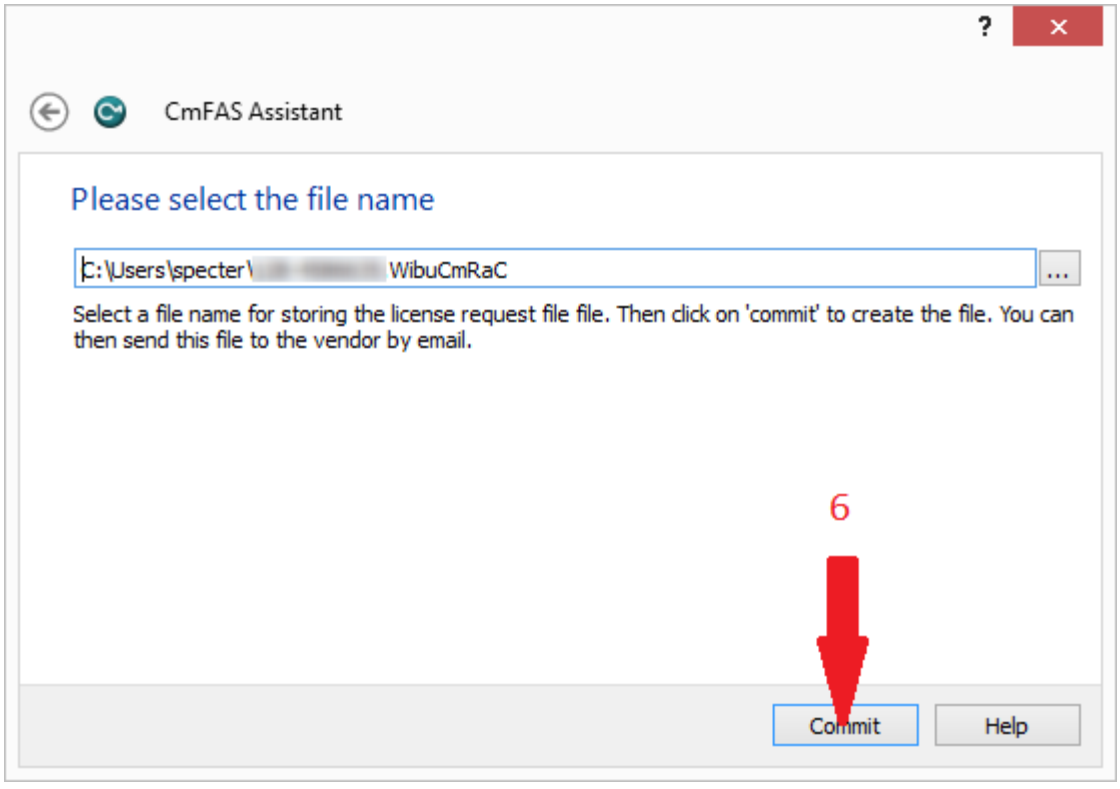
Select the container with the active license (1). The Status indication will verify "Empty license container". Then click Activate License (2).



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



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

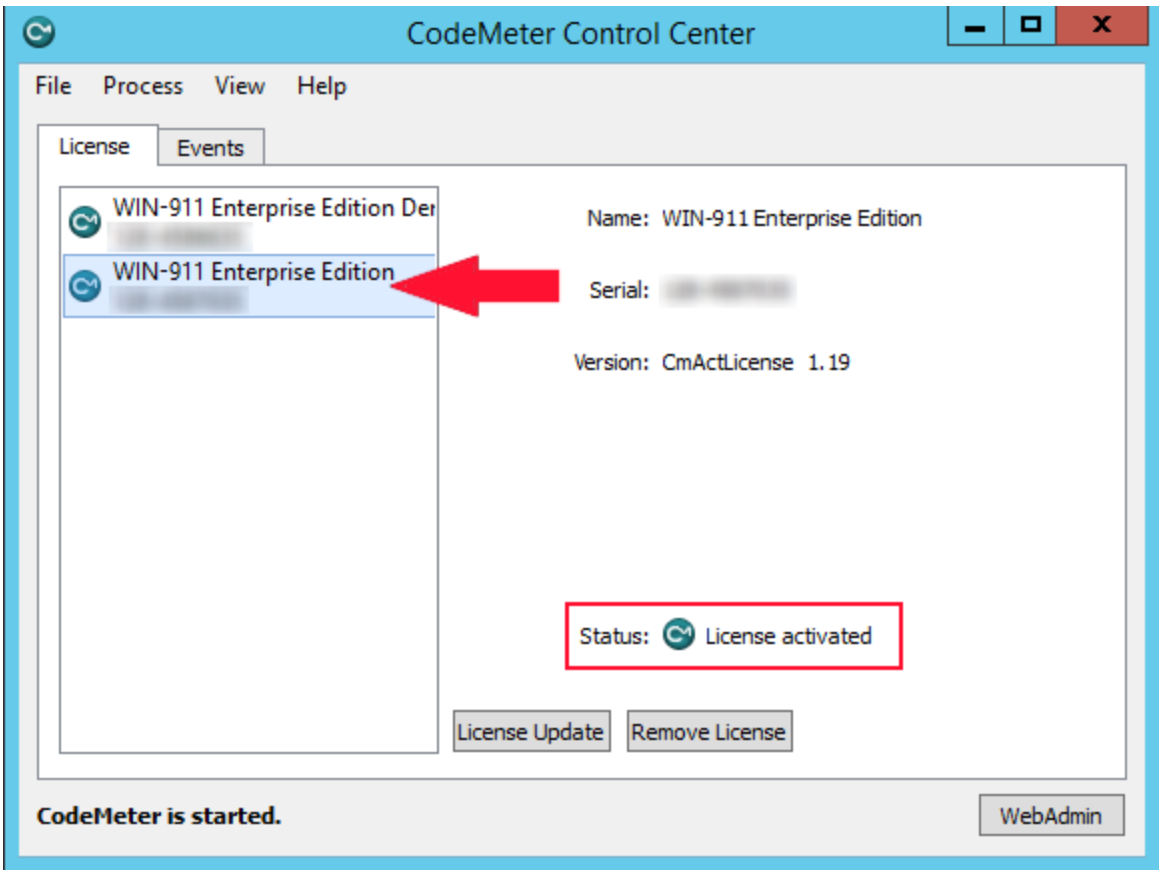


Note the location of the license request and then click Commit (6).

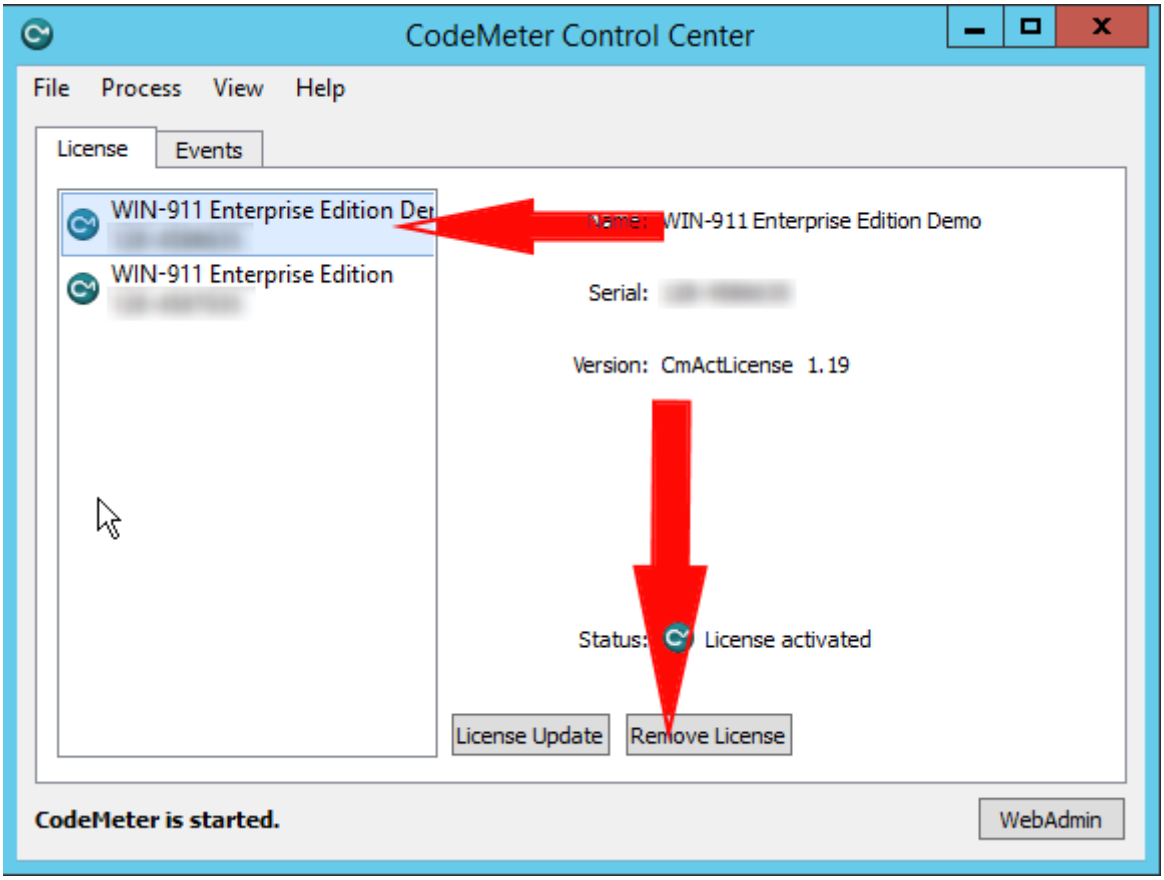
Email the license request file to license@win911.com or submit via website.

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".



Upgrading from a version prior to 2.16.1

WIN-911 v.2.16.1 introduces a new licensing schema that is incompatible with licenses issued for prior versions. If you have a license version previous to 2.16.1, you will need to request a new license before you can install the upgrade.

Affected Versions

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

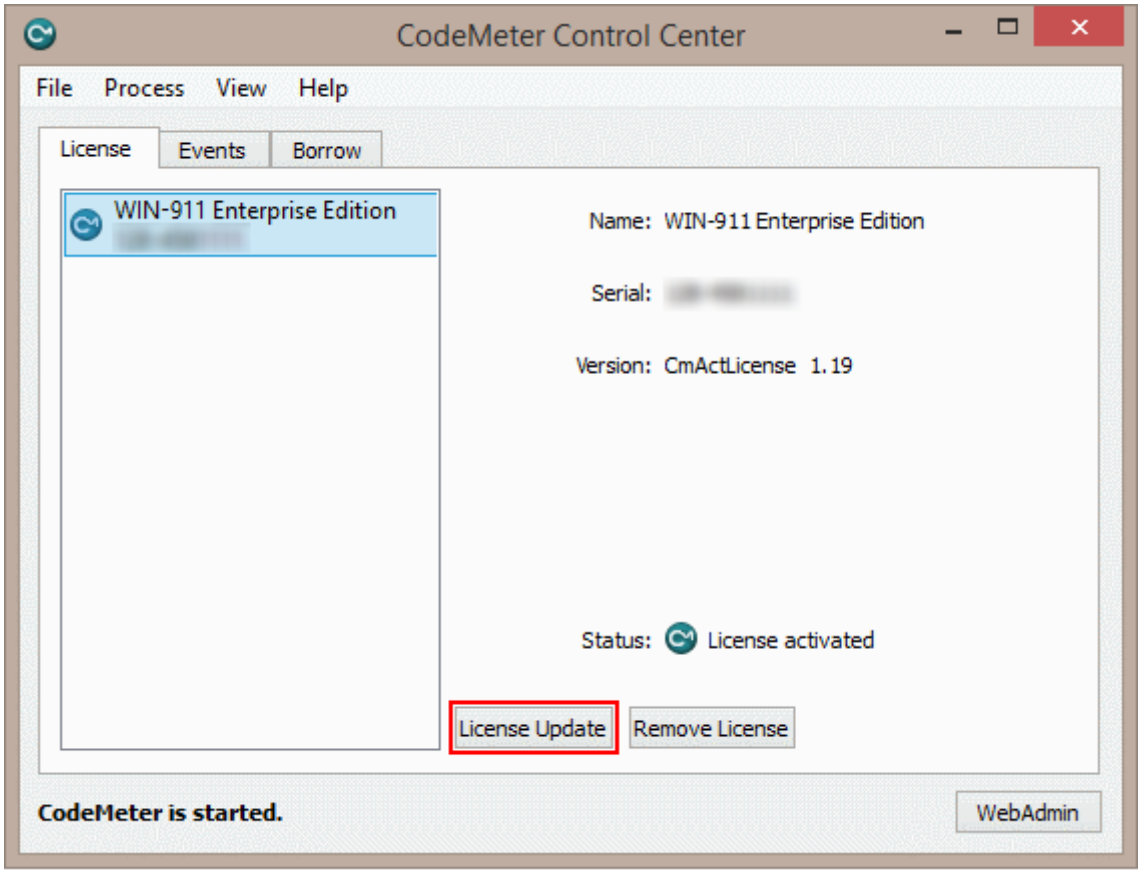
Re-licensing

Requesting a New License for WIN-911 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**. If you did not purchase WIN-911 with the FactoryTalk Alarms and Events connection, jump to **Requesting a New License for WIN-911**.

****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 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 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**.



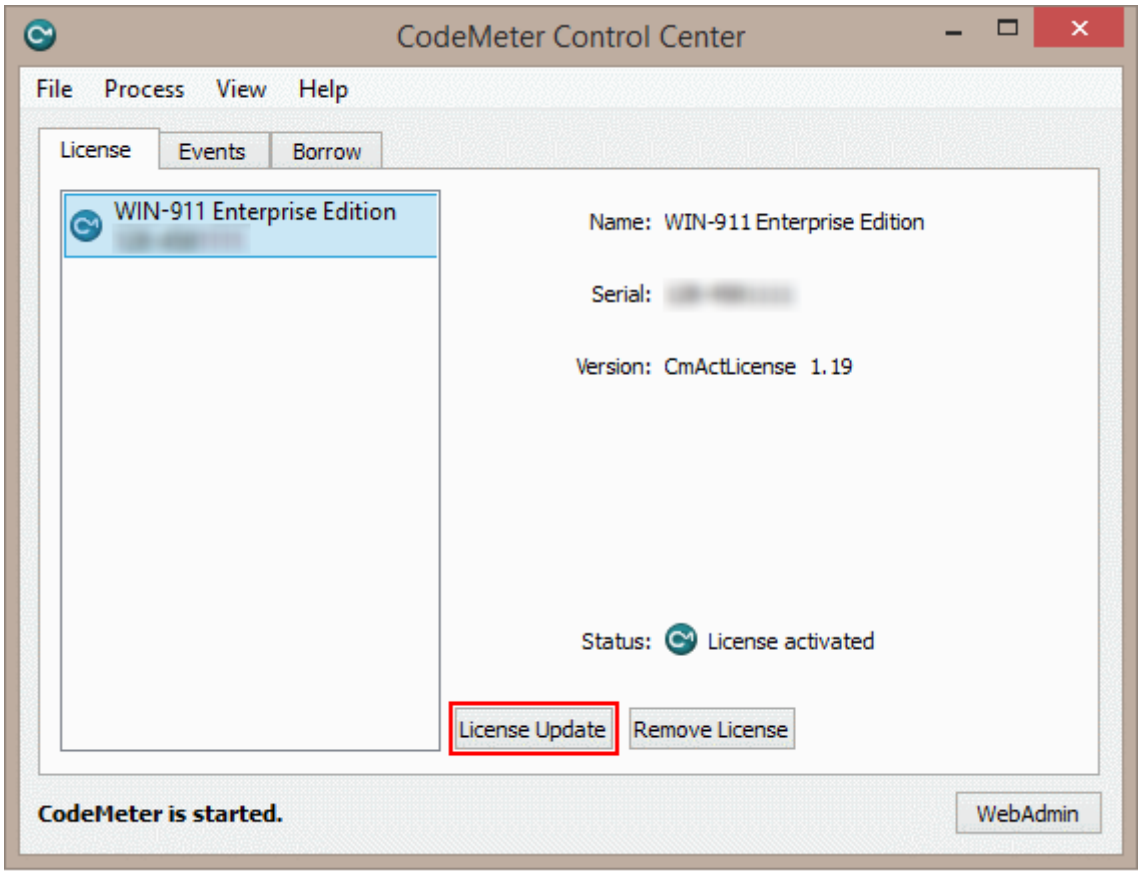
- The **CmFAS Assistant** wizard will appear. Select **Next >**
- Select **Create license request** and select **Next >**
- Choose where you would like to save the license request file and select **Commit.**
- Your license request file will be generated. Select **Finish** to close the wizard.
- Upload your license request file to **our licensing page**. You will need to enter your WIN-911 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

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

Note: If you have installed a previous version of WIN-911 and it was never licensed, you will need to contact us to request a new demo license before installing v.3.17.5.

- 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.

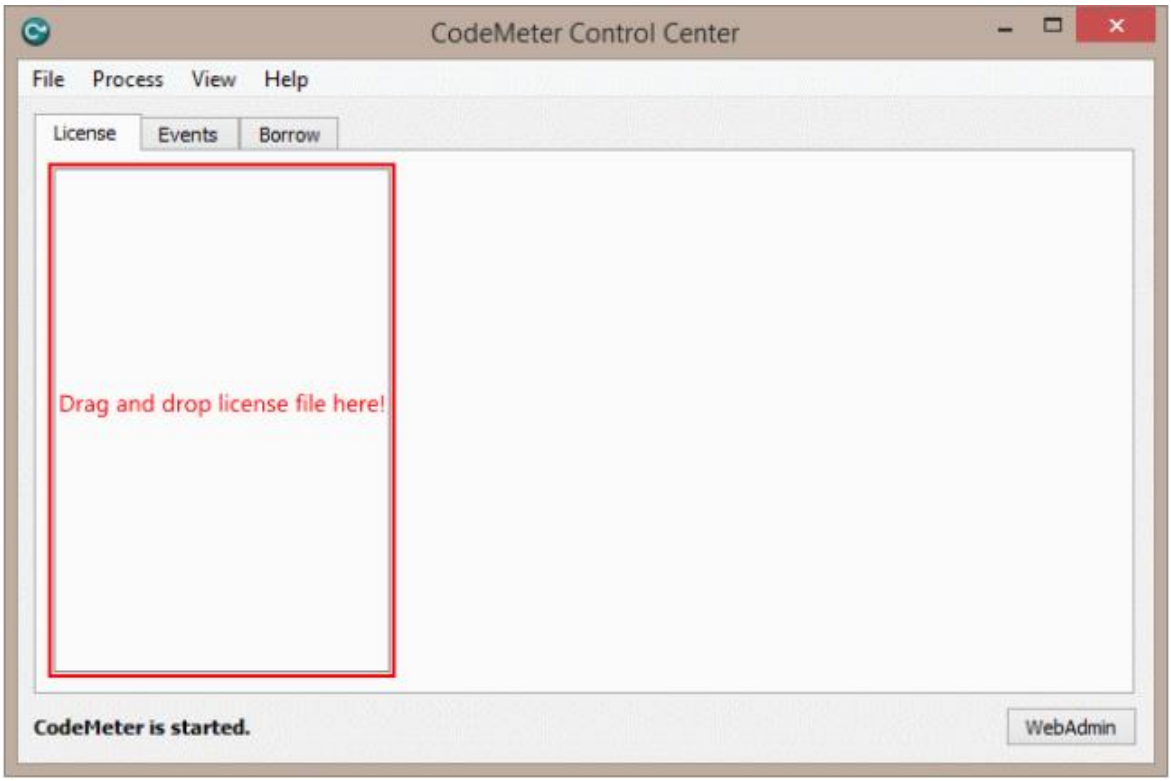


- The CmFAS Assistant wizard will appear. Select Next >
- Select Create license request and select Next >.
- Choose where you would like to save the license request file and select Commit.
- Your license request file will be generated. Select Finish to close the wizard.

- Upload your license request file to our licensing page. You will need to enter your WIN-911 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 3.17.5 and newer versions

WIN-911 Overview

WIN-911 provides an innovation to alarm notification products and methods. With these new concepts, complex alarm notification rules can be easily rendered, significantly reducing development, deployment, and maintenance efforts. WIN-911 Software introduces a novel flow chart-style graphical interface to easily set up notification "Strategies" and "Tactics." Appropriate strategies are triggered by events such as an alarm state (for example, a new alarm condition or alarm that has recurred within a defined amount of time, etc.), and in response the strategy invokes a set of instructions (tactics) based on the policies developed by the WIN-911 administrator. Each tactic can contain multiple instructions, and can even contain other tactics (which are referred to as sub-tactics). The method of assembling remote alarm notification scenarios afforded by WIN-911 is substantially easier to build, understand, visualize, and modify than other currently available products.

Figure 1

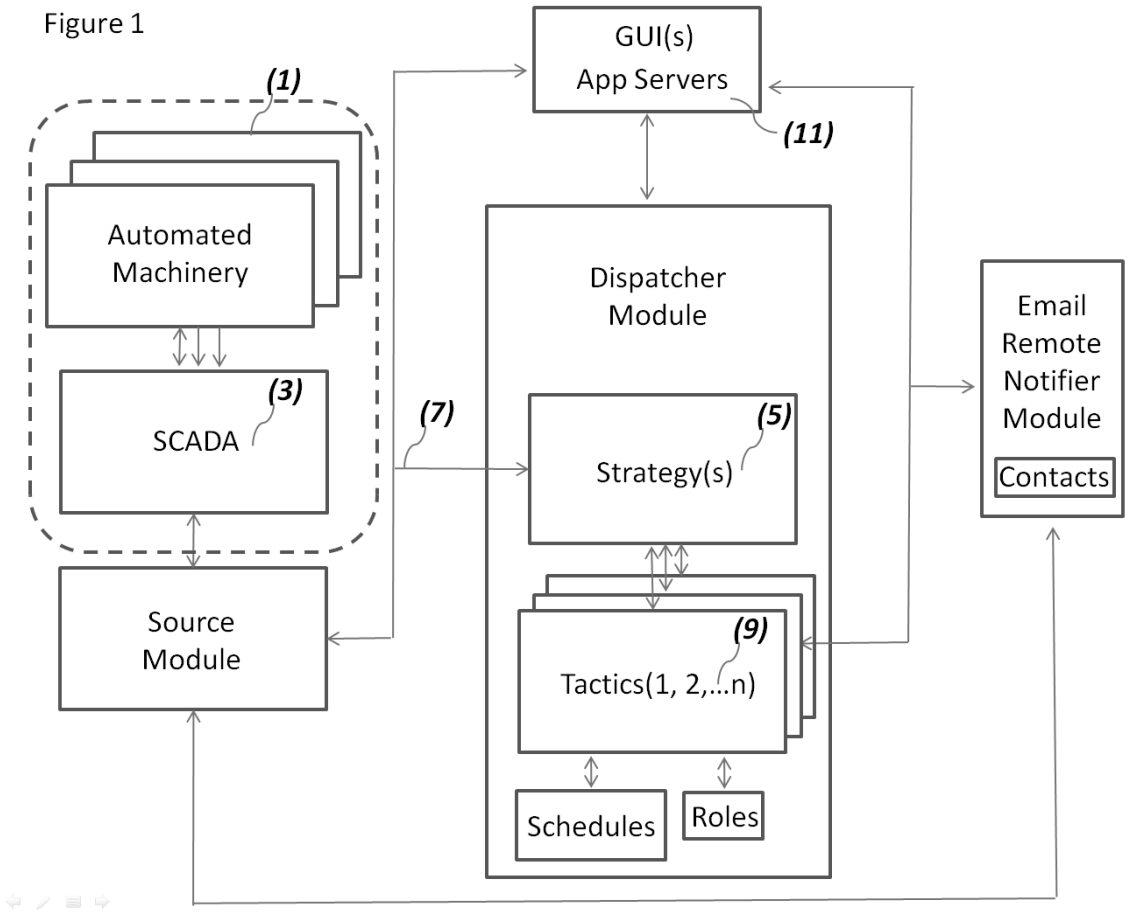


Figure 1 is a conceptual drawing that shows both the environment of WIN-911 Version 8 and its main components. The typical environment will be a plant or factory controlled by automated machinery (1) embodying programmable logic controllers (PLCs) or the like. Such machinery will typically be integrated into a SCADA network (3) hosted by operating systems that will likewise host WIN-911. The automated machinery uploads its data to the SCADA Network which centralizes that data in a well-known manner and makes it available to other applications and services running within the operating systems. WIN-911 may comprise user-defined modules that query data from the SCADA network and invoke strategies that receive alarm events and queue tactics that conduct remote notification procedures. A configuration can contain an unlimited number of strategies (5). Based upon a derived alarm event (7) each strategy can then invoke

any number of user defined tactics (9). Each tactic may comprise a logical series of tasks that handle alarm event messaging based on predetermined conditions and user input. The tasks are configured by utilizing a set of instructions that are subdivided into notifications, decisions and miscellaneous. A tactic can likewise invoke other tactics, which are called sub-tactics. When the tactics are complete or the alarm event terminates, the tactics and strategies end.

WIN-911's architecture is distributed between software modules that seamlessly interact with each other. Each module consists of three primary components which include an application server and GUI that runs within Microsoft's Internet Information Services (IIS) (11). This allows the invention to be programmed and monitored through internal password protected URLs that can be accessed by any computer in the network. The third component is the runtime executable that runs in the Operating System's Services. The module manifest includes the dispatcher, data source, Email notifier, and report modules, which are detailed below.

Dispatcher

The Dispatcher module is the primary component of WIN-911's infrastructure. It maintains the execution of all strategies and tactics; receives and implements programming from the GUI whenever a schedule, strategy, tactic, or role edit is saved, and directs notifier modules during runtime operations.

Data Source

The data source module communicates directly with the SCADA network and receives alarm event data which it distributes to the Dispatcher and the GUI. It receives and implements programming from the GUI whenever an edit is saved and works in conjunction with

the GUI to conduct alarm database imports. The module subscribes to alarm services provided by the SCADA and validates the data's integrity and security. It also receives alarm acknowledgement messages from the Email notifier modules which it delivers to the SCADA and receives acknowledgement confirmation messages which it routes to the controlling strategy.

Notifier

Notifier modules receives remote notification tasking from tactics running in the Dispatcher, subscribes as a client to the configured gateway server, and contains the contact connection and gateway data entered from the GUI. It receives and implements programming from the GUI whenever an edit is saved. It utilizes the configured notification protocols to deliver alarm messages, receives responses from the alarm-responder with alarm acknowledgement requests and report requests which it relays to the data source module for processing by the SCADA.

Reporting

The Reporting module receives report tasking from tactics running in the Dispatcher Module and interfaces directly with the data source and notifier modules to conduct reporting as required by a tactic or an alarm-responders request. The Reporting module receives and implements programming from the GUI whenever an edit is saved.

Figure 2

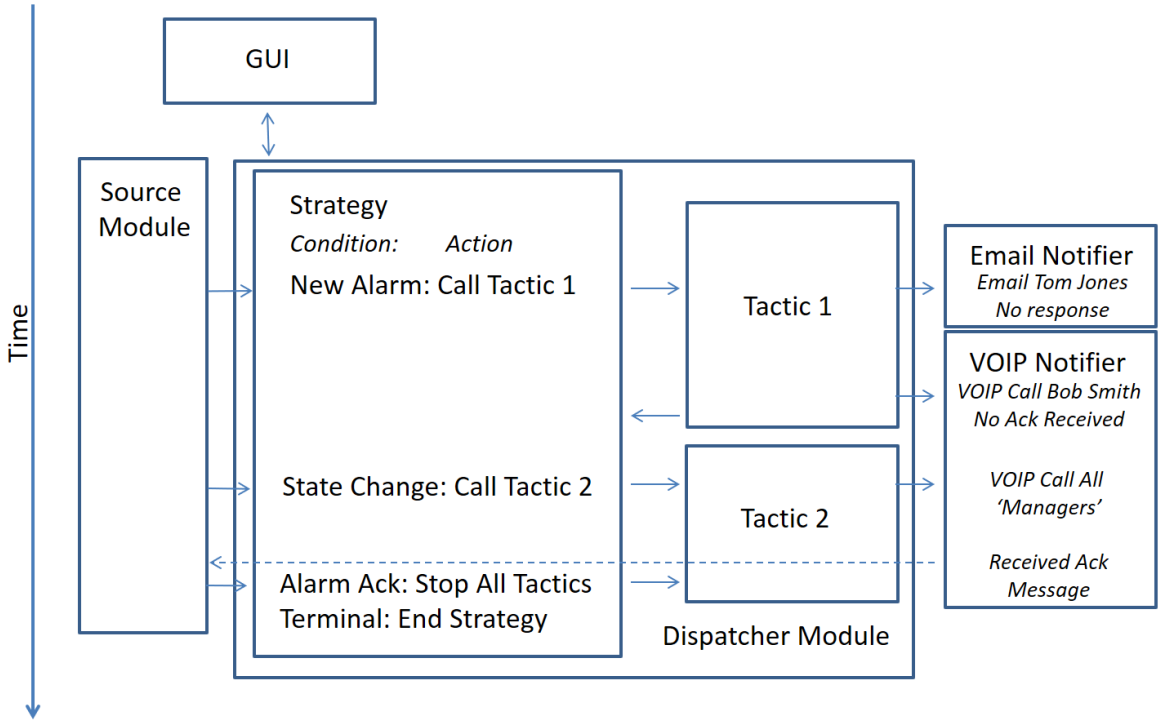


Figure 2 shows a hypothetical time-based series of events that demonstrate the interaction of the modules during runtime. This figure highlights how strategies and tactics share information in order to execute remote notification rules during the life of an alarm event.

The scenario begins when the WIN-911 administrator assigns an alarm event to the strategy he/she developed in the GUI.

Sometime after the configuration goes live the source module delivers an alarm event message that it received from the SCADA and routes it to the associated strategy within the Dispatcher module.

The strategy processes the alarm event condition according to its policy and calls Tactic 1.

Tactic 1 immediately instructs the Email Notifier to send an alarm message to Tom Jones and waits the configured amount of time for a response from Tom.

After the elapsed time expires, Tactic 1 again instructs the Email Notifier to call Bob Jones and deliver the alarm event message and process Bob's response, if any. In the scenario, Bob declines to acknowledge the alarm and Tactic 1 informs the strategy and terminates.

Sometime later the source module receives an updated message from the SCADA that the alarm event has escalated and routes the update to the Strategy. The escalation event takes the form of a state change and the stategy's state change policy calls Tactic 2.

Tactic 2 instructs the Email notifier module to broadcast an asynchronous batch of Email messages to all Email connections designated with "Manager" roles. One of them responds with an acknowledgement code which the Email notifier relays to the source module and subsequently delivers acknowledgement request to the SCADA.

The SCADA accepts the acknowledgement and informs the source module. The source module routes the acknowledgement confirmation to the strategy which stops all tactics in progress in accordance with its alarm acknowledgement policy and then terminates the strategy.

Overview of Tactics and Strategies

Tactics are smart notification lists that determine who gets notified and in what order. Strategies receive alarm events and invoke tactics in response. As the state of the alarm changes the strategy updates the tactic by stopping it, restarting it, or invoking an entirely different

tactic. When the alarm state becomes terminal (inactive and acknowledged) the strategy concludes by ending all associated tactics. So, tactics determine who gets notified, and strategies determine when.

Two kinds of tactics are available for the WIN-911 user: 1) Basic and 2) Advanced. The basic tactic (Figure 3) is a simplified, straightforward callout list that operates in a synchronous fashion using configurable delays to stagger the callout progression. Advanced tactics (Figure 4) utilize a highly configurable notification flowchart that give the user the ability to render complex escalation rules in an intuitive visual format.

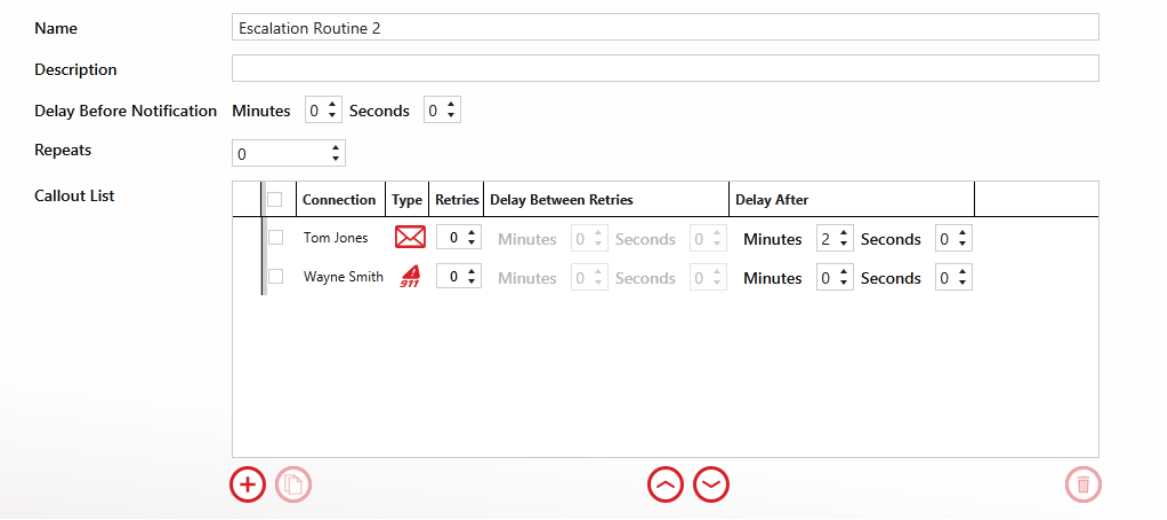


Figure 3: Basic Tactic

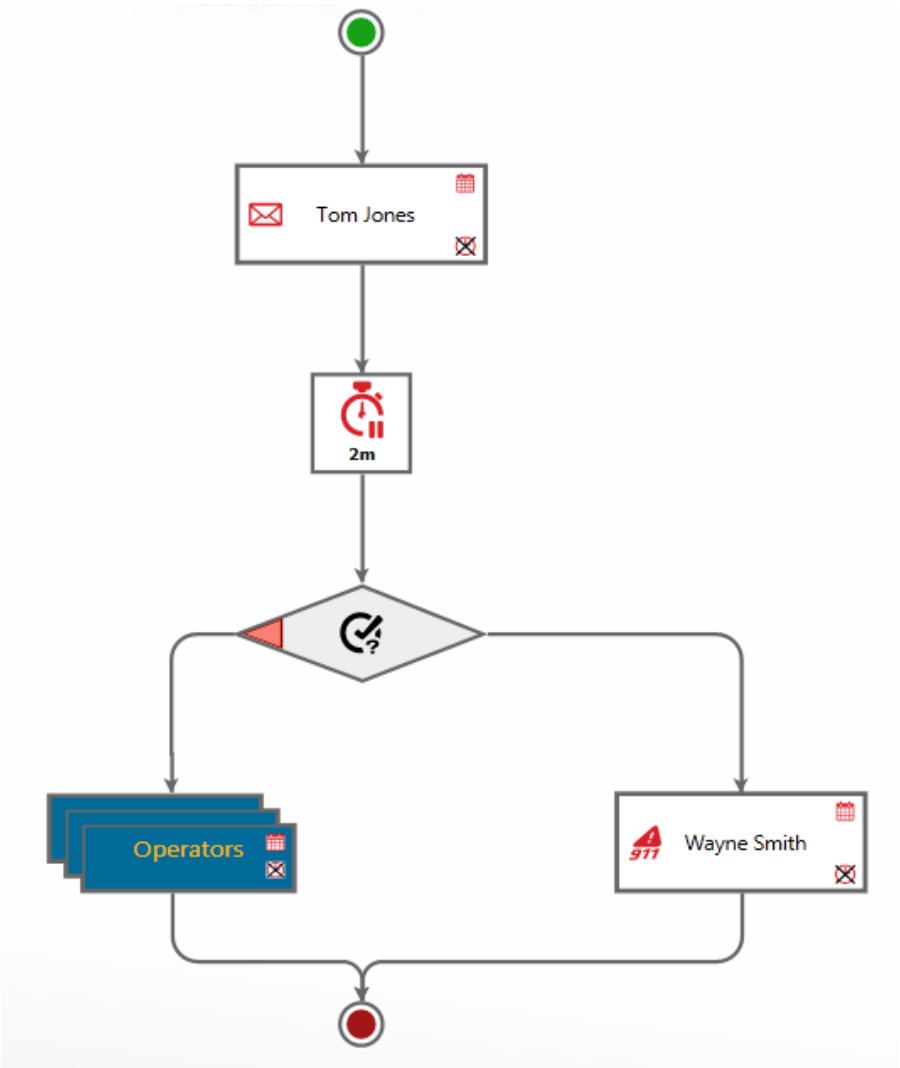


Figure 4: Advanced Tactic

Strategies are composed of policy statements that specify a condition and a subsequent action. For example: a policy could state that when an initial alarm event occurs a particular tactic is to be invoke to dispatch alarm notifications. The condition would be the initial alarm event and the action would be to start tactic X.

In its simplest form (Figure 5), a strategy will contain three policy statements, 1) an initial condition -> start tactic x, 2) on a change of state -> renotify, and 3) on termination of the alarm event -> Stop Strategy. An unlimited number of policy statements (Figure6) can be used by clicking the Advanced Mode button.

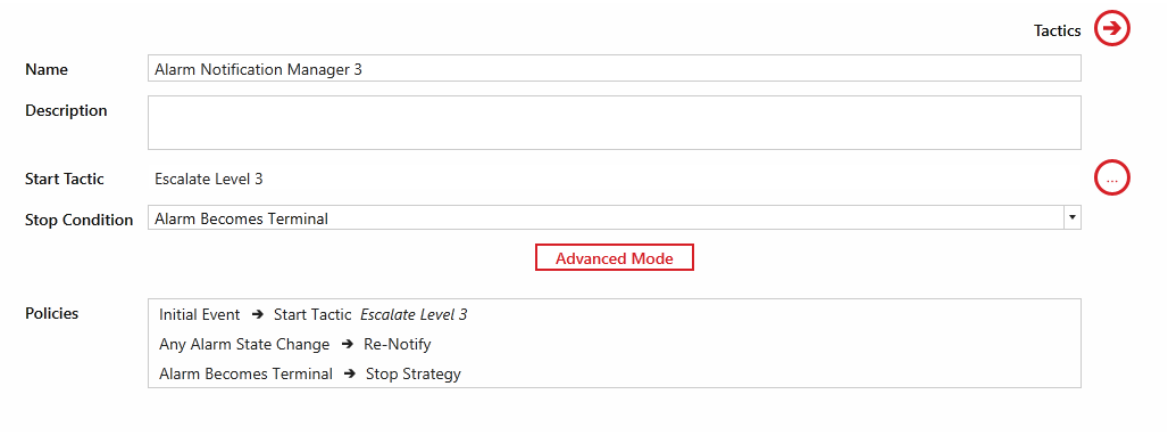


Figure 5: Strategy

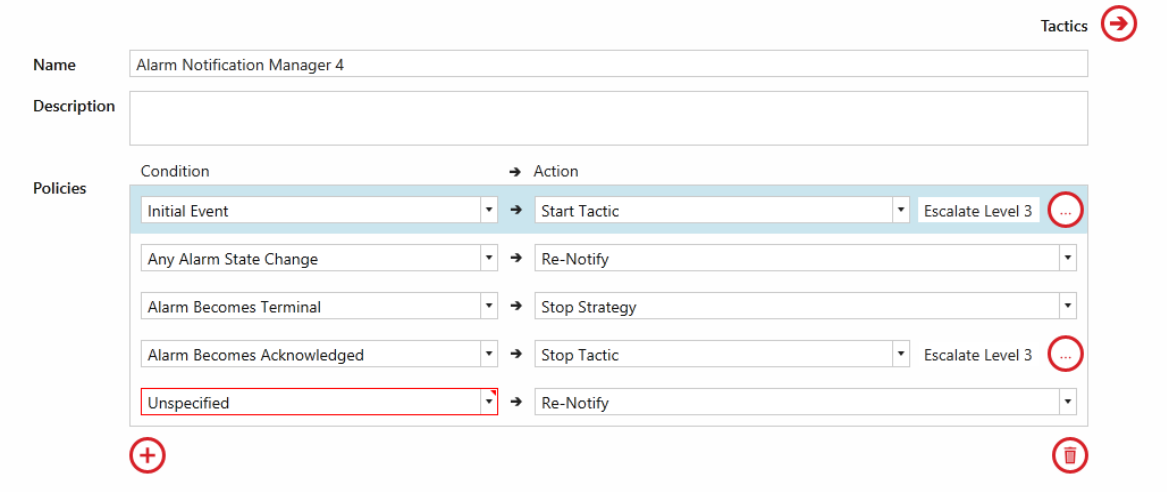
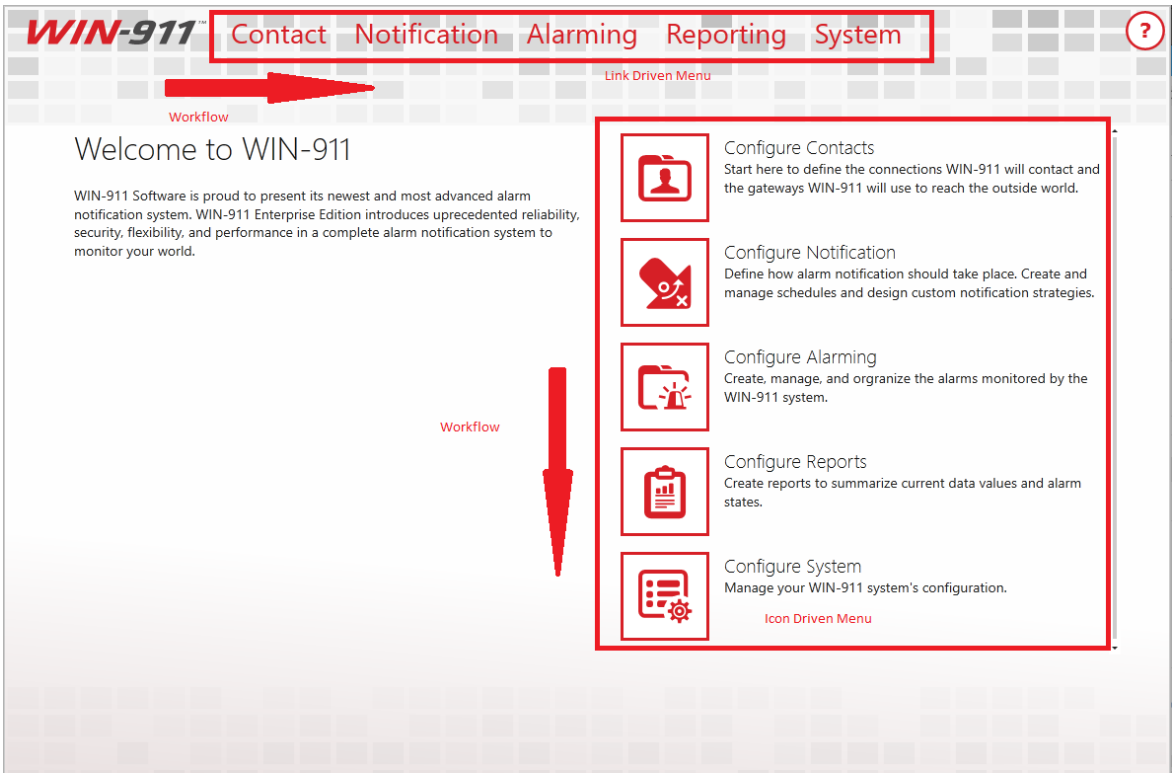


Figure 6: Advanced Mode Strategy

WIN-911 Graphical User Interface Basics

WIN-911 introduces a website driven GUI that can be accessed anywhere on the network. This frees the user to configure WIN-911 from any computer on site after providing the proper credentials.



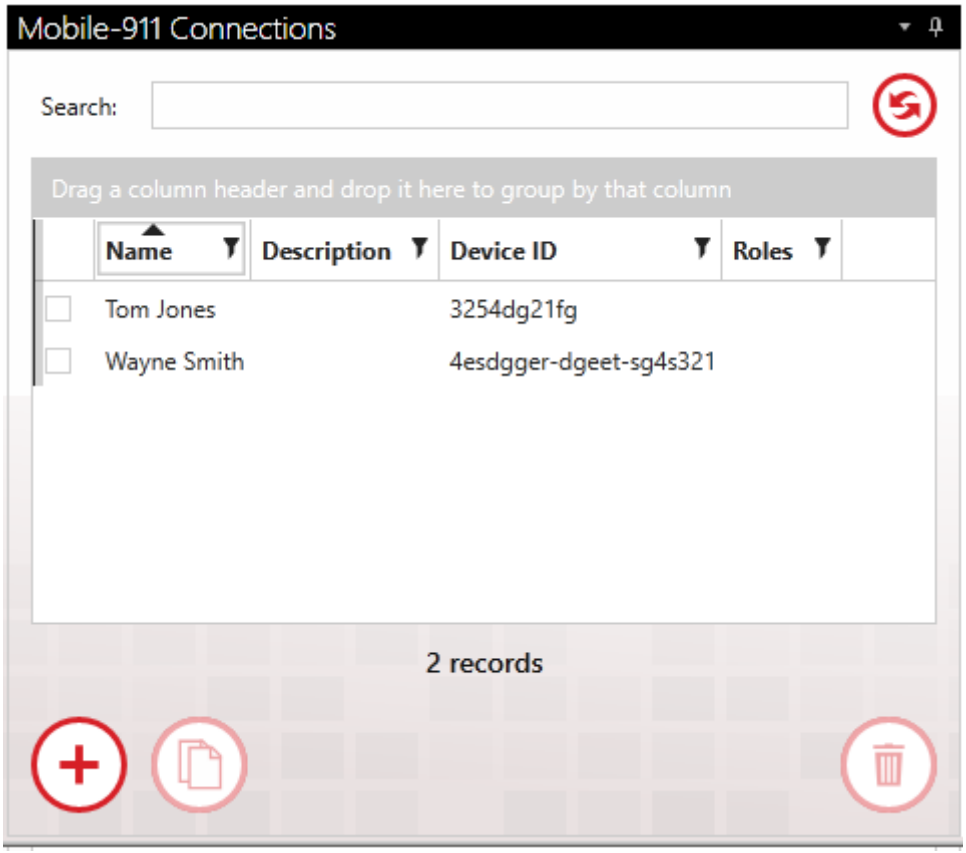
The GUI is logically designed to follow a left-to-right (and top to bottom) configuration workflow that is largely self-documenting. Across the top is a link-driven menu the provides navigation to all the WIN-911 workspaces. The large icon menu located in the center of the welcome page is the more verbose workspace and leads the user through the configuration process with little need to refer to user documentation. In the event that more information is required a help icon ⓘ can be found on the upper right corner.

Connections Selector List

On the left side of any workspace that exposes multiple objects for editing is a collections selector list. Each list is equipped with powerful tools for sorting, filtering and grouping the objects based on their properties. The active sorting column is indicated by a black triangle

in the middle of the column heading. Active filtering is indicated by a yellow column header.

In the example below the Mobile-911 Connections list is shown.



Selecting a connection to edit: An individual connection is selected by clicking the check box to the left of the connection's properties. Only one connection can be selected at a time.

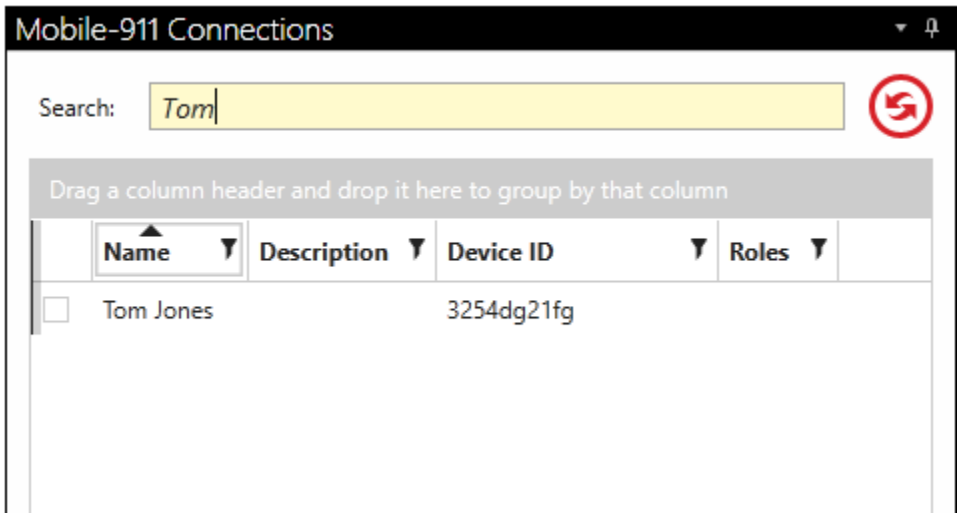
Sorting

When the name column has a black triangle pointing down, the Mobile-911 connections will be arranged by name in descending alphabetical order. Clicking on the triangle will reverse the list and cause it to be arranged in ascending order. A third click on the

triangle will deselect the column. Any property column can be sorted.

Search

The search field will filter the Mobile-911 connections collection selector list by suppressing the display of Mobile-911 connections that do not contain the character string entered. Any property column can be searched. The search field will be highlighted yellow while the search filter is in session. The refresh button to the right.



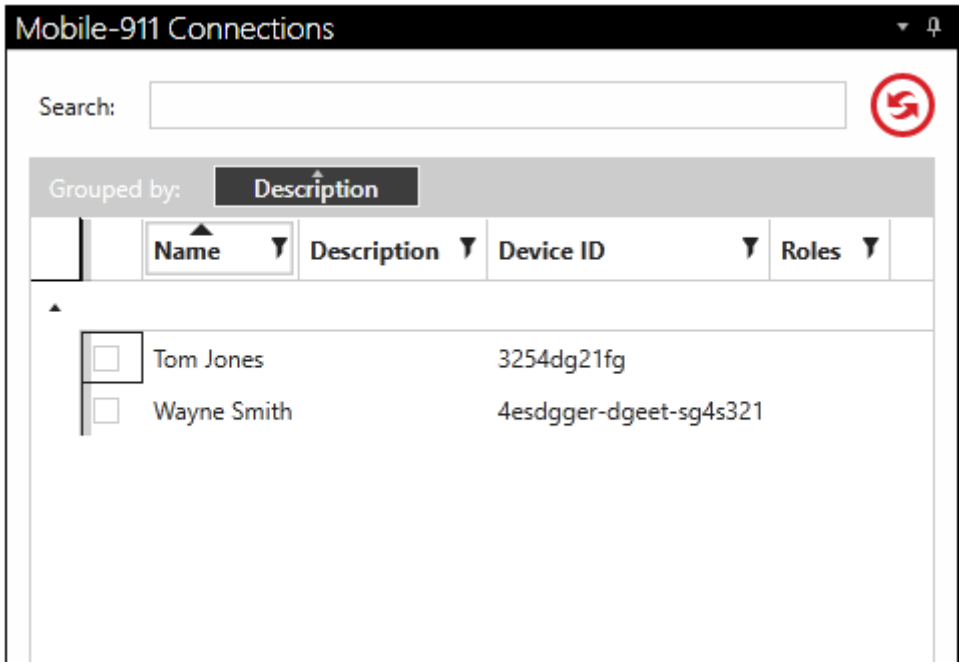
Filtering

On the right side of the property column heading is a black filter symbol. Clicking it brings up a custom filter design form. This form provides several options the WIN-911 administrator can use to exclude unwanted Mobile-911 connections from being listed in the collection selector. "And/Or" expressions can be created that key on the selected property data for inclusion or exclusion. A filter can be configured for any property column. The selected property (Name or Description) column header will be highlighted yellow while the custom filter is

applied. If more than one column has filters applied, each will be highlighted.

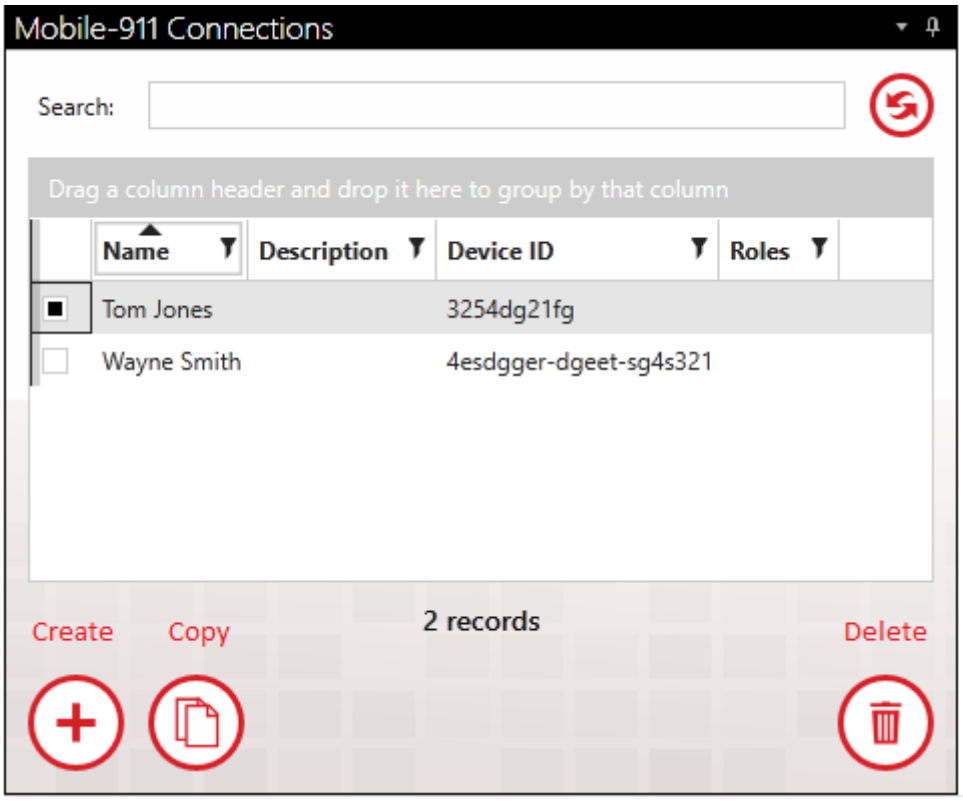
Grouping

Dragging and dropping a property column header into the grey area above the Mobile-911 connections list will cause the collection selector to group the Mobile-911 connections accordingly. The collection selector now lists the title of the selected object in bold font with a drop-down arrow to the left. Click on the drop-down arrow and the collection selector will drop a list of all the Mobile-911 connections that contain a particular object title. Groups can be compounded by dragging another object into the "Group by" field. Grouping can be removed by hovering over the group title and clicking the "X" that appears to the right of the title. Any property can be grouped.



Create/Copy/Delete

Select an object by clicking on the selection tick-box to the left of the object name. This will enable the Create, Copy, and Delete buttons on the bottom list. With them you can make copies of objects, create new ones and delete existing objects.



Example: Configuring an Advanced Tactic

Design advanced tactics by clicking the navigation links */notification/tactics/advanced tactics/*. Click the *add-create* icon *(+)* at the bottom right of the tactics list to bring up a blank advanced tactic workspace in edit mode (Figure 7). Enter a unique name for the tactic

and give it a brief description in the fields provided. The blank tactic is represented by a green circular start node (where the tactic begins) and red end node (where the tactic concludes) and directional link lines that represent the flow of tasking. Entering

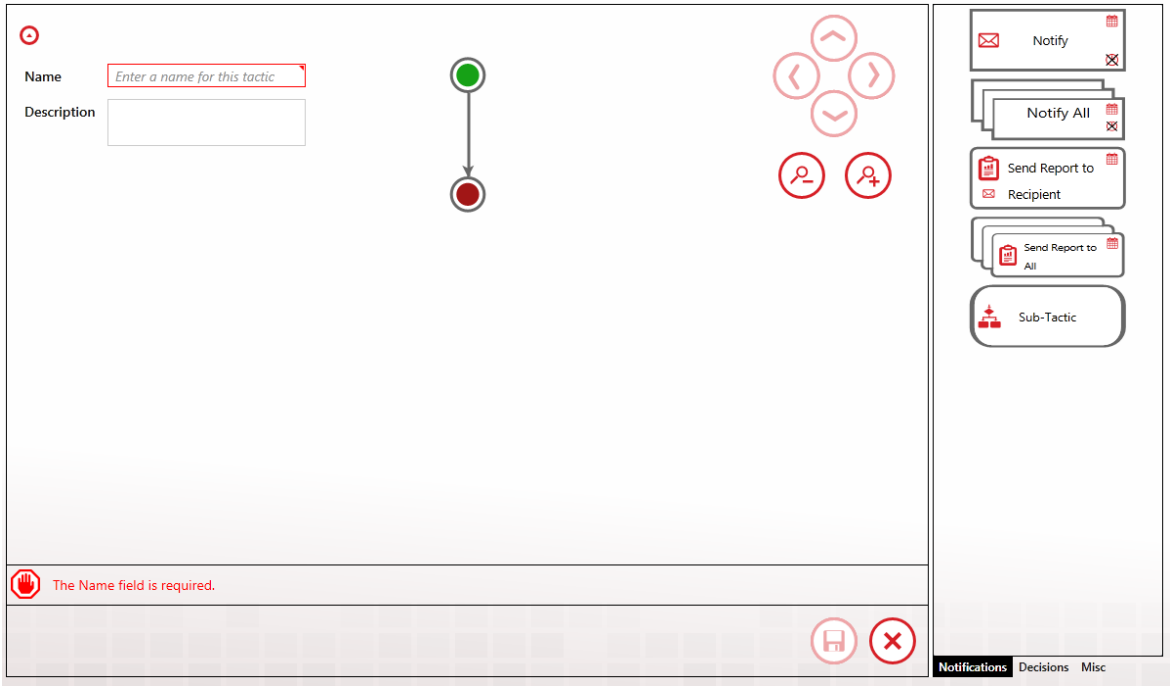


Figure 7: Blank Tactic Workspace

Drag and drop tactical instruction blocks from the right-hand pane (1) directly into the tactic design workspace (2). Blocks are chosen from the three categories Notification, Decision, and Miscellaneous. Position the block by dropping it on the link in the place where you want the block to execute (Figure 8).

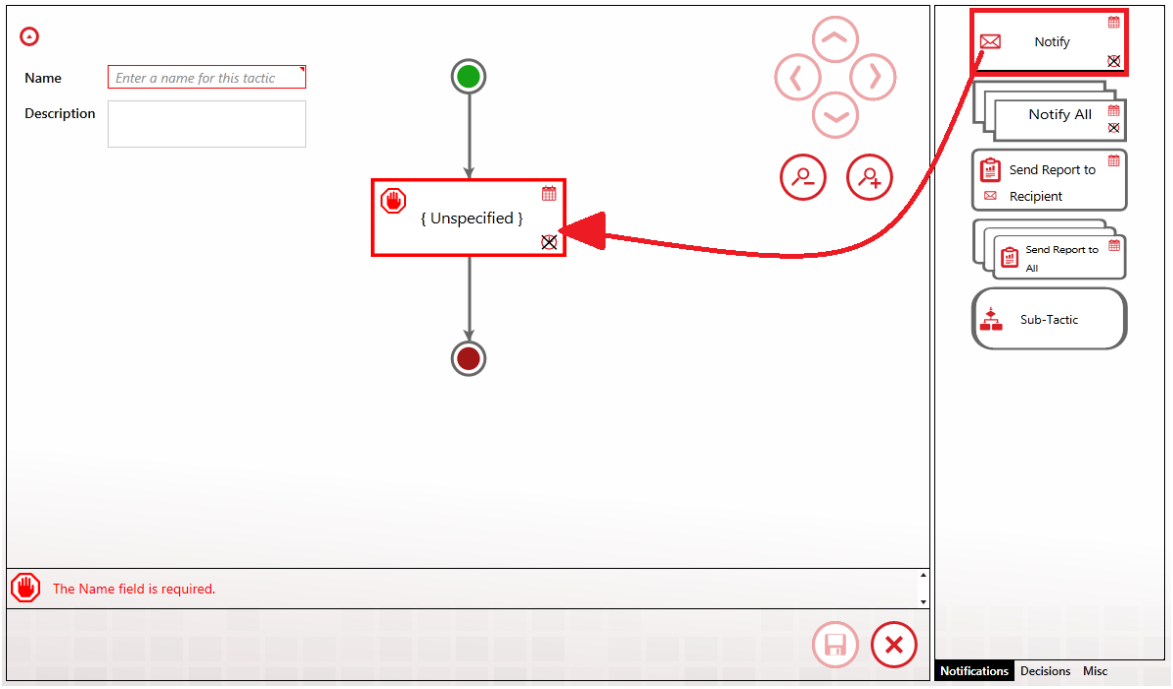


Figure 8: Placing Notification Block in Tactic

One the notification block is in place, double-click over the center (Unspecified) of the block with your mouse to open the edit option selection box. Click  to enter the edit dialog.

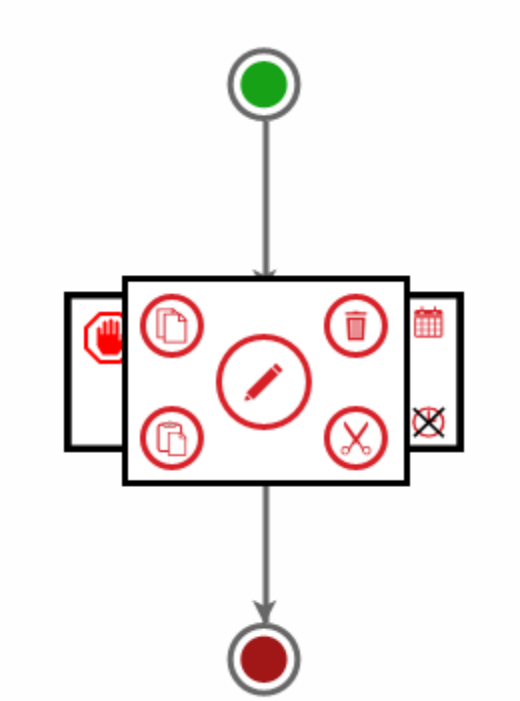


Figure 9: Entering Notification Block

The Edit Properties box will populate the connections list with all of the connections in your Contact database. Select the one you want to remotely notify and then close the properties box by clicking

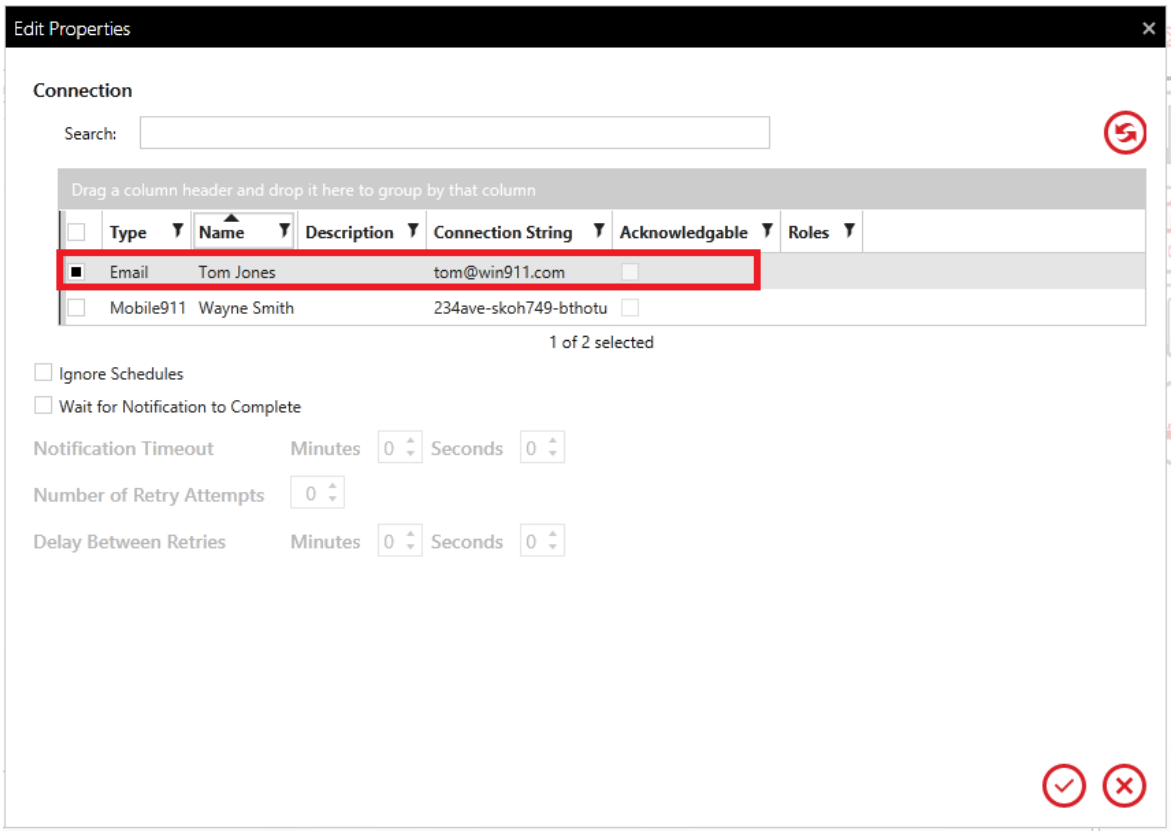


Figure 10: Edit Properties of Notification Block

Once the edit is complete the tactic will appear (Figure 11) with the Notification block appearing with the selected connection named and type of connection shown by the red icon on the left (in this example Tom Jones is an Email connection).

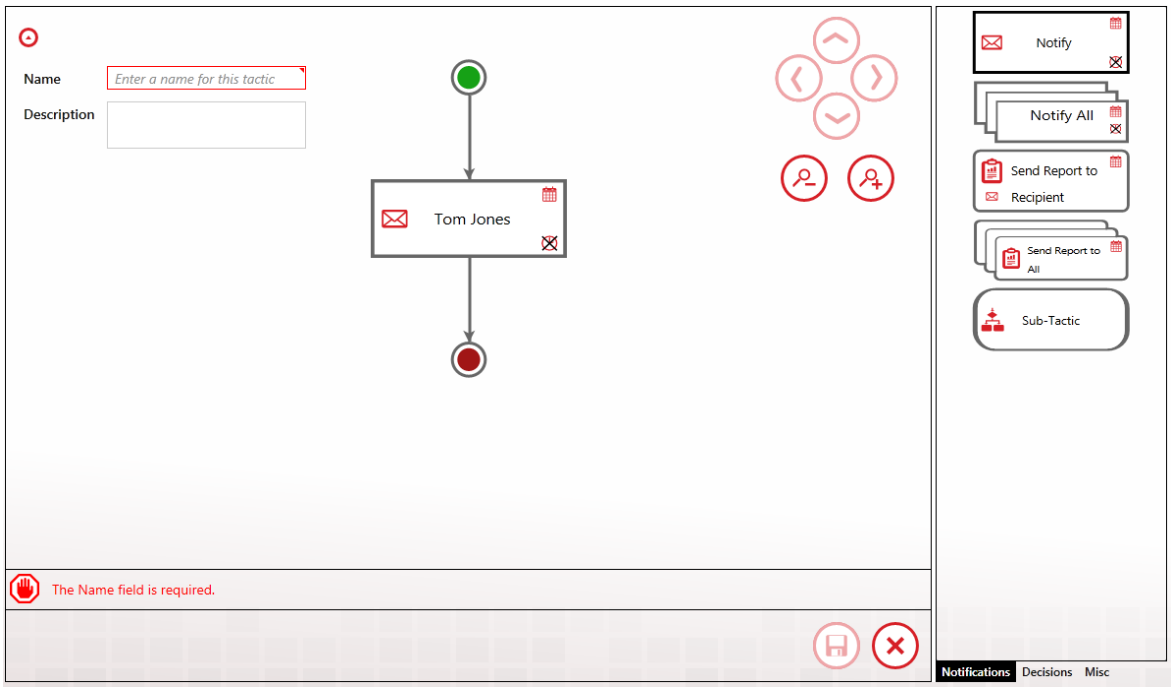


Figure 11: Complete Edit of Notification Block

To add a delay (Figure 12) between Tom Jones notification and the next task, click the Misc tab (1) at the bottom right. The Misc panel with display and from that click and hold the Delay block (2) icon and drag-and-drop (3) it on the tactic beneath Tom's Notification block.

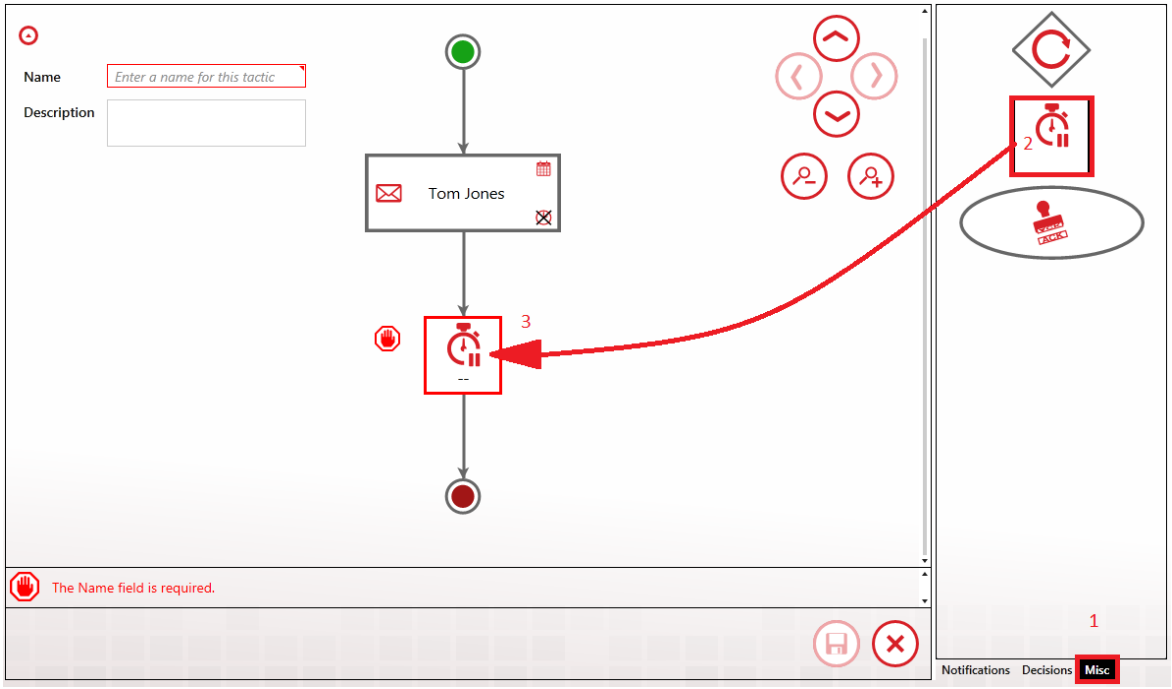


Figure 12: Adding Delay Block to Advanced Tactic

Double-click the center of the Delay block to open the Edit Properties dialog. From there, use the up-arrows in the Minutes combo-box to set the delay for 5 minutes. Click 

Figure 13: Editing Delay Block Properties

Next click the Decisions tab (1) and the Decisions selection panel appears. Drag-and-drop the Ack Decision block (2) on the tactic, beneath the Delay block (3). The left side of the Decision icon with the red tip points to the false path that the tactic will take of the alarm event is NOT acknowledged when the tactic reaches that point. If the alarm event IS acknowledged then the tactic will make a right turn and take the true path.

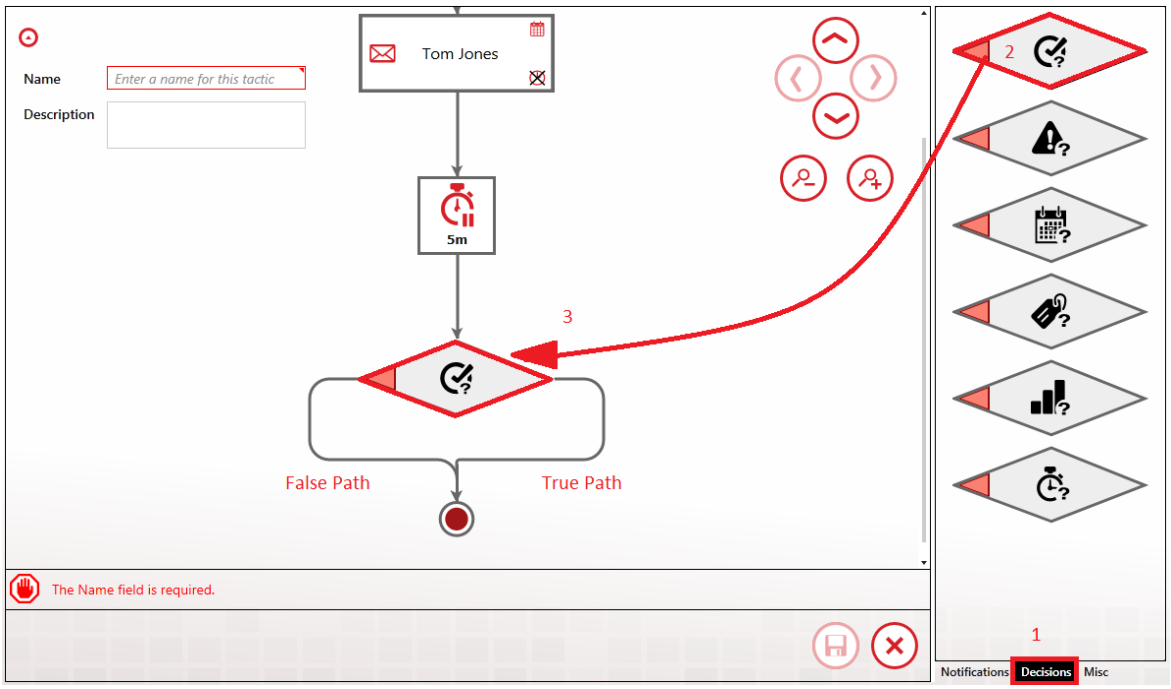


Figure 14: Adding Decision Block to Advanced Tactic

Lastly in this example, click the Notification tab (1) and the Notification panel reappears (Figure 15). Drag-and-drop the Notify All block (2) in the false path (3) of the Ack Decision block.

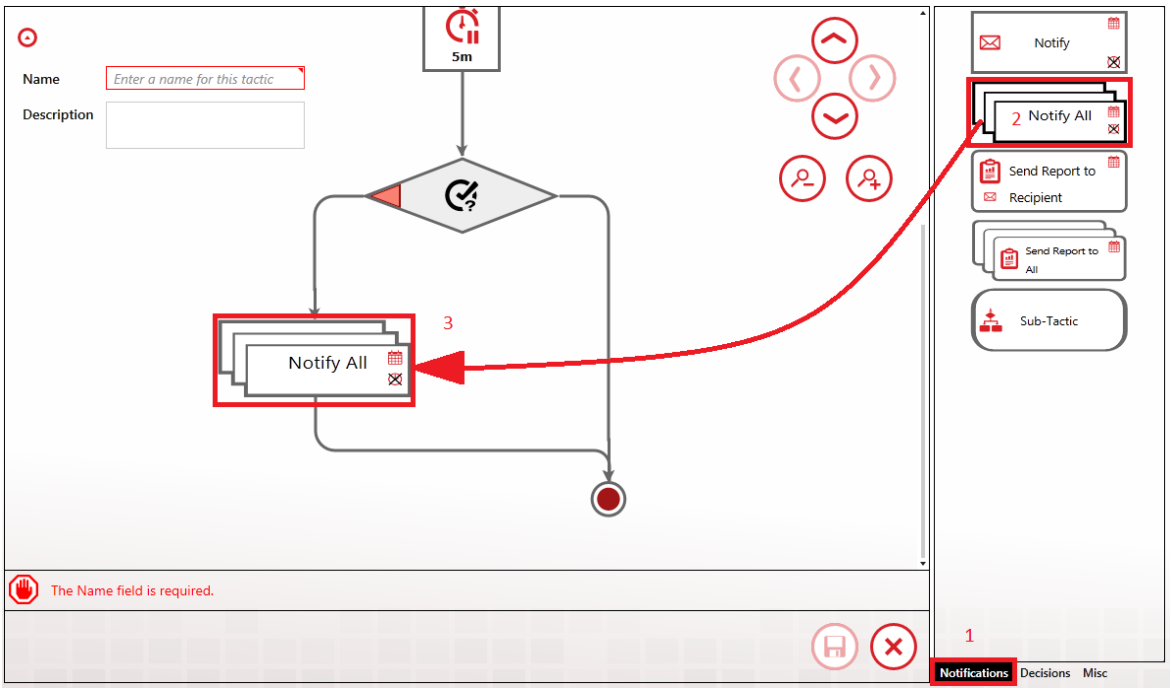


Figure 15: Adding Notify All to Decision Block

Edit the Notify All block by double-clicking the center of the icon. This will open the Edit Properties dialog (Figure 16) of the Notify All block. Select Operators Role and then click

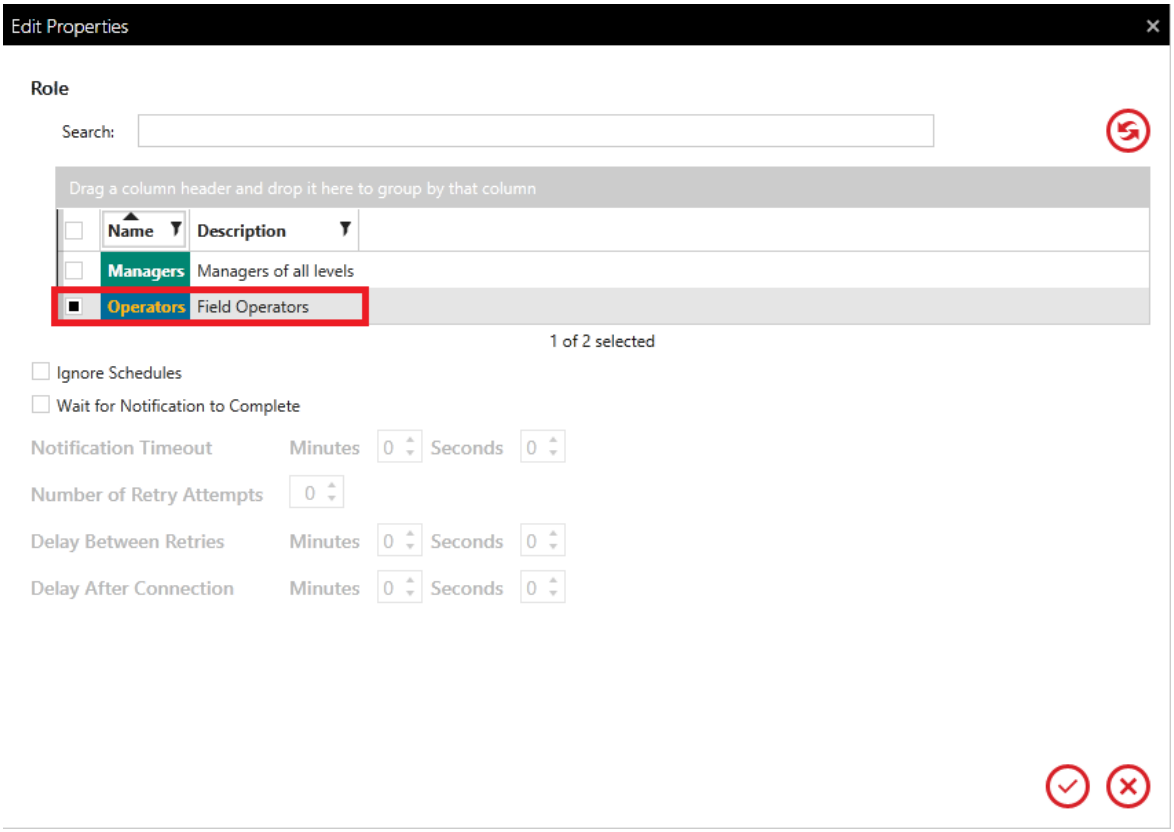


Figure 16: Notify All Edit Properties Dialog

The advanced tactic is now complete and ready to be saved (Figure 17), however, the button is disabled (1). The configuration information bar at the lower left (2) states that the tactic must be given a name before it can be saved. Enter a unique name in the Name field (3) and the save button will be enabled, allowing you to save the tactic for use in a strategy.

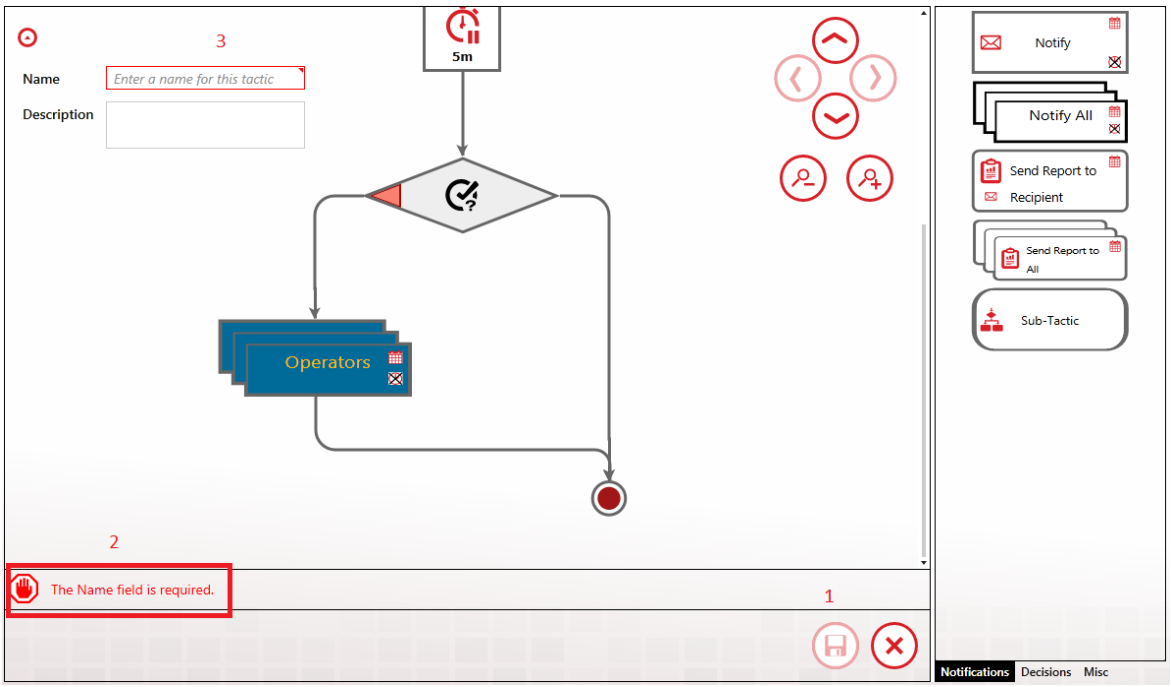


Figure 17: Tactic Complete

Tech Support

You can contact WIN-911 Tech Support at Support@WIN-911.com.

Contacts

The contact information, including Gateway Settings, Connections, Roles, and Schedules are specified in the Contact pages.

Start here to define the connections WIN-911 will contact and the gateways WIN-911 will use to reach the outside world.

Manage Email Settings

Email notification allows for one-way or two-way communications with any Email capable device. Messages may contain either rich HTML or plain text for compatibility with a wide range of devices.

Manage Mobile-911 Settings

Start here to define the connections WIN-911 will contact and the gateways WIN-911 will use to reach the outside world.

Manage Voice Settings

Voice notification allows for two-way communications with land-line, mobile, and soft phones using TAPI or VoIP technology.

Organize with Roles

Roles represent a label for organizing connections based on availability, location, or responsibility. Roles can be used in a

notification tactic to notify all connections with something in common.

Schedules

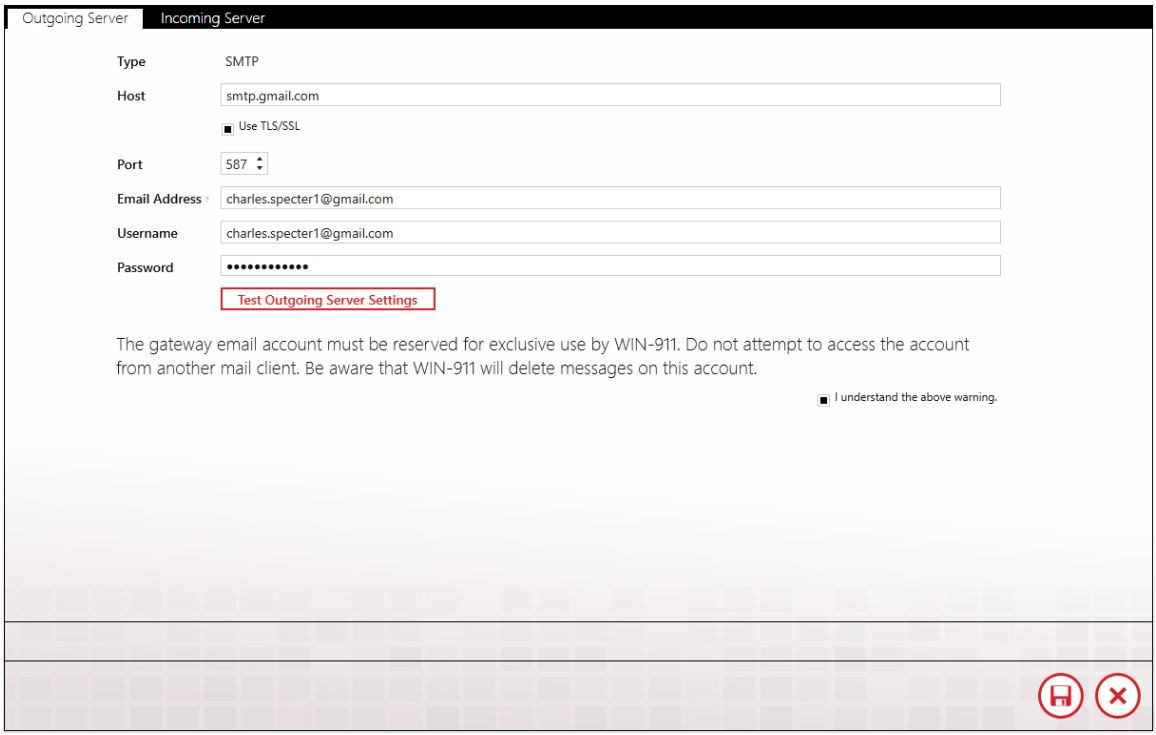
Schedules define the availability of connections and can be used in a notification tactic to control notifications.

Email Gateway

Define the settings required to connect to your local or Internet-based Email server.

- *All required settings are available from your Email administrator.*
- *WIN-911 is capable of using different servers for outgoing and incoming mail.*
- *WIN-911 requires a dedicated Email address due to the way it handles the inbox. Any messages left in the inbox will be deleted from the server by WIN-911 at runtime.*

Outgoing Server



Type

WIN-911 uses SMTP as the outgoing server protocol.

Host

Specify the server name or IP address of your outgoing Email server.

Use TLS/SSL

Check this box if the outgoing server WIN-911 will use requires encryption.

Port

Enter the port number that the WIN-911 Email server will use to send outgoing Email.

Email Address

Enter the *dedicated* Email address in the text entry box that WIN-911 will use to dispatch alarm and report messages, and receive acknowledgement and report requests.

Username and Password

Specify the credentials required by your server.

Test Outgoing Server Settings

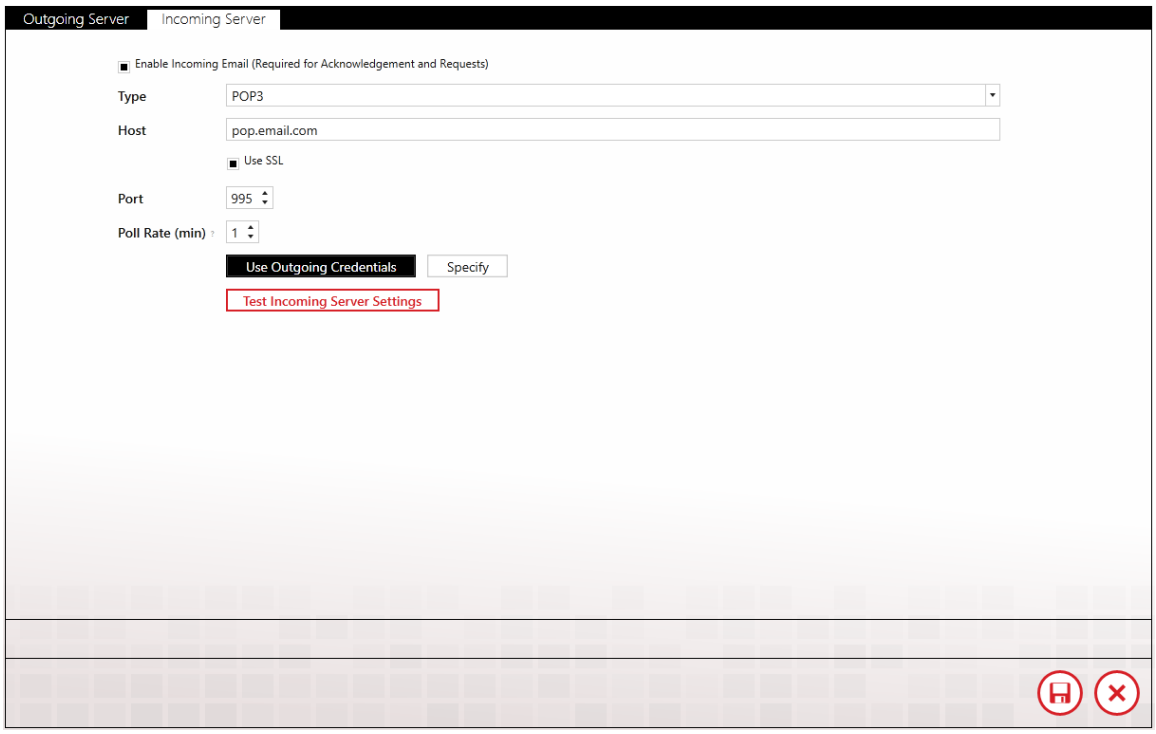
Click "Test Outgoing Server Settings" button to test WIN-911 ability to connect to the mail server and send messages. If the server values have been properly set, WIN-911 will display a "success" message. If the test fails, refer to the Windows Event Viewer for details concerning the error that occurred when the test was attempted and take corrective action.

Understanding required Warning Message

Note: Before the gateways settings can be saved, WIN-911 requires that you read the following warning and check the confirmation box to the lower right.

The gateway Email account must be reserved for exclusive use by WIN-911. Do not attempt to access the account from another Email client. Be aware that WIN-911 will delete messages on this account.

Incoming Server



The incoming server can use either the POP3 or IMAP protocol to receive incoming acknowledgement and report requests.

Enable Incoming Email (required for Acknowledgement and Report Requests)

Click this check box to configure WIN-911 to receive incoming mail.

Type

WIN-911 supports POP3 and IMAP as the incoming server protocol. The default protocol is POP3.

Host

Specify the server name or IP address of your incoming mail server.

Use SSL

Check this box if the incoming server requires encryption.

Port

Enter the port number that the WIN-911 Email server will use to receive incoming mail.

Poll Rate (min)

Enter frequency in minutes that WIN-911 will poll the server for incoming mail.

Use Outgoing Credentials or Specify

In the event that the mail server uses the same credentials for incoming mail as it does for outgoing, use the default setting of "Use Outgoing Credentials". Otherwise select "Specify" and enter the username and password required by the incoming server.

Test Incoming Server Settings

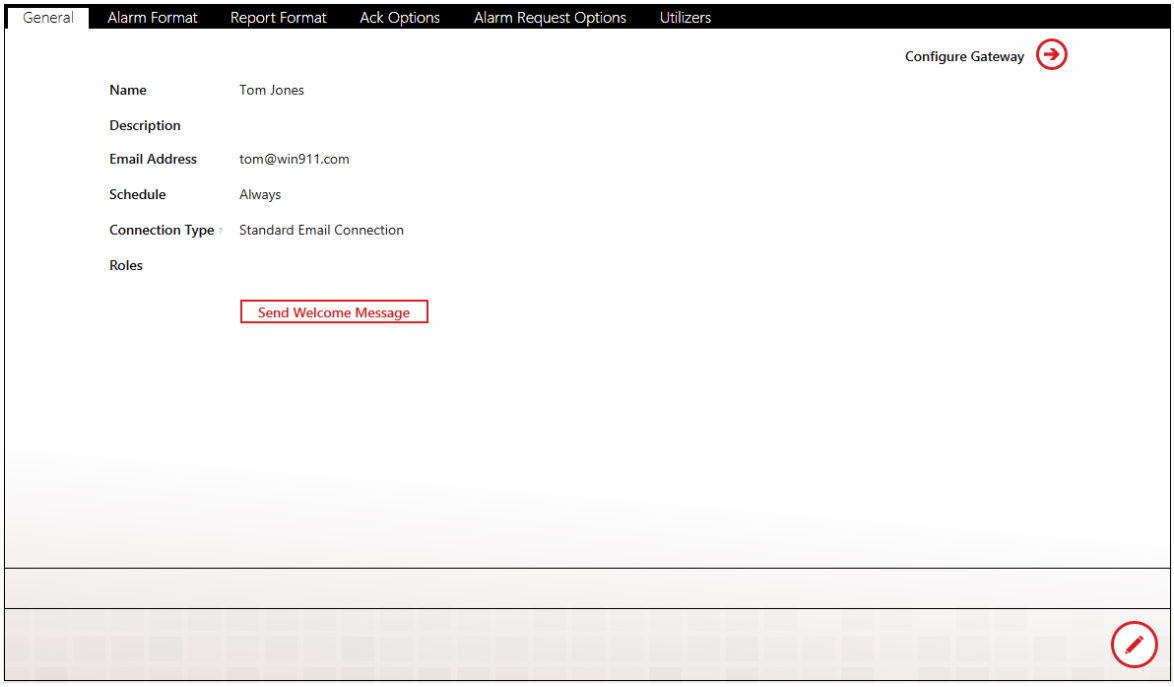
Click the "Test Incoming Server Settings" button to test WIN-911 ability to connect to the mail server and receive mail. If the server

values have been properly set, WIN-911 will display a "success" message.
If the test fails refer to the Windows Event Viewer for details concerning the error that occurred when the test was attempted and take corrective action.

Email Connections

Connections specify a destination for alarm notification reports. Email connections also determine just what you will see in alarm and report Email messages, connection availability and the permissions a connection has been granted concerning acknowledgement and report requests.

General



Name

Each Email connection must have a unique name that identifies the particular Email connection.

Description

An extra text field for organization and administration purposes, similar to a code comment.

Email Address

View or enter the Email address that WIN-911 will send assigned alarm and report messages to for this connection. It is acceptable to assign a unique Email address to multiple connections if your situation warrants such action; however, a warning message will be generated to inform the WIN-911 administrator that a pre-existing connection already uses this address and lists the number of times it has been used.

Schedule

View or select the schedule that WIN-911 will honor when sending alarm and report messages. A connection can have only one assigned schedule, but a schedule can contain multiple appointments. See Schedules.

Connection Type

Standard Email Connection

This connection type is for sending email messages that will be received as email.

User an Email to SMS Gateway

This connection type is for sending SMS messages to the alarm responder that originate from WIN-911 as an Email connections. This type requires a 3rd party Email to SMS proxy. Most wireless

service providers offer this service. The alarm responder can acknowledge the alarm by replying to the text using the ticket number and password, which is discussed in the Ack O

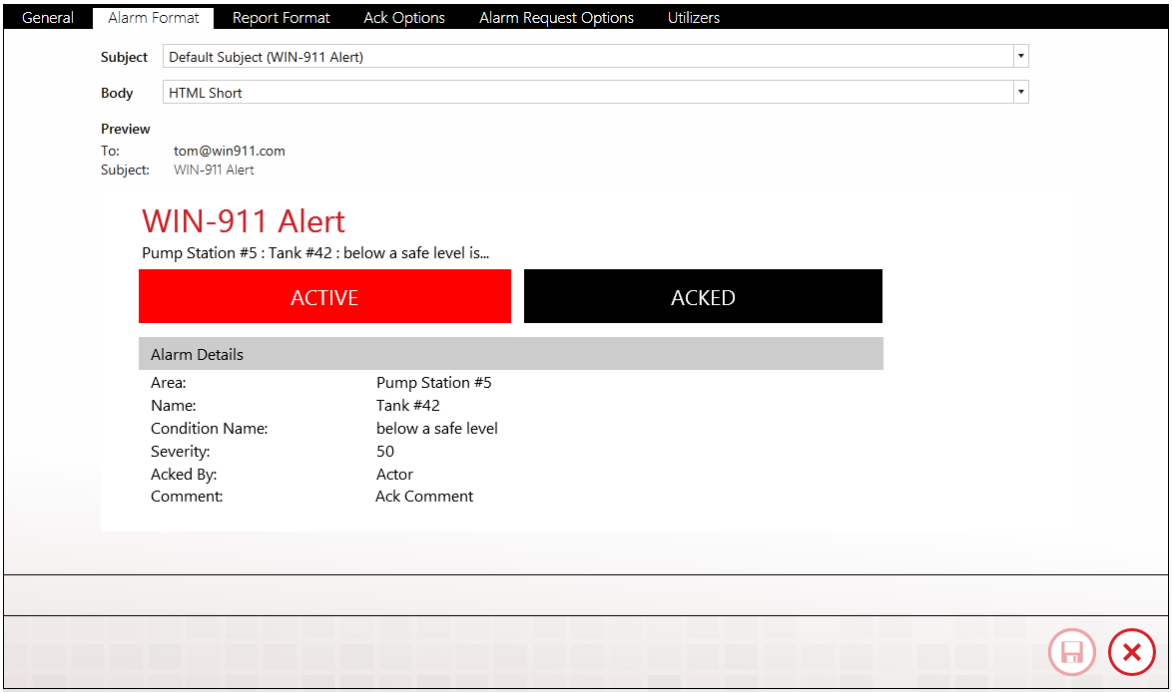
Roles (for use by Advanced Tactics)

View or assign roles to the selected connection by clicking the add button in edit mode. Each connection can have multiple roles. See Roles.

Send Welcome Message

Click the "Send" button in view or edit mode to send a WIN-911 Welcome message to the selected connection. The welcome message will test the gateway and connection settings as well as provide the recipient vital information about how to use his/her Email account to receive alarm and report messages and request acknowledgements, reports, and alarm updates.

Alarm Format



Subject

View or select the contents of the alarm message subject. It can contain a static default subject of "WIN-911 Alert" or use a dynamic alarm descriptor that is taken from the report definition during runtime.

Body

View or select an alarm message format from the five available options: Default Text Simple, Default Text Verbose, Default HTML Simple, Default HTML Verbose, and Diagnostic. The simple selections include minimal information about the alarm whereas the verbose options include amplified details. The Diagnostic option is the most detailed and includes information regarding Email notifier modules interaction with the Email server and is not intended for normal

remote notification operations. The HTML options include a more visually appealing, rich presentation with a color-coded alarm condition and acknowledgement information but will not be compatible with "text-only" Email servers or devices.

Preview

A "What You See is What You Get" window shows the administrator what an alarm message will look like with the current options selected.

Report Format

Subject

View or select the contents of the report message subject. It can contain a static default subject of "WIN-911 Report" or use a dynamic report descriptor that is taken from the report definition during runtime.

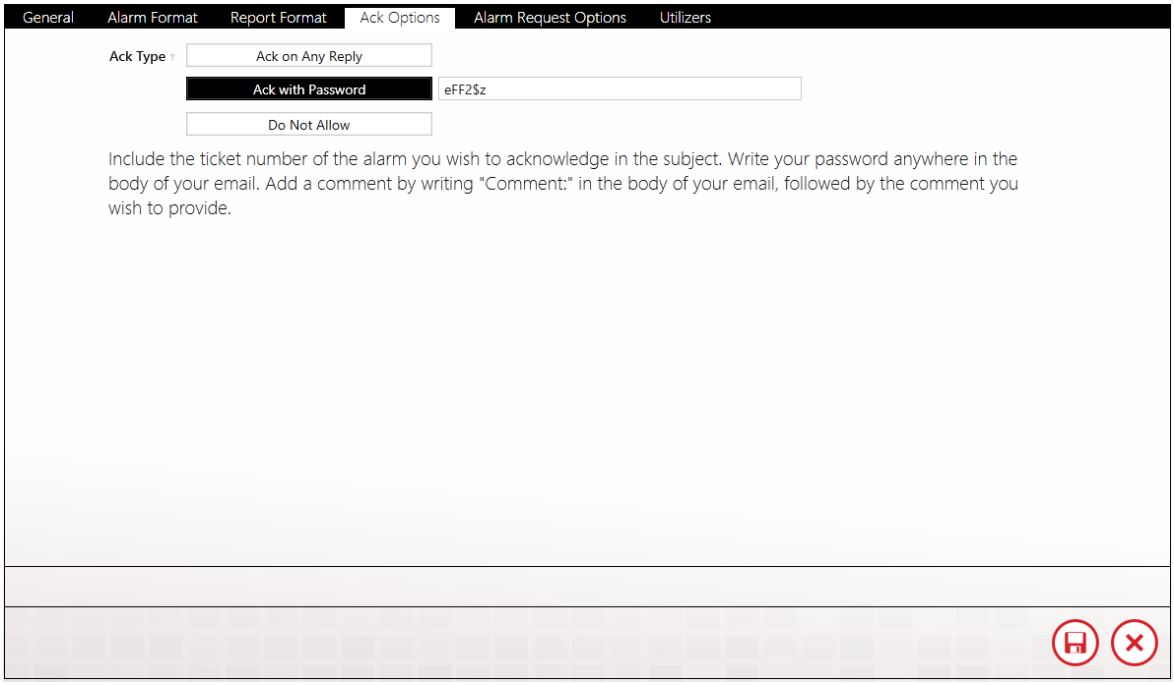
Body

View or select the report message format from the four available options: HTML Report, Default Report (Horizontal), Plain Text Vertical Report, and Plain Vertical Report Verbose. The simple selections include minimal information about the alarm whereas the verbose options include amplified details. The HTML options include a more visually appealing rich presentation with color-coded alarm condition and acknowledgement information but are not compatible with text only Email servers or end-users.

Preview

A "What You See if What You Get" window shows the administrator what a report message will look like with the current options selected.

Ack Options



Select the connection's acknowledgement options with this tab.

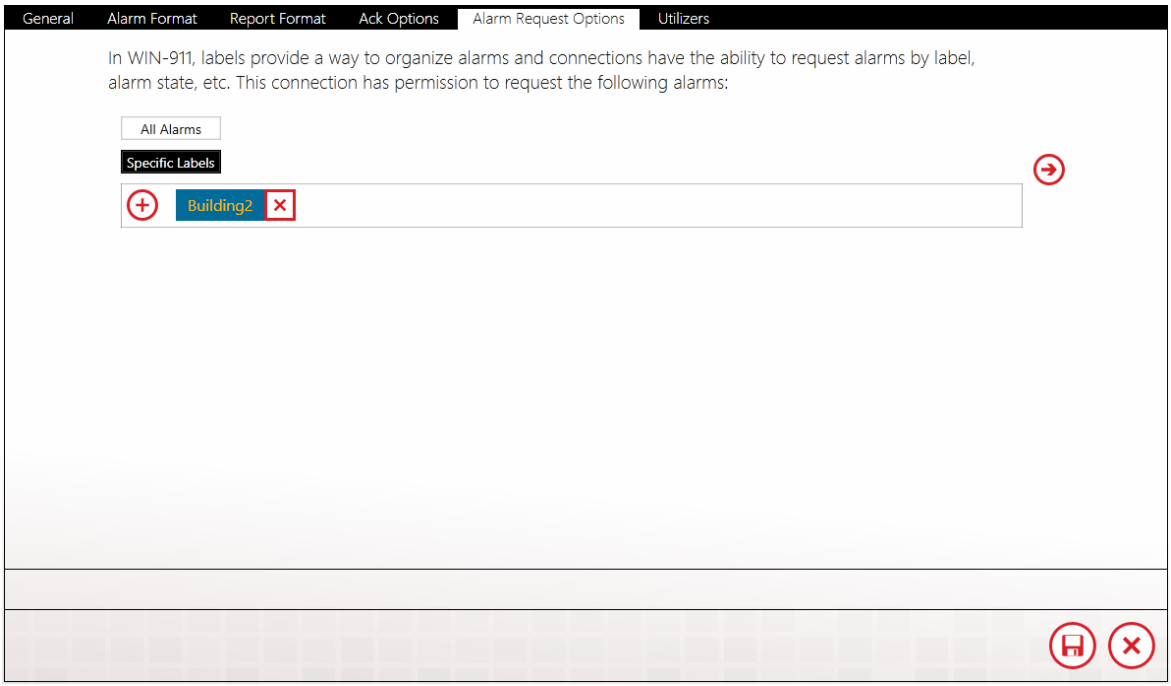
There are three options each Email connection can be configured for concerning the ability to issue acknowledgement requests: Ack on Any Reply, Ack with Password, and Do Not Allow. In edit mode this setting can be selected or modified by clicking the desired button. The "Ack with Password" option contains a text entry box where the ack password is defined. The password will not be visible in view mode.

To provide a comment with your acknowledgement, enter "comment:" followed by your comment in the body of your reply Email.

To acknowledge alarms using a password, include the password in the body of your reply Email.

Note: If the connection type is set for "Use an Email to SMS Gateway" you may not select "Ack on Any Reply" as your ack type.

Alarm Request Options



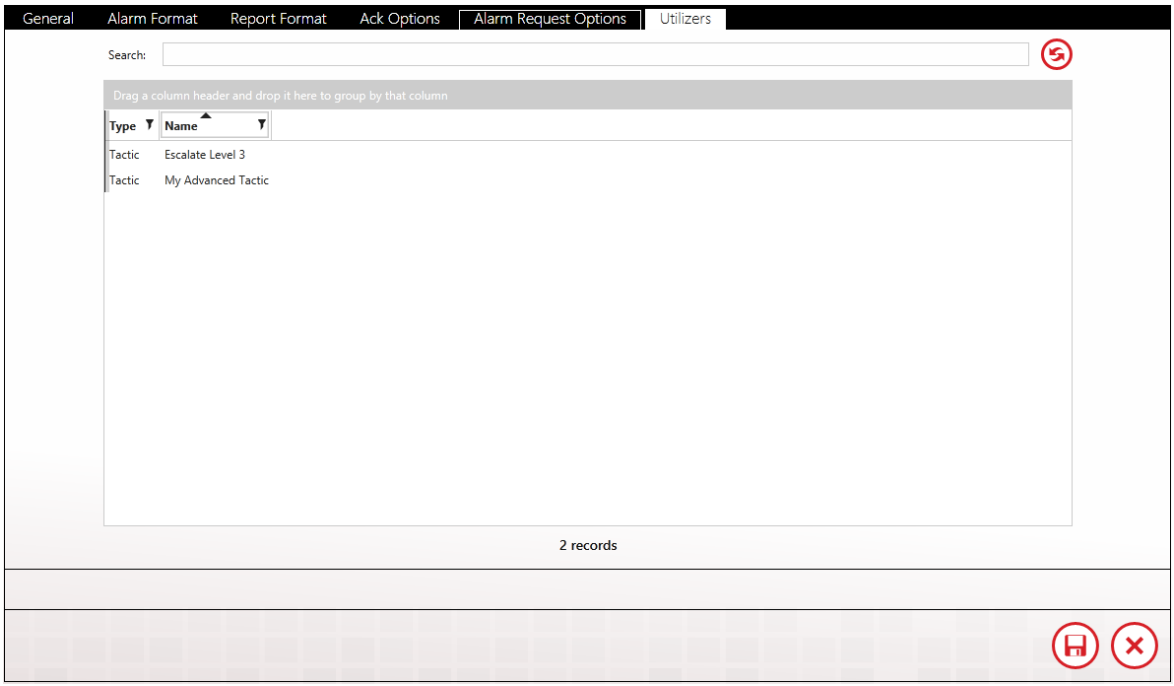
WIN-911 labels provide a way to organize alarms and connections have the ability to request alarms by label, alarm state, etc.

Select the connection's alarm request options by clicking one of the two options: All Alarms, or Specific Alarms. If the Administrator wishes to limit the connect's alarm request to specific labels, the

labels must be added using the labels selection tool. There are no limits to the number of labels that can be assigned to a connection.

See Labels for more details.

Utilizers

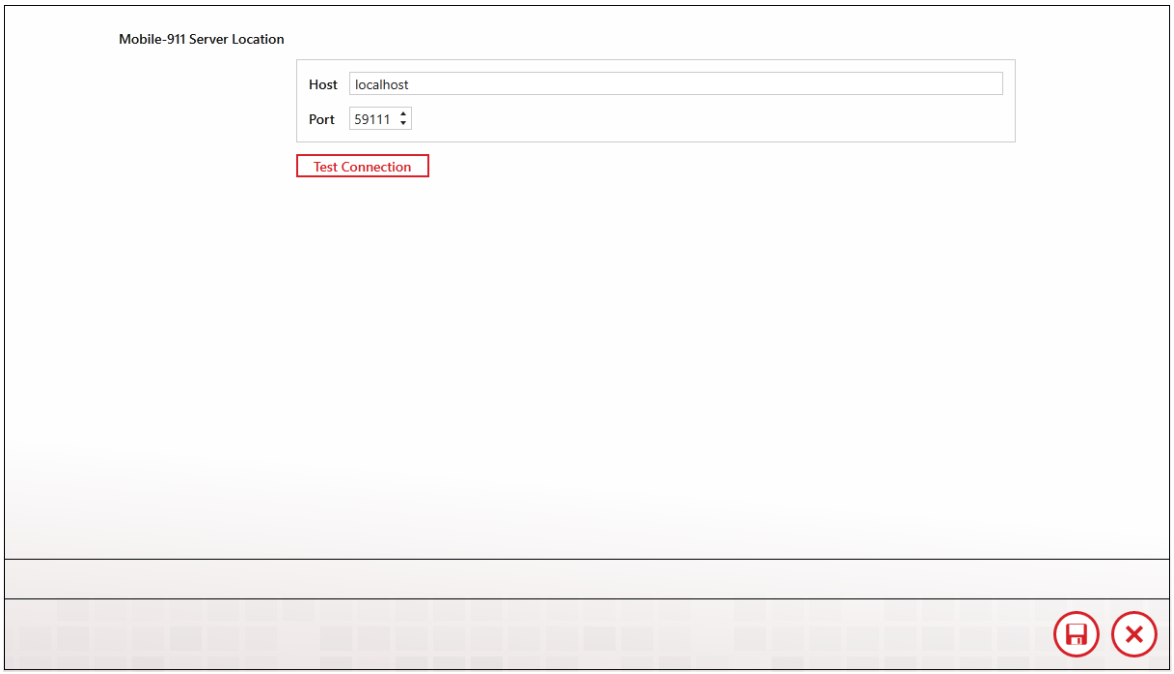


The Utilizers tab is a booking keeping device that lists all of the tactics associated with this contact. When utilizers are present WIN-911 prevents the contact from being deleted. If you wish to delete the contact you will first have to modify the utilizing tactic in a manner that will unlink it to this contact. Once all utilizers are cleared, the contact can be safely deleted.

Mobile-911 Gateway

WIN-911 communicates with your Mobile-911 clients through a server. Specify the address of your Mobile-911 Server here.

Mobile-911 Server Location



Specify

With this selection, the location of the Mobile-911 Server can be entered manually by the WIN-911 administrator by entering the IP address and port number in the text boxes that appear when the Specify button is selected. The default IP address for Host is "localhost" and the default Port number is 59111.

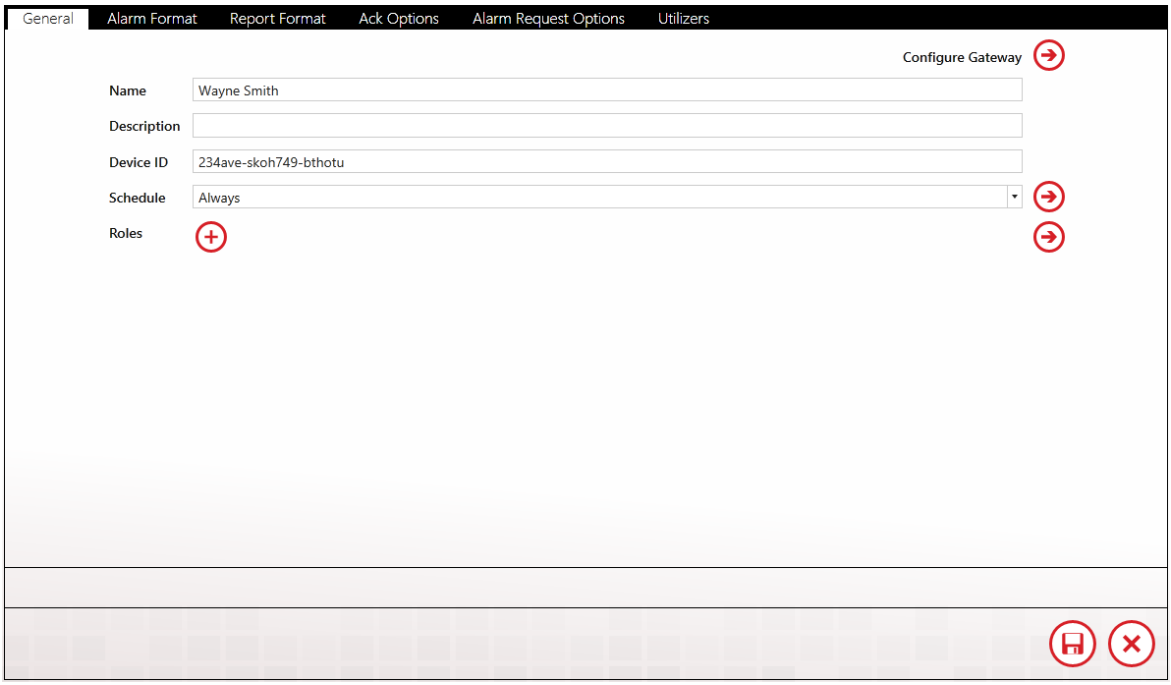
Test Connection

Click this button to verify the Mobile-911 Server location. If WIN-911 cannot connect to the server check your settings and ensure that the Mobile-911 Service is running.

Mobile-911 Connections

Connections specify a destination for alarm notification reports. Mobile-911 connections also determine what you will see in alarm and report messages, connection availability and the permissions a connection has been granted concerning acknowledgement.

General



Name

Each Mobile-911 connection must have a unique name that identifies the particular Mobile-911 connection.

Description

An optional field for entering information concerning the particular connection.

Device ID

Enter the Mobile-911 Device ID for this connection. The Device ID is found in the device's app under Settings. Since the ID is typically long and cryptic we recommend using the Send Device ID option to Email the Device ID to the WIN-911 computer. From there you can copy and paste it directly into WIN-911.

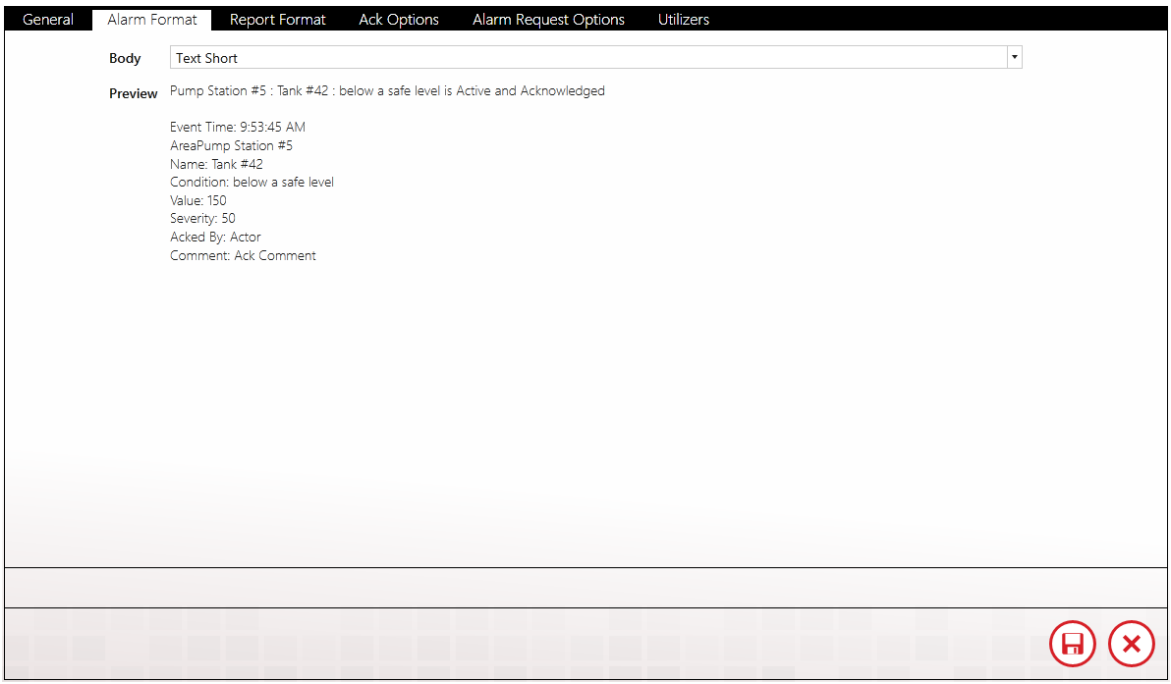
Schedule

Select the schedule that WIN-911 will honor when sending alarm and report messages. A connection can have only one assigned schedule, but a schedule can contain multiple appointments. See Schedules.

Roles (for use by Advanced Tactics)

View or assign roles to the selected connection by clicking the add button in edit mode. Each connection can have multiple roles. See Roles.

Alarm Format

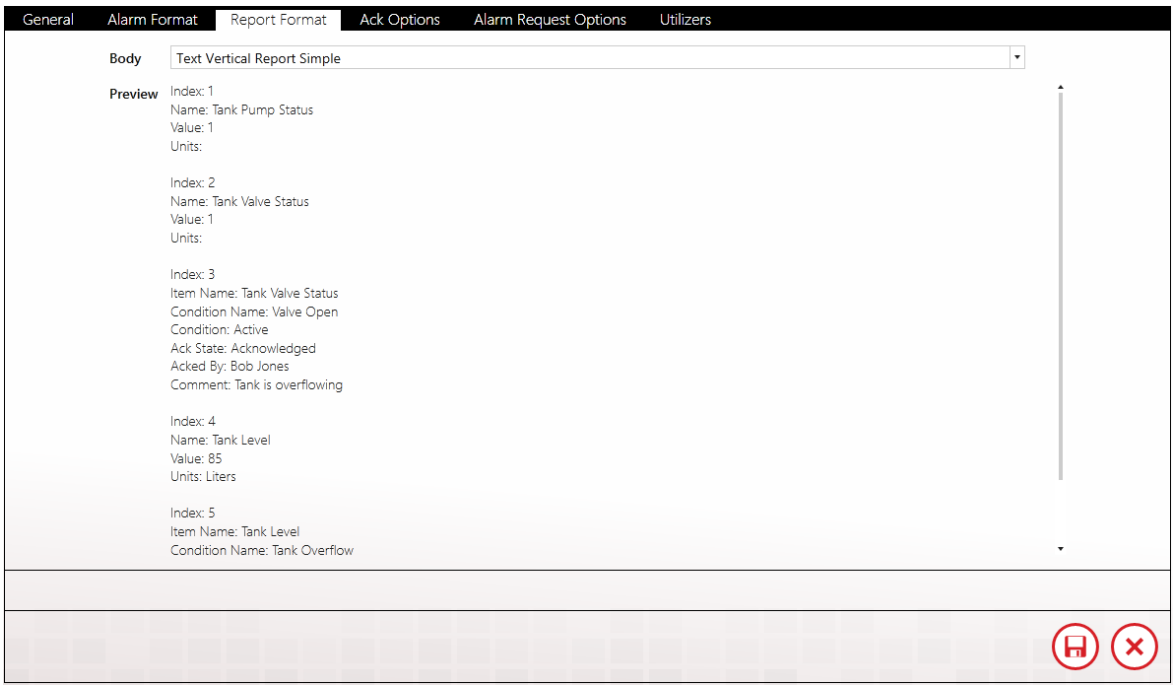


View or select an alarm message format from the two available options: Default Text Simple or Default Text Verbose. The simple selection includes minimal information about the alarm whereas the verbose option includes amplified details.

Preview

The Preview window shows the administrator what an alarm message will look like with the current options selected.

Report Format

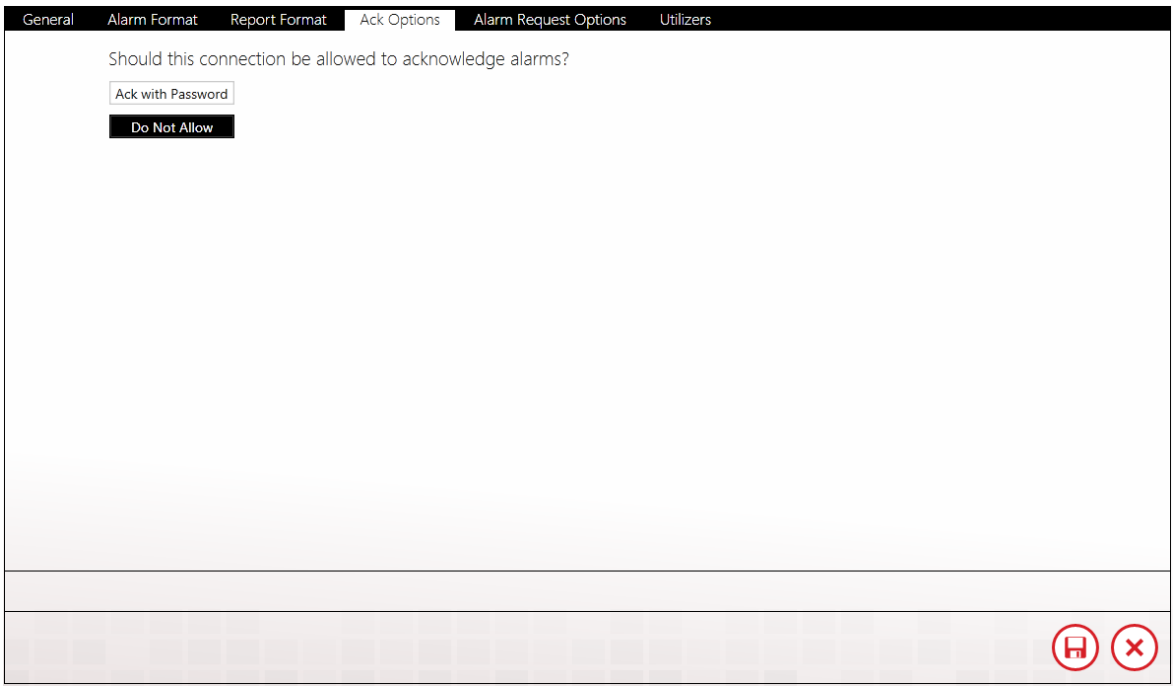


Select the report message format from the two available options: Plain Vertical Report or Plain Vertical Report Verbose. You can also create custom formats using the Mobile -911 Formats tab.

Preview

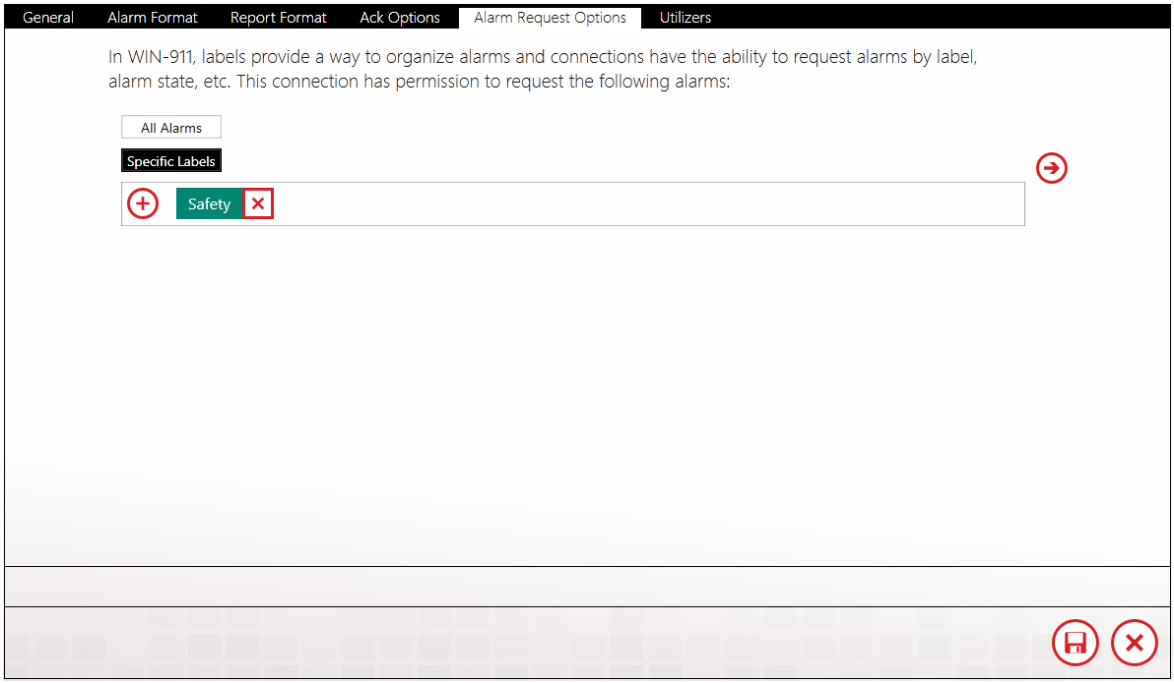
The Preview window shows the administrator what a report message will look like with the current options selected.

Ack Options



Select the connection's acknowledgement options on this tab.

Alarm Request Options

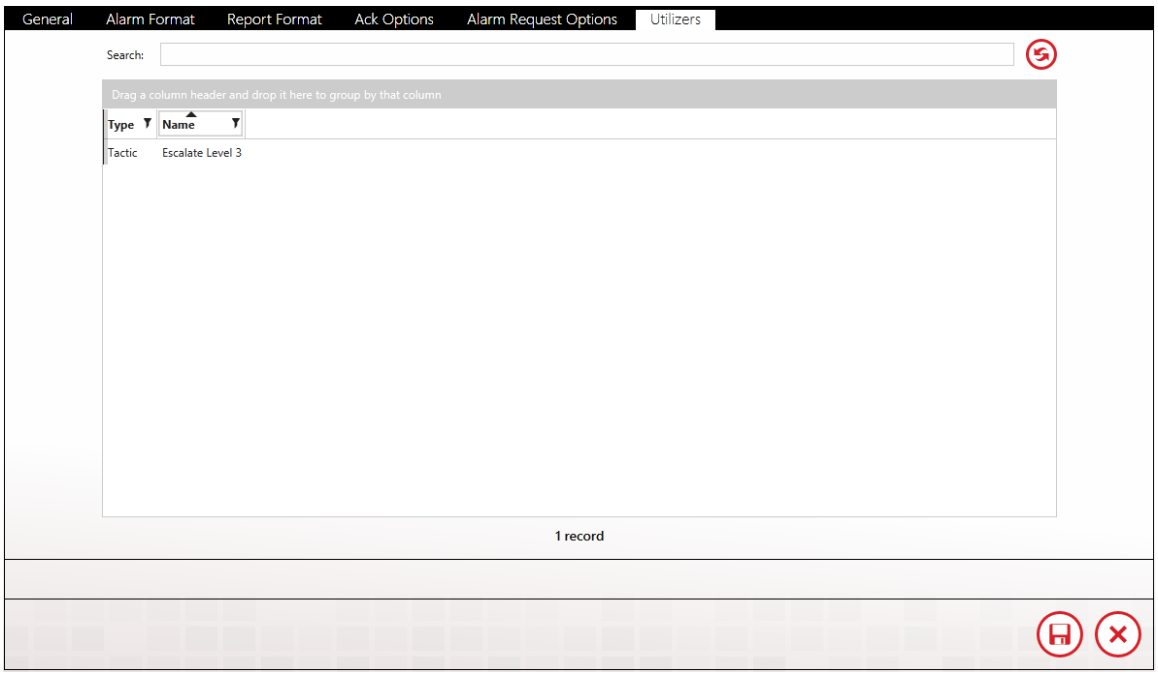


WIN-911 labels provide a way to organize alarms and connections have the ability to request alarms by label, alarm state, etc.

Select the connection's alarm request options by clicking one of the two options: All Alarms or Specific Labels. If the Administrator wishes to limit the connection's alarm request to specific labels, the labels must be added using the labels selection tool. There are no limits to the number of labels that can be assigned to a connection.

See Labels for more details.

Utilizers



The Utilizers tab is a device that lists all of the tactics associated with this contact. When utilizers are present, WIN-911 prevents the contact from being deleted. If you wish to delete the contact you will first have to modify the tactic in a manner that will unlink it to this contact. Once all utilizers are cleared, the contact can be deleted.

Mobile-911 Advanced Network Considerations

The Mobile-911 Server is a separate product that facilitates WIN-911's dispatching of alarm notifications to Android, iPhone, and Blackberry smart-phone apps. It receives tasking from the WIN-911 Notifier and interfaces with Google's, Apple's, and RIM's push notification service through a live Internet connection. The Mobile-911 Server can be deployed on the local WIN-911 platform or on a separate computer with network access to WIN-911.

In cases where the Mobile-911 Server is deployed on a remote node, WIN-911 will need a method for locating Mobile-911. If WIN-911 is on the same network segment, then "Discovery" is the preferred and most easily configured method. When WIN-911 is located on a separate network (or network segment), the Mobile-911 Server location must be specified by entering the IP and port number at the WIN-911>Contacts>Mobile-911>Gateway tab.

The network administrator will need to set up "port-forwarding" on the Mobile-911 network router to enable incoming messages from WIN-911 to be routed to the Mobile-911 Server's computer port. Likewise, WIN-911's network router will need to be configured to route incoming messages and from the Mobile-911 Server to WIN-911.

When configuring WIN-911to interface with a Mobile-911 Server on a remote network, enter the Public IP address (or URL) of the Mobile-911 network router. Then enter the router port number that has been forwarded to the Mobile-911 Server.

The WIN-911 Bridge port is set to 59109 and must be configured as such in the Mobile-911 Server Settings Manager.

The Mobile-911 Server listening port is set to 59111.

Mobile-911 Server Router Setup

For WIN-911 Access

1) Open a browser on a computer that is part of the Mobile-911 Server network, and enter the router administration URL (normally 192.168.1.1). This usually requires a username and password for administrative access.

Note: Be careful not to confuse the internal URL (192.168.1.1) with the Public URL of the router. For this example we'll use 24.123.252.111 for the router's Public URL.

2) Navigate to the Port Forwarding page of the router administration GUI. Select a unique port number for WIN-911 to request communications with. For this example we'll use 59100.

3) Enter the local network URL of the Mobile-911 computer (for example: 192.168.1.123).

4) Enter the port number that Mobile-911 will use to receive messages from WIN-911. The default port is 59111.

5) Click the "Apply" button to establish the new forwarding.

The router now actively sends any outside communication request for Port 59100 to endpoint 192.168.1.123:59110. Thus Mobile-911 can hear messages from WIN-911 on a different network.

For Mobile-911 Smartphone Access

In order for a Mobile-911 Smartphone App to send data to a Mobile-911 Server it will need a Public Port forwarded from the Mobile-911 network router to the Mobile-911 Server computer. This port is separate from the port that WIN-911 will use.

6) Back at the Port Forwarding page of the router administration GUI, select a new port number for Mobile-911 Smart phones to request communications with. For this example we'll use 59102.

7) Enter the local network URL of the Mobile-911 Server computer (for example: 192.168.1.123).

8) Enter the port number that Mobile-911 will use to receive messages from the smartphones. The default port is 59112.

9) Click the "Apply" button to establish the new forwarding.

The router now actively sends any outside communication request for Port 59102 to endpoint 192.168.1.123:59112. Thus Mobile-911 can hear messages from any smartphone configured with this endpoint.

10) From your Mobile-911 Smartphone App, navigate to the Settings Tab. Select the Primary Server setup and enter the URL of Mobile-911 Server (24.123.252.111) and set the Port for 59102.

11) Click the Test Connection button and Mobile-911 App will attempt to contact the Mobile-911 Server and provide feedback indicating success or failure.

WIN-911 Mobile Gateway Setup

1) From the WIN-911>Contacts>Mobile-911>Gateway page, select Specify.

2) Enter the Mobile-911 Server router's Public URL (24.123.254.111, in the example above).

3) Enter the Public Port Number for the Mobile-911 Server (59100, in the example above).

4) Click the Test button and WIN-911 will attempt to contact the Mobile-911 Server and provide feedback indicating success or failure.

5) If the test fails, ensure the perspective operating system firewalls are set to grant local and public access to Mobile-911 Server and WIN-911.

WIN-911 Network Router Setup

1) Open a browser on a computer that is part of the WIN-911 network and enter the router administration URL (normally 192.168.1.1). This usually requires a username and password for administrative access. For the sake of this example we'll use 24.123.252.222 for the router's Public URL.

2) Navigate to the Port Forwarding page of the router administration GUI. Select a unique port number for Mobile-911 Server to request communications with. For the sake of this example we'll use 59101.

3) Enter the local network URL of the WIN-911 computer (for example: 192.168.1.223)

4) Enter the port number that WIN-911 will use to receive messages from Mobile-911 Server. The default port is 59109.

5) Click the "Apply" button to establish the new forwarding.

The router now actively sends any outside communication request for Port 59101 to endpoint 192.168.1.223:59109. Thus WIN-911 can hear messages from Mobile-911 Server on a different network.

Mobile-911 Server Setup

1) From the Mobile-911 Server Manager Bridge Server tab, select Specify.

2) Enter WIN-911's public router URL (24.123.254.222, in the above example).

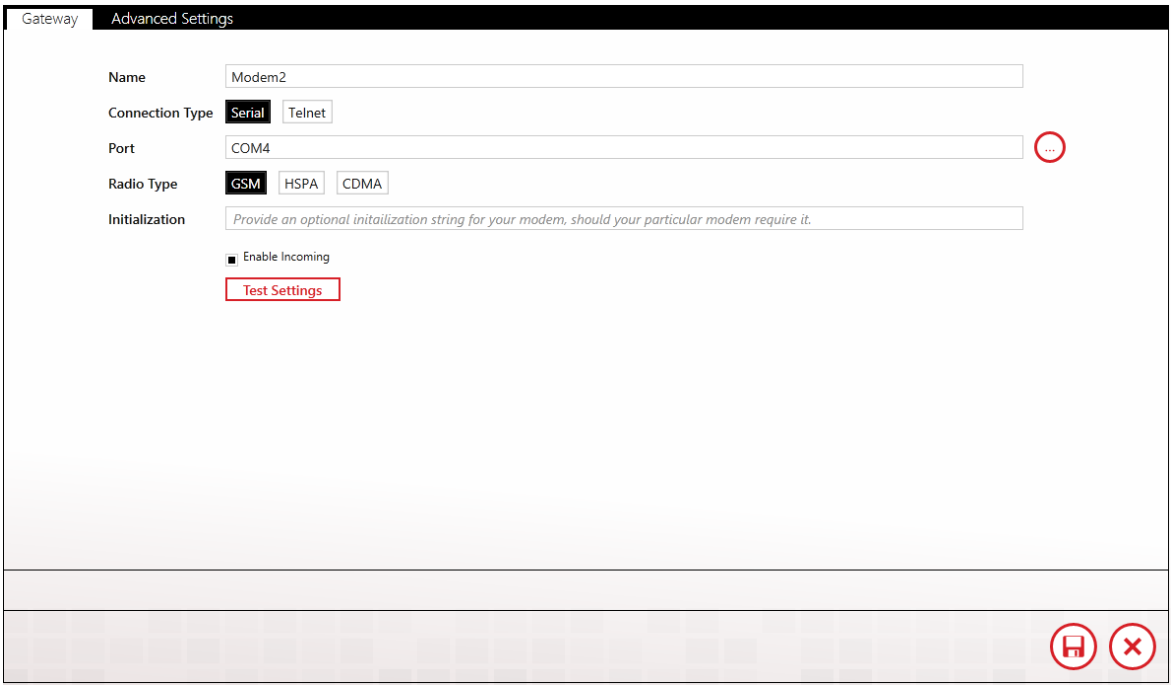
3) Enter the Public Port Number for WIN-911 (59101, in the above example).

5) Ensure the operating system firewall is set to grant local and public access to Mobile-911 Server.

SMS Gateway

The SMS Gateway is used to configure the necessary settings for WIN-911 to communicate with the cellular modem(s) it will use to conduct remote notifications.

Gateway



WIN-911 needs exclusive access to a cellular modem registered with a text service provider account. The gateway settings include the location of the modem as well as all the necessary information about modem COM parameters.

You can configure multiple modem gateways for failover protection in the event that one modem becomes unavailable. WIN-911 automatically load balances tasking between the configured gateways to ensure optimum throughput.

Name

A unique name must be given to each SMS gateway. We suggest a name that would help the administrator identify attributes of the modem like its service provider, phone number, etc. The name given is at the discretion of the administrator and does not have any bearing on the systems functionality.

Connection Type

Serial
When a cellular modem is physically connected via USB or RS232 to the WIN-911 host click the Serial button. You will then be prompted for the associated COM port.

Port Option
Browse and select the serial port that WIN-911 will use to communicate with the cellular modem. The proper syntax would be "COM3" for comm port number 3. See Phone and Modems or Device Manager for details.

Telnet
Remotely located cellular modems can be used by WIN-911 using Telnet

Address (for Telnet connections)
Enter the IP address (or host name) and port number of the remote cellular modem

User Login (for Telnet connections)
Tick this box if the remote cellular modem is configured to require credentials in order to log in.

User Name (for Telnet connections)

Enter the user name that the remote modem requires for authentication during login.

Password (for Telnet connections)

Enter the user password that the remote modem requires for authentication during login.

Radio Type

WIN-911 supports three types of radio standards, GSM, HSPA, and CDMA. The type of radio you choose is dictated by the modem hardware and the SMS texting service provider you choose to support application. Check with your service provider and hardware manufacturer to determine your radio type.

GSM

Multitech models MTC-G3, MTR-G3, MTCBA-G2 are supported with GSM networks like AT&T and Verizon.

HSPA

Multitech models MTC-H5, MTR-H5, are supported with HSPA networks like AT&T and Verizon

CDMA

Multitech models MTC-C3, MTR-C2, MTCBA-C1 are supported with CDMA networks like Verizon.

Initialization

This string represents the AT command sent to initialize and test the modem.

Enable Incoming

Tick this box to enable WIN-911 to receive SMS messages from the remote users such as alarm, acknowledgement, and report requests.

Test Settings

Several parameters that determine the modem's ability to conduct remote notification are tested when this button is clicked: signal strength, registration with the service provider, and the bit error rate. It also sends a test message to the phone number you enter when prompted by WIN-911.

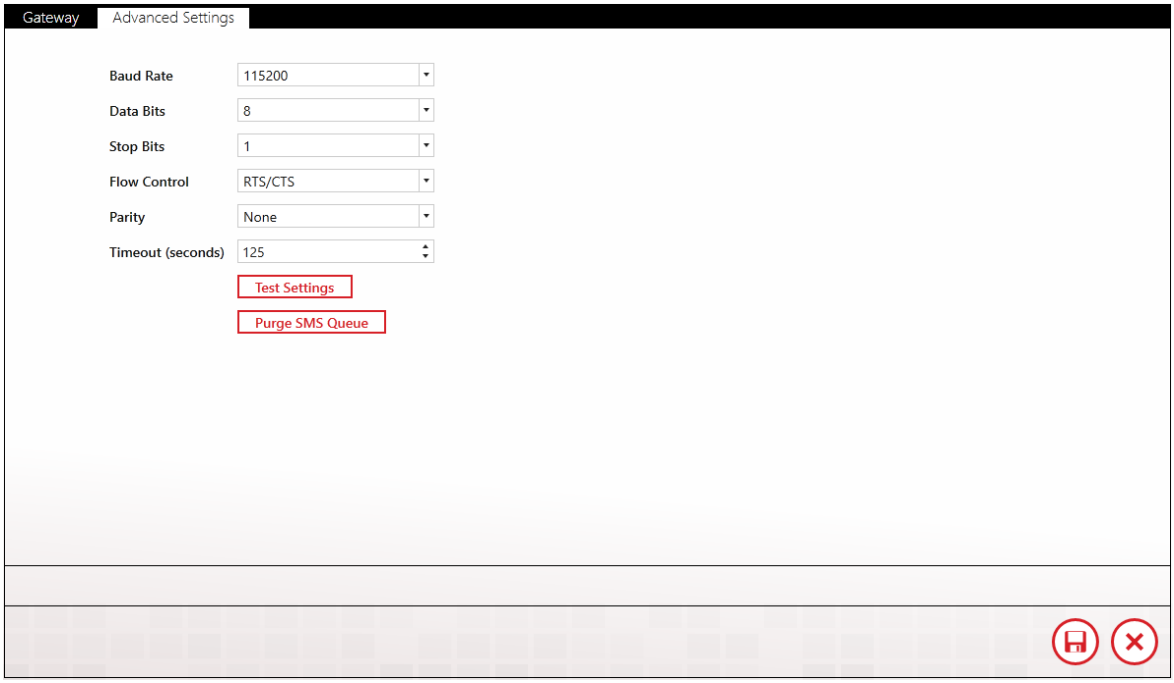
Network Registration Status: your modem should be properly registered with your service provider and on its home network (not roaming). If it reports as roaming, please contact your service provider to correct the problem or check our https://supportdesk.WIN-911.com/support/solutions.

Signal Quality: the network's signal strength should be in the acceptable range to ensure a reliable connection to your service provides. If the strength is insufficient you should consider moving your modem to an area with better reception. Note that the Telnet option allows WIN-911 to connect to a remotely located modem, in the event that your WIN-911 host is located in an area with bad reception. The appropriate signal strength should be 10 or more.

Bit Error Rate: the number of bit errors per unit time.

Test Message: WIN-911 sends a test message to the phone number you enter at the prompt. If WIN-911 receives a "message sent successfully" response from service provider then the test message will be considered successful. The phone will receive a message: The Modem configuration your provided appears correct.

Advanced Settings



Baud Rate (serial connection)

The cellular modem's baud rate may be set from 110 to 921600 (115200 default). This selection controls the speed at which WIN-911 will communicate with the cellular modem. Refer to the modem's documentation or contact the modem manufacturer for the specified recommended Baud.

Data Bits (serial connection)

The cellular modem data bits can be set to "Unspecified, 5, 6, 7, or 8". The default setting is 8 data bits. Refer to the modem's documentation or contact the modem manufacturer for recommended Data Bits.

Stop Bits (serial connection)

The cellular modem stop bits can be set to "None, 1, 1.5, or 2". The default setting is 1 stop bit. Refer to the modem's documentation or contact the modem manufacturer for recommended Stop Bits.

Flow Control (serial connection)

The cellular modem flow control can be set to "None, XON/XOFF, RTS/CTS (default), and RTS/XOnXOff". The default setting is RTS/CTS. Refer to the modem's documentation or contact the modem manufacturer for recommended flow control.

Parity (serial connection)

The cellular modem Parity can be set to "Even, Odd, None, Mark, and Space". The default setting is None. Refer to the modem's documentation or contact the modem manufacturer for recommended Data Bits.

Timeout (seconds)

This is total time WIN-911 will wait for an expected response from the modem. Setting this value too low may cause the initialization and/or modem commands to fail. The default value is 125 seconds and can be varied from a minimum of 20 and a maximum of 600.

Test Settings

Several parameters that determine the modem's ability to conduct remote notification are tested when this button is clicked: signal strength, registration with the service provider, and the bit error rate. It also sends a test message to the phone number you enter when prompted by WIN-911.

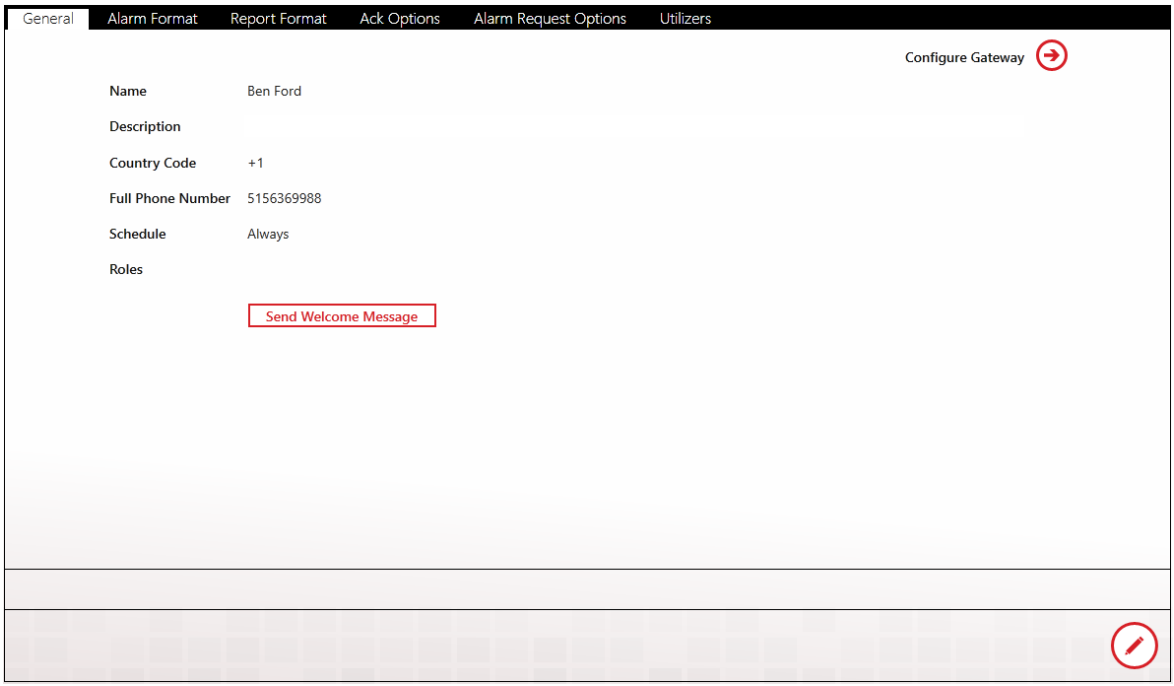
Purge SMS Queue

Purge all pending SMS messages from the queue so WIN-911 will be able to send alarm messages immediately.

SMS Connections

Connections specify a destination for alarm notification messages. SMS connections also determine just what you will see in alarm and report text messages, connection availability and the permissions a connection has been granted concerning acknowledgement and report requests.

General



Name

Each SMS connection must have a unique name that identifies the particular connection.

Description

An extra text field for organization and administration purposes, similar to a code comment.

Country Code

Enter the country code of the alarm recipient. US and Canadians users enter +1 (default).

Full Phone Number

Enter the entire cell phone number, excluding the country code.

Schedule

View or select the schedule that WIN-911 will honor when sending alarm and report messages. A connection can have only one assigned schedule, but a schedule can contain multiple appointments. See Schedules.

Roles (for use by Advanced Tactics)

View or assign roles to the selected connection by clicking the add button in edit mode. Each connection can have multiple roles. See Roles.

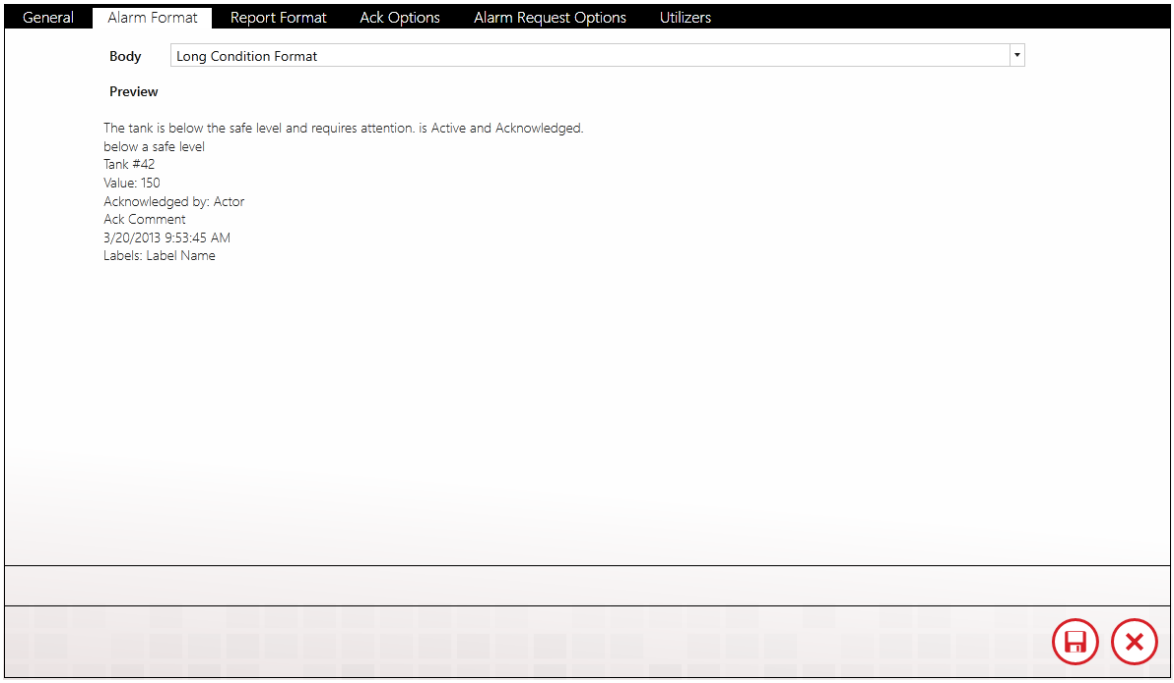
Send Welcome Message

Click the "Send" button in view or edit mode to send a WIN-911 Welcome message to the selected connection. The welcome

message will test the gateway and connection settings. The test message should read the following:

"Welcome to the WIN-911 System! For instructions on how to use the system, make sure your SMS connection is saved, and send in the text "help"."

Alarm Format



Body

Select an alarm message format from the six available options: Condition Format, Diagnostic Format, List Format, Long Alarm Format, Long Condition Format, and Short Alarm Format.

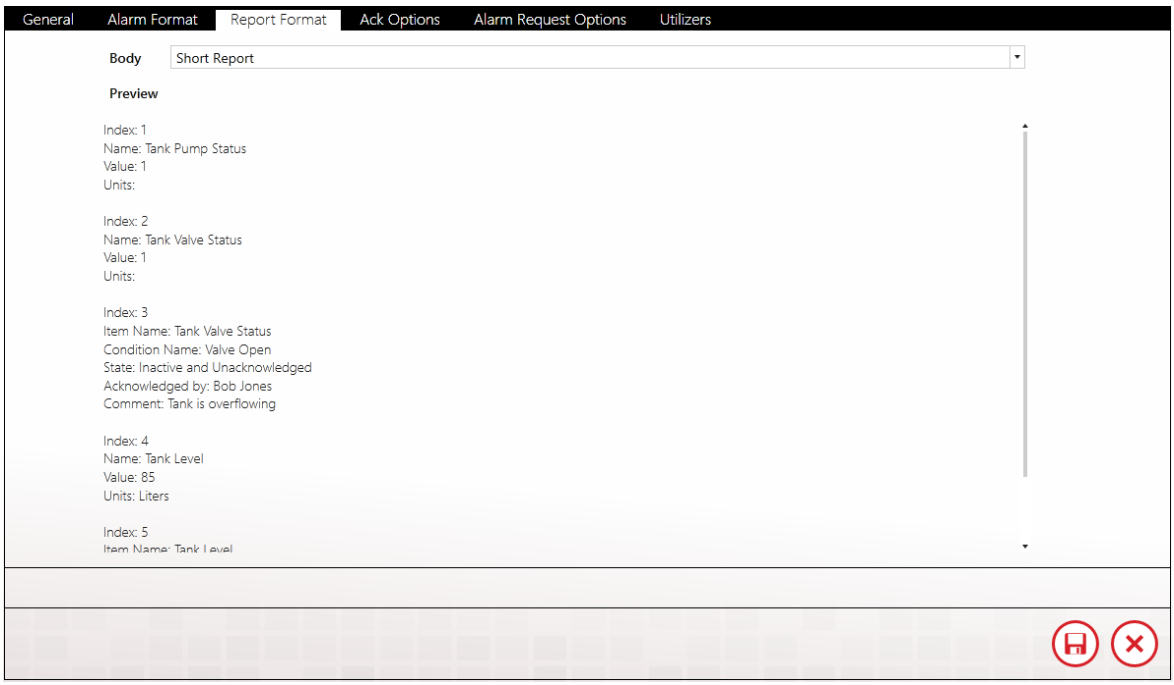
Condition Format, Diagnostic Format, List Format, Long Alarm Format, Long Condition Format, and Short Alarm Format. The simple selections include minimal information about the alarm whereas the

verbose options include details. The Diagnostic option is the most detailed and includes information

Preview

A "What You See is What You Get" window shows the administrator what an alarm message will look like with the current options selected.

Report Format



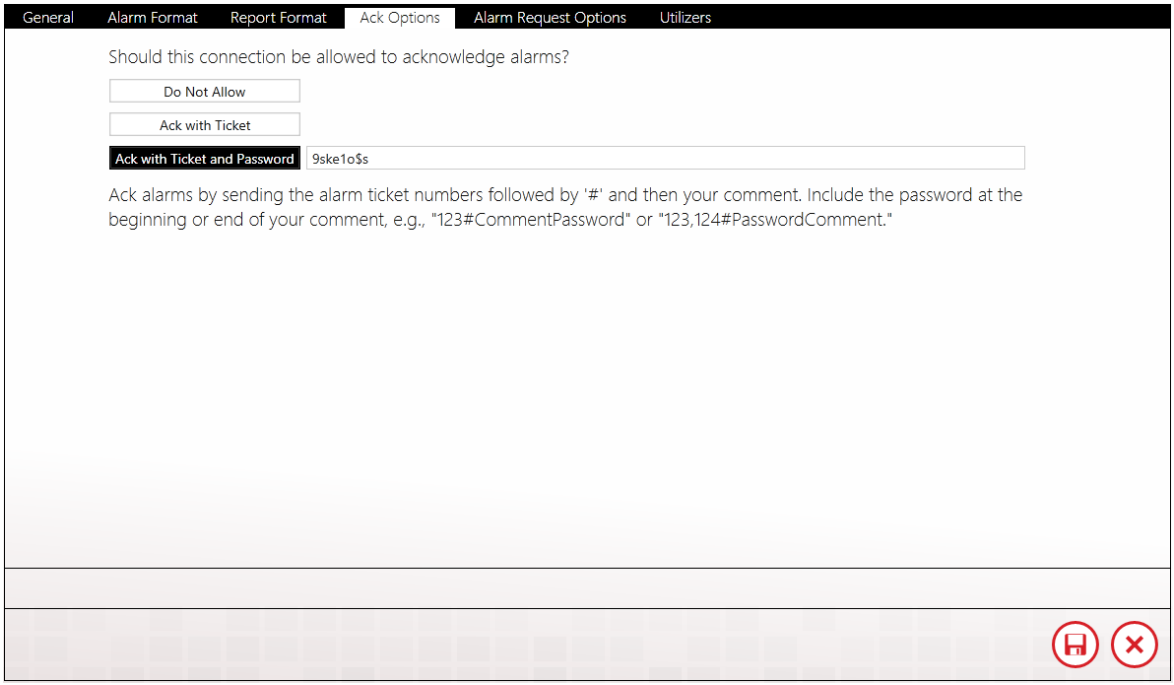
Body

View or select the report message format from the two available options: Long Report and Short Report. The short selection includes minimal information about the alarm whereas the long option includes amplified details.

Preview

A "What You See is What You Get" window shows the administrator what a report message will look like with the current options selected.

Ack Options



View or select the connection's acknowledgement options with this tab.

Do Not Allow

The default selection for SMS connections is to not allow the connection the ability to acknowledge alarms.

Ack with Ticket

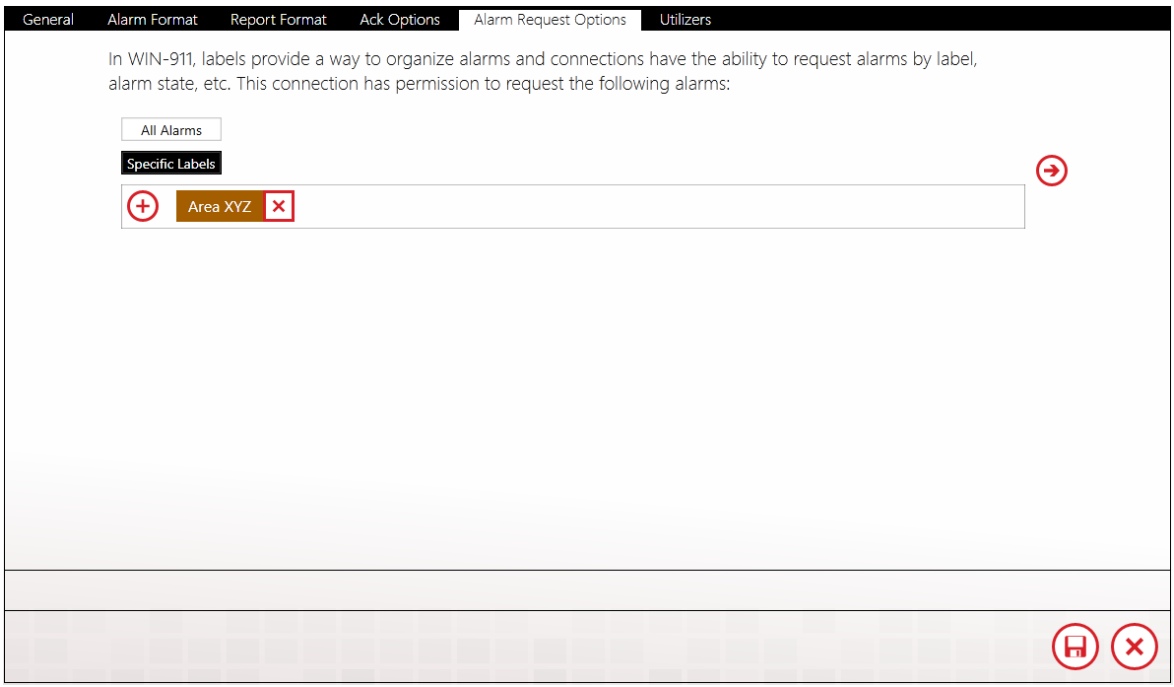
Alarms can be acknowledged by responding to the alarm message with the ticket number included in the alarm message.

Ack with Ticket and Password

An added layer of security can be added by requiring the actor to include a password along with the ticket number of the alarm in the response message. This option contains a text entry box where the ack password is defined. The password will not be visible in view mode. To acknowledge alarms using a password, include the password in the body of your reply SMS.

To provide a comment with your acknowledgement, enter "#:" (pound or hash character) followed by your comment in the body of your reply SMS.

Alarm Request Options

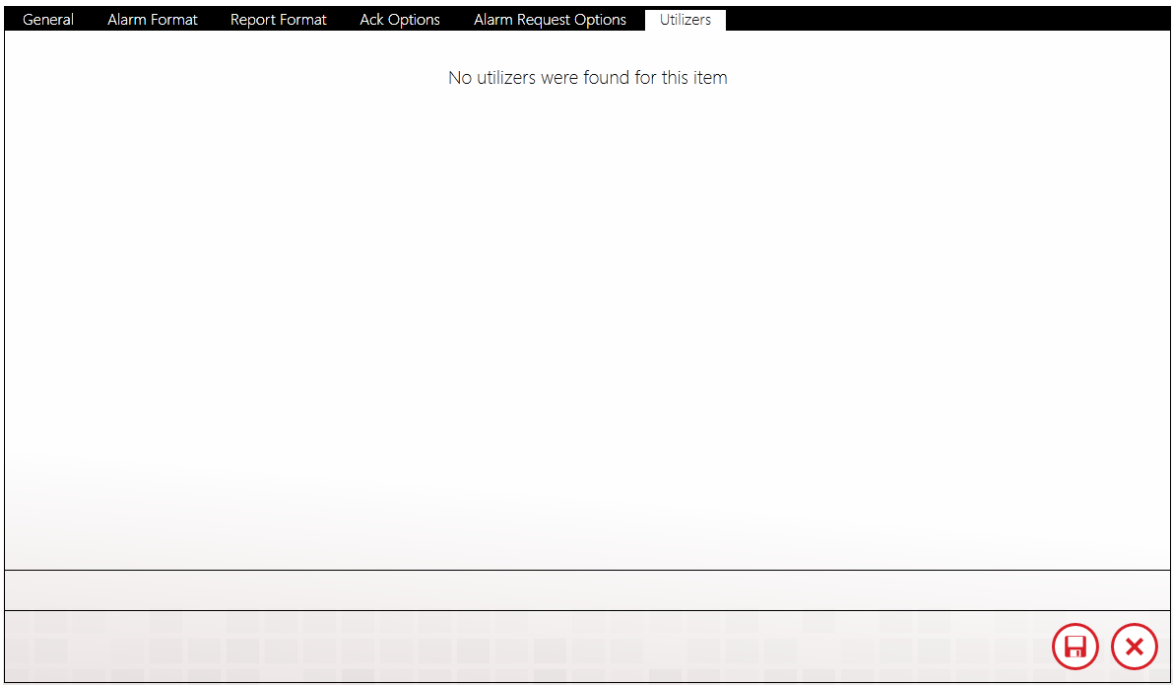


Connections have two options available for actively requesting alarm information: All Alarms, or Specific Alarms. If the Administrator wishes to limit the connection's alarm request to specific Labels, they must be specified by using the Labels selection tool. There are no limits to the number of labels that can be assigned to a connection.

See Using SMS for an example of an SMS alarm request.

See Labels for more details.

Utilizers



The Utilizers tab is a book keeping device that lists all of the tactics associated with this contact. When utilizers are present WIN-911 prevents the contact from being deleted. If you wish to delete the contact you will first have to modify the utilizing tactic in a manner that will unlink it to this contact. Once all utilizers are cleared, the contact can be safely deleted.

Using SMS

Alarm event messages can be sent to a cellular device when triggered by a WIN-911 Strategy or in response to a request made by a cellular device user. The SMS notifier can provide one-way or two-way communication with any number of cellular devices. With the two-way setting the user can respond to alarm events with an acknowledgement code, or request current conditions by querying reports.

Acknowledging Alarms

Alarm events will be assigned a ticket number that the recipient can use to acknowledge the alarm. This is done by sending a text message to WIN-911 with the ticket number and that the users alarm

An example of an alarm text message with a ticket number of 308 and a valid acknowledgement response with a password of 123:

Message

308
TankLevel is
Above the High Limit & Unacknowledged
Value: 12 ft
1/22/2016, 3:03 PM

Response

308:123

If you wish to enter a comment, type "#" and then your comment, e.g., '123#Comment' or '123, 124#Comment.'

Requesting Alarms

Request alarms by texting in the word "get" followed by an alarm state. e.g., "get active unacked." Your choices are a combination of "active/inactive + acked/unacked."

get active unacked
get active acked
get inactive unacked

Requesting Reports

Request reports by texting the word "report" followed by a report's name or number. e.g., 'report 1'.

report 3
report safety

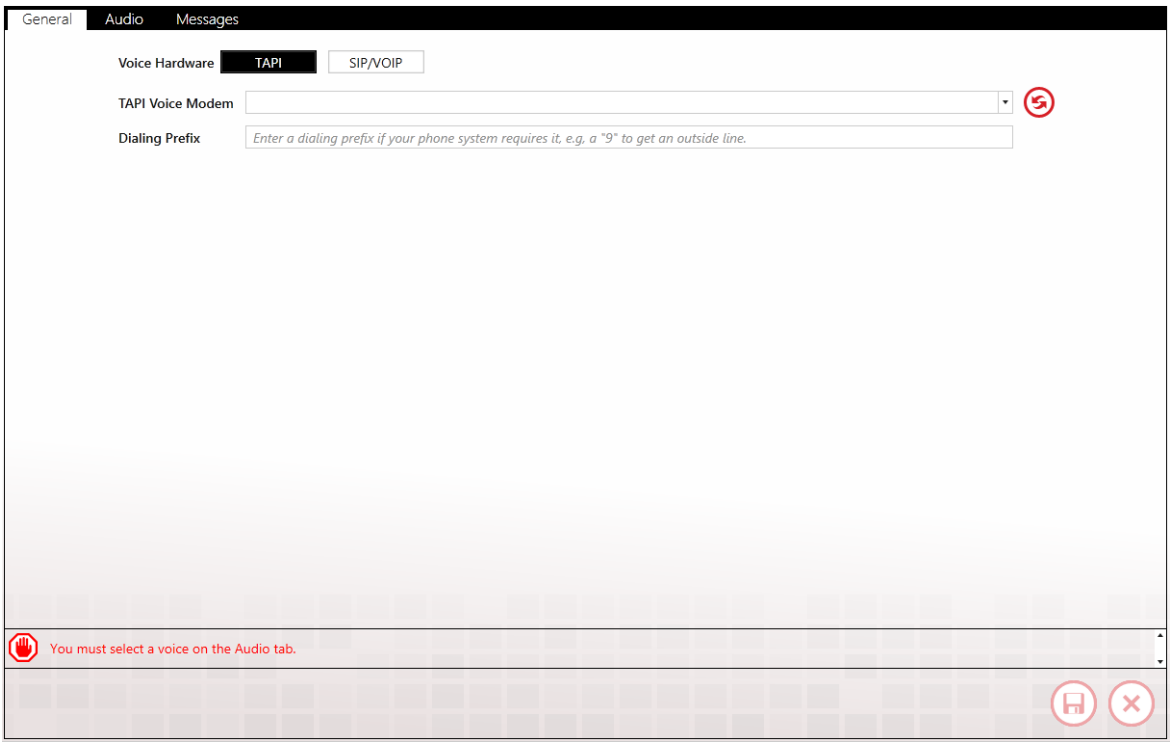
Request a list of available reports by sending in "list reports."

Voice Gateway

General

WIN-911 provides its users with two options for conducting voice alarm notification: 1) SIP/VoIP or 2) a TAPI compliant voice modem. The SIP/VoIP option uses the Internet to place phone calls and must be used in conjunction with a SIP service provider account. The TAPI option requires a TAPI complaint modem and a dedicated analog phone line. (See System Requirements for more details)

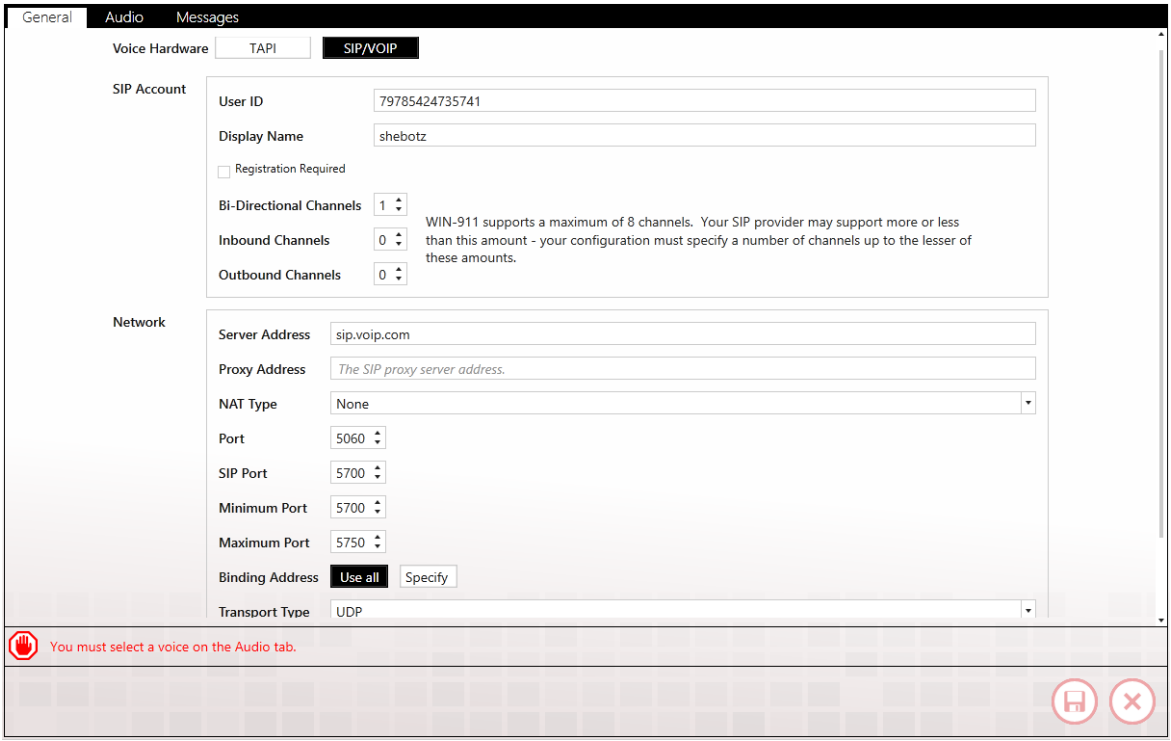
Voice Hardware: TAPI



TAPI Voice Modem

Select the TAPI compatible voice modem currently installed on the WIN-911 Voice Notifier machine. If the pull-down list is empty when the down arrow is clicked then there is no TAPI compatible modem installed or the current drivers for the modem do not include support for TAPI.

Voice Hardware: SIP/VoIP



SIP Account

User ID

The user name that identifies you as a subscriber to the SIP server.

Display Name

The name that will be displayed by the call receiver's caller ID.

Authentication Required

If your SIP server requires additional credentials tick this box to enter an additional user name and password.

ID
SIP identification code for account authentication.

Password
SIP password for account authentication.

Number of Unreserved Channels
Channels can be reserved for inbound or outbound only call processing. This setting designates the number of unreserved channels for the specified SIP account.

Number of Inbound Channels
Channels can be reserved for inbound call processing only. These channels will not process outbound calls.

Number of Outbound Channels
Channels can be reserved for outbound call processing only. These channels will not process inbound calls.

Network

Server Address
Enter the URL of SIP server that WIN-911 will use to conduct alarm notification.

Proxy Address (Optional)
Some SIP providers require connection via a proxy server. Enter the URL of the proxy server that WIN-911 will use to conduct alarm notification.

NAT Type
Select the type of Network Address Translation the SIP server requires for WIN-911 to conduct alarm notification.

- None: Default
- STUN: Simple Transversal of UDP over NATs is a protocol for assisting devices behind a NAT firewall or router with their packet routing.
- TURN: Transversal Using Relay NAT is an extension for STUN-bis protocol to facilitate NAT traversal when one or both endpoints are behind NAT.
- Manual

Server

NAT types STUN and TURN use servers to route data behind the NAT firewall. Enter the name of the NAT server that WIN-911 will use to interface with the SIP provider.

Username

Enter the username that WIN-911 will use when logging on to either a STUN or TURN NAT.

Password

Enter the password that WIN-911 will use when logging on to either a STUN or TURN NAT.

Public IP

Enter the public IP address will use when logging on to a Manual NAT.

SIP Port

Enter the port number that WIN-911 will use to interface with the SIP server.

Minimum Port

Enter the lower port number of the range of possible ports WIN-911 will use the conduct alarm notification.

Maximum Port

Enter the upper port number of the range of possible ports WIN-911 will use the conduct alarm notification.

Binding Address

IP Address used to bind to a particular port.

Transport Type

Select the transport protocol that WIN-911 will use to interface with your SIP provider.

- UDP: User Datagram Protocol uses packet-based data that is sent as discrete packets. UDP does not provide error correction.
- TCP: Transmission Control Protocol uses a stream of packets and provides error correction.
- TLS: Transport Layer Security is a cryptographic protocol that provides communication security over the Internet.
- STCP: Simple TCP is a full duplex, connection oriented transport layer that guarantees in-order delivery.

SRTP Mode

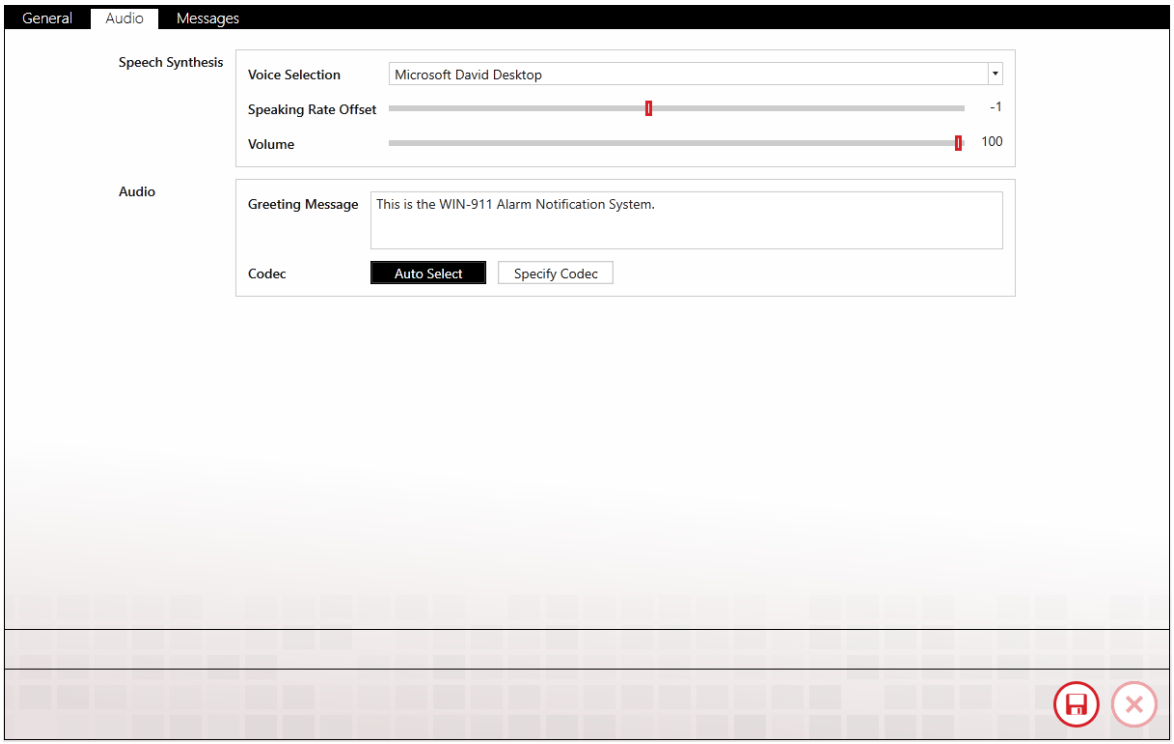
Select the desired mode of Secure Real-time Transport Protocol that WIN-911 will use to interface with the SIP provider. SRTP provides encryption, message authentication and integrity, as well as playback protection.

- None: Default
- Prefer: This mode prefers but does not require SRTP be used.
- Force: This mode requires the use of SRTP.

Test SIP Settings

This button only appears in view mode and when clicked will invoke a dialog that will send a test message to the phone number that you enter. Once the call rings through a test message will be played indicating that your SIP gateway settings are correct. If the settings are not correct then a error message will be displayed which will advise you to check your settings. Check you Event Viewer for a more detailed explanation of the nature of the failure.

Audio



Speech Synthesis

These are global settings that can be overridden in Connections>Speech Synthesis section for individual voice connections.

Voice

Select the Text to Speech voice that WIN-911 will use to conduct voice alarm notification. The voice must use SAPI 5 or higher speech engine.

Speaking Rate Offset

Modify the default rate of speech -10 to 10 with the slider bar to refine the speech rate for your application.

Volume

Modify the volume of speech -100 to 100 decibels with the slider bar to refine the volume for your application.

Audio

Greeting Message

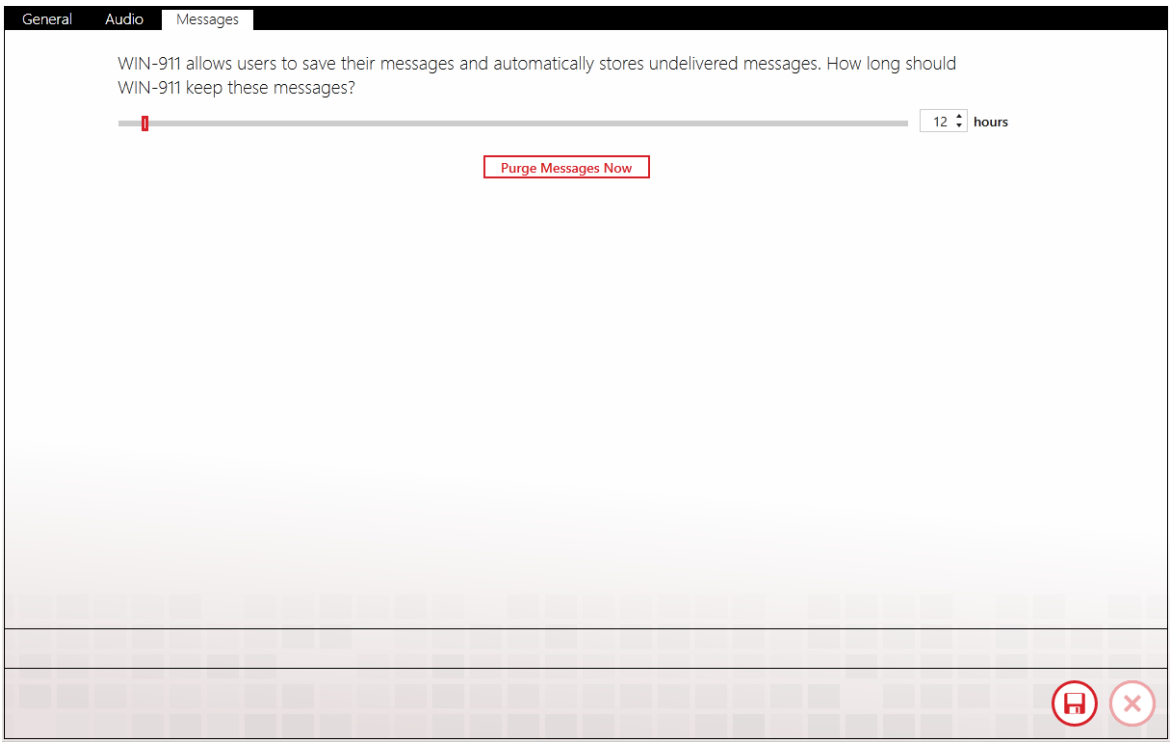
Enter the string that WIN-911 will use to speak the salutation.

Codec

A codec encodes a data stream for transmission, storage or encryption, or decodes it for playback or editing.

- Autoselect: WIN-911 will automatically select the codec to use. (Default)
- Specify Codec: Enter the particular codec that WIN-911 will use to verbalize alarm notification messages.

Messages

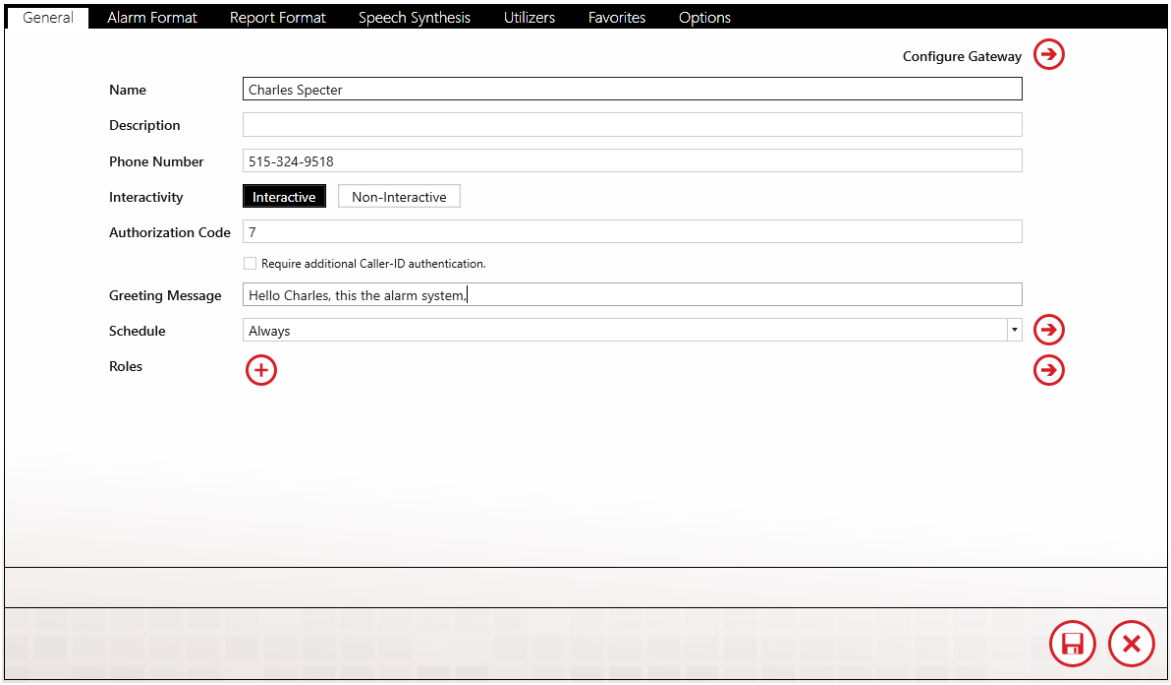


WIN-911 allows users to save their messages and automatically stores undelivered messages. How long should WIN-911 keep these messages.?
This parameter can be entered using the slider bar or the text selector. The minimum entry is 8 hours and the maximum is 168.

Voice Connections

Connections specify a destination for alarm notification, as well as scheduled availability and permissions. Voice connections also determine what your alarms and reports sound like on the phone.

General



Name

Each voice connection must have a unique name that identifies the particular connection.

Description

An extra text field for organization and administration purposes, similar to a code comment.

Phone Number

Enter the phone number of this particular connection. SIP account require, the country code at the beginning of the number. Many VoIP providers alternatively use an alpha-numeric string in place of a phone number. It is acceptable to assign a unique phone number to multiple connections if your situation warrants such action; however, a warning message will be generated to inform the WIN-911 administrator that a pre-existing connection already uses this number/string and lists the number of times it has been used.

Interactivity

Interactive

This mode of alarm notification is a two-way dialog between WIN-911 and the user. It requires the recipient to enter an authorization code and can be configured to allow remote acknowledgements by use of an ack code. The user can optionally be given permission to make inbound calls to request alarm conditions and reports.

Note: The star key "" can be used at anytime to have WIN-911 repeat the current segment of the message and the zero key "0" can be used to move the alarm message back one level. The message can be backed up as far as the main menu and then a subsequent zero key will end the call.*

Non-Interactive

This mode of alarm notification is a one-way transmission of alarm messages. It only conducts outbound calls, reports the alarm conditions, and disconnects the call on completion. It is intended for public address announcements and leaving

messages on voice mail. It does not accept user input or answer inbound calls.

Authorization Code

Interactive calls require user authentication by entering a numeric code that can range from one to 24 digits in length.

Allow call in only from this phone number for this connection

Checking this box will cause WIN-911 to refuse access to this user if he/she calls in on another line than the one listed in the Phone Number as identified by caller ID.

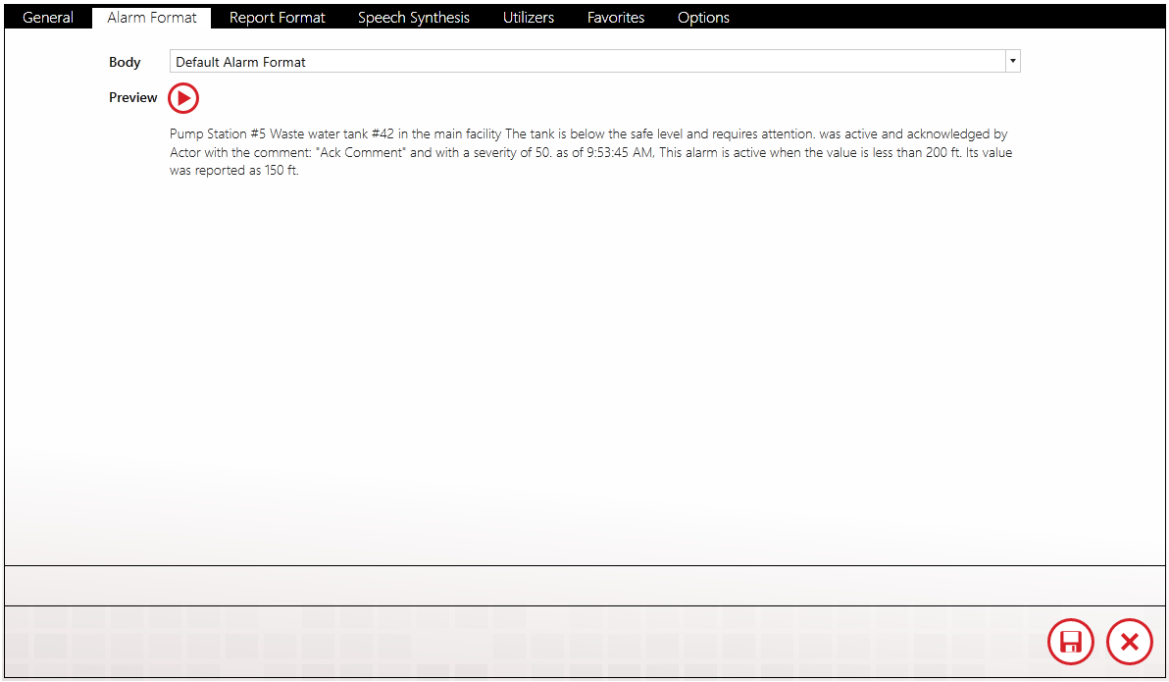
Schedule

View or select the schedule that WIN-911 will honor when sending alarm and report messages. A connection can have only one assigned schedule, but a schedule can contain multiple appointments. See Schedules.

Roles (for use by Advanced Tactics)

View or assign roles to the selected connection by clicking the add button in edit mode. Each connection can have multiple roles. See Roles.

Alarm Format



Body

The body of the voice notification consists of the information about the individual alarms. The body is played after the salutation, authorization code entry (Interactive only), and alarm enumeration segment, and before the ack code menu (interactive only). If the call is non-interactive then the authorization code entry and ack code menu are omitted. Each alarm message is announced as per the alarm format and then the ack code menu is presented before moving on to the next alarm message. Once all alarm messages and ack/save/delete menus are processed the user is returned to the main menu. Parenthesis indicate optional fields.

Short Alarm Format

Area, Item Description, Alarm Condition Description, Alarm State, Ack State, Actor, Event Time

Default Alarm Format

Area, Item Description, Alarm Condition Description, Alarm State, Ack State, Actor, (Ack Comment), (Severity), Event Time, Limit , (Value), (Units)

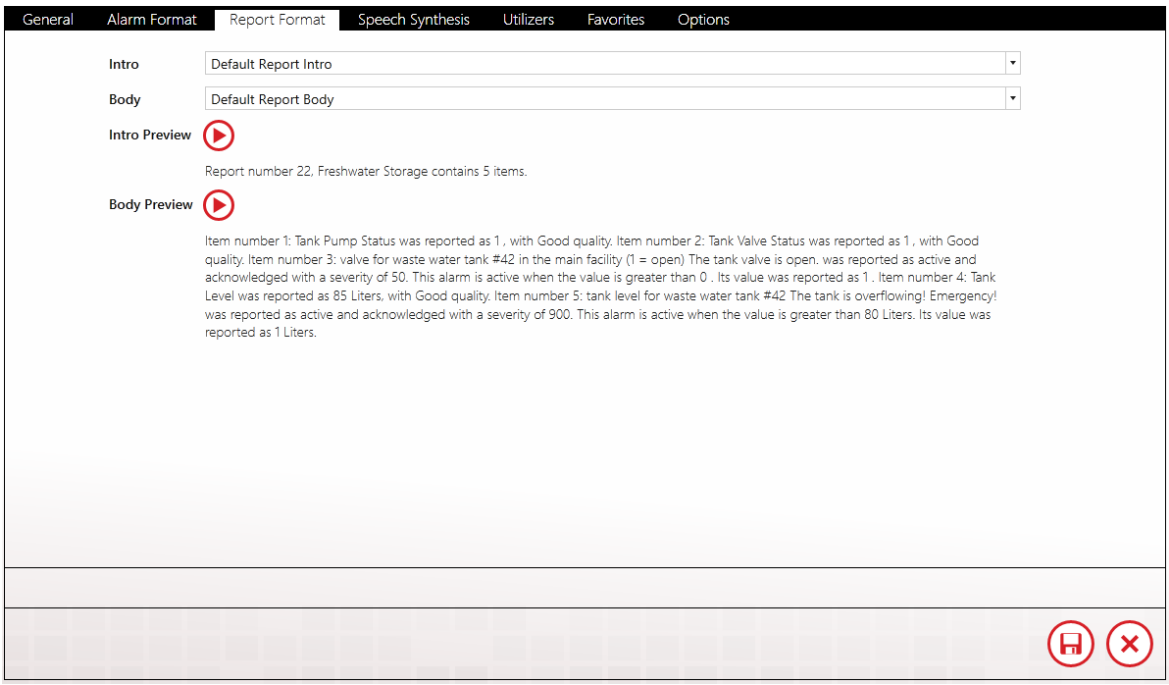
Long Alarm Format

Area, Item Description, Alarm Condition Description, Alarm State, Ack State, Actor, (Ack Comment), (Severity), Event Time, Limit , (Value), (Units), (Activation Time), (Label)

Preview

Click the play button to hear a sample of the alarm message format that the user will hear.

Report Format



Intro

The introduction of the report identifies the particular report and enumerates the number of items it contains.

Short Report Intro

Report Description, Total Number of Items

Default Report Intro

Report Number, Report Description, Total Number of Items

Body

The body of the voice report consists of the information about the individual items. The body is played after the salutation, authorization code entry (Interactive only), and report menu. If the call is non-

interactive then the authorization code entry and ack code menu are omitted. Each item in the report is announced as dictated by the report format body. Once all items are processed the user is returned to the main menu.
Parenthesis indicate optional fields.

Short Report Body

Data Items:
Item Number, Item Description, Value, Quality

Alarm Items
Item Number, Area, Item Description, Alarm Condition Description, Alarm State, Ack State, Actor, Event Time, Limit, (Value), (Units)

Default Report Body

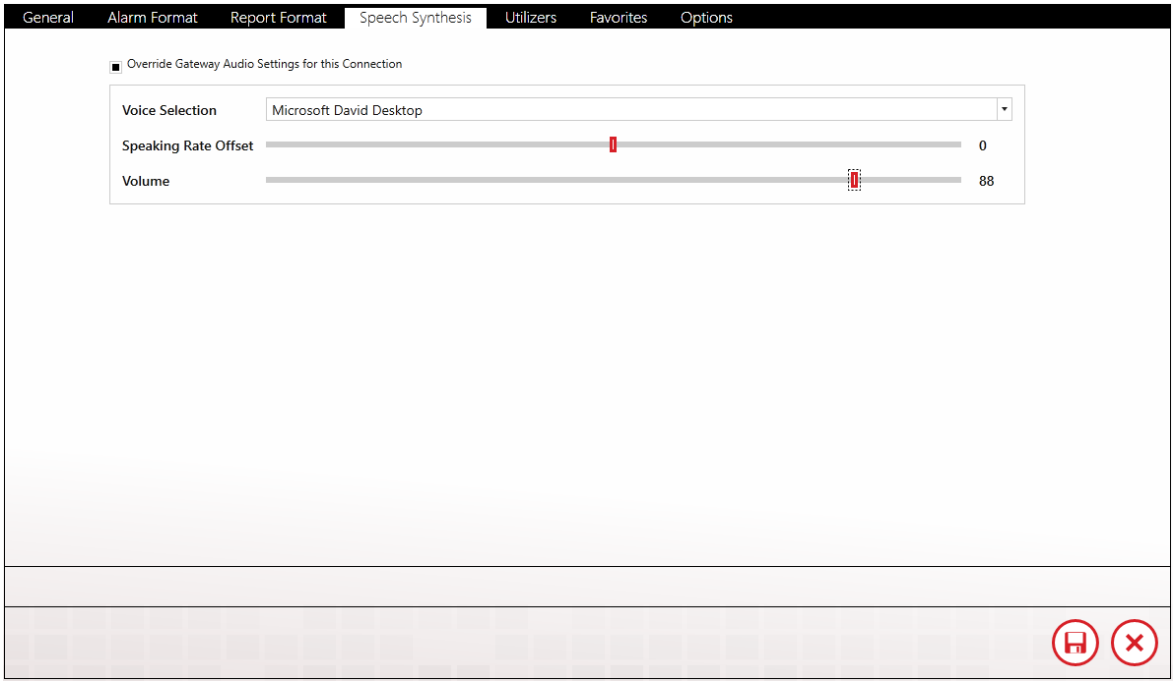
Data Items:
Item Number, Item Description, Value, Quality, (Labels)

Alarm Items
Item Number, Area, Item Description, Alarm Condition Description, Alarm State, Ack State, Actor, (Ack Comment), (Severity), Event Time, Limit, (Value), (Units), (Labels)

Intro and Body Preview

Click the play button to hear a sample of the report format that the user will hear.

Speech Synthesis



Override Gateway Audio Settings

Each voice connection has to option to substitute the global speech synthesis setting for the ones set on this page. If a particular user is hearing-impaired then his/her connection can be set to use a higher volume than the rest of the users.

Voice

Select the Text to Speech voice that WIN-911 will use to conduct voice alarm notification. The voice must use SAPI 5 or higher speech engine.

Speaking Rate Offset

Modify the default rate of speech -10 to 10 with the slider bar to refine the speech rate for your application.

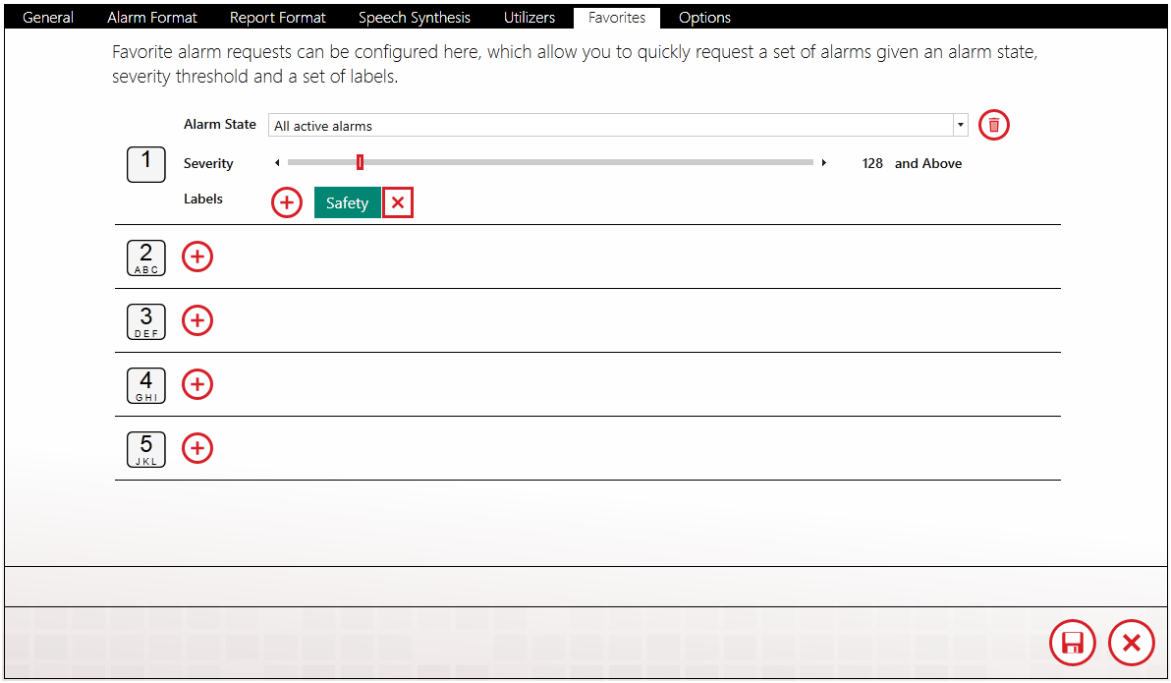
Volume

Modify the volume of speech -100 to 100 decibels with the slider bar to refine the volume for your application. This is a global setting that can be overridden in Connections>Speech Synthesis section for individual connection.

Utilizers

The Utilizers tab is a booking keeping device that lists all of the tactics associated with this contact. When utilizers are present WIN-911 prevents the contact from being deleted. If you wish to delete the contact you will first have to modify the utilizing tactic in a manner that will unlink it to this contact. Once all utilizers are cleared, the contact can be safely deleted.

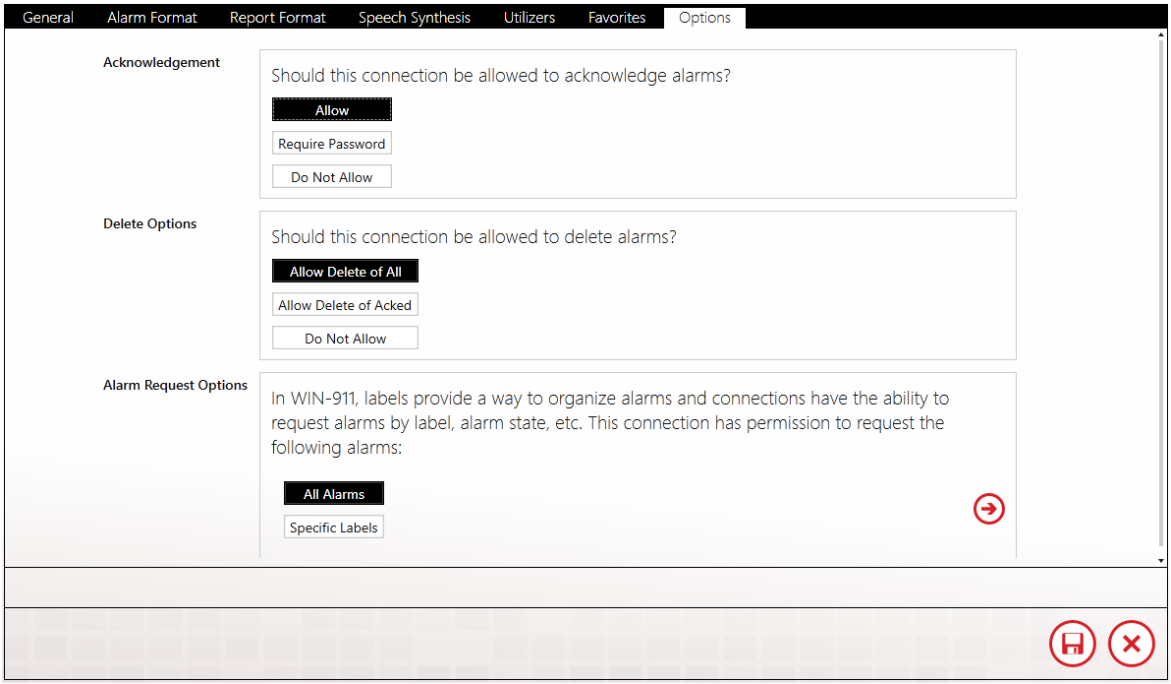
Favorites



Favorite alarm requests can be configured here, which allow you to quickly request a set of alarms given an alarm state, severity threshold and a set of labels.

Each connection can be configured for as many as five favorites filters. Each of the selected alarm properties (Alarm State, Severity, and Labels) are combined together to define the filter in such a way that the alarm would have to fall within the range of all defined properties to be included in the request.

Options



Acknowledgement

Should this connection be allowed to acknowledge alarms?

Allow

Allows the user to acknowledge the alarm by pressing the One key.

Require Password

Allows the user to acknowledge the alarm by entering the assigned connection ack code.

Do Not Allow

Default selection that does not offer the user the option to acknowledge the alarm.

Delete Options

Should this connection be allowed to delete alarms?

Allow Delete of All

Allows the user to delete all of his/her alarm messages by pressing the One button.

Allow Delete of Acked

Allows the user to delete all of his/her acknowledged alarm messages while retaining the those which have not been acked.

Do Not Allow

Default selection that does not offer the user the option to delete alarm messages.

Alarm Request Options

In WIN-911, labels provide a way to organize alarms and connections have the ability to request alarms by label, alarm state, etc. This connection has permission to request the following alarms:

All Alarms

Specific Labels

Roles

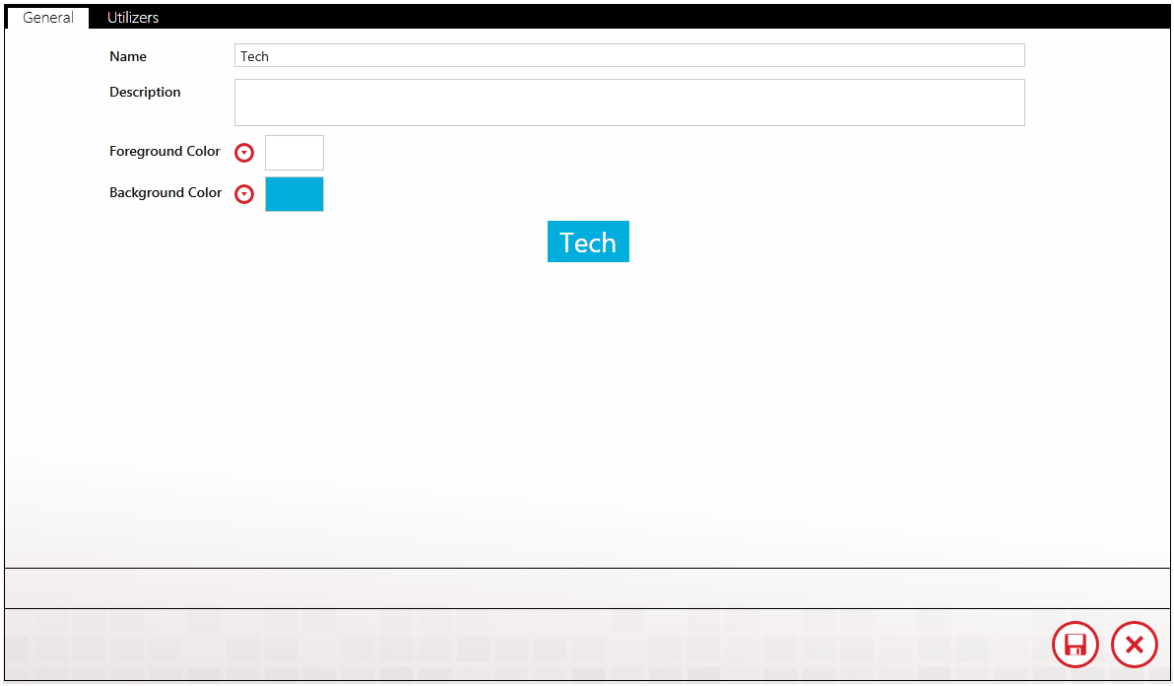
Roles represent a label for organizing connections based on availability, location, or responsibility. Roles can be used in a notification tactic to notify all connections with something in common.

Note: Roles are utilized by advanced tactics only.

Roles Collection Selector List

On the left side of the roles workspace is a master list of all defined roles. Each role object contains two properties, the Name and Description, that are displayed in columnar format. These properties can be used to sort and filter roles using tools provided within the form.

Role Workspace Editor



Clicking one of the edit buttons below the roles list or selecting one of the individual roles will bring up the Role Workspace Editor to the right of the list. This environment allows the WIN-911 Administrator to create roles to meet the exact needs of his/her specifications.

Edit/View Mode

The roles workspace (like any WIN-911 workspace) can be toggled between view mode (which allows the WIN-911 Administrator to view the details of the role), and edit mode (which allows the properties of the role to be changed). In view mode, the edit icons appears at the bottom right of the workspace. In edit mode the edit icons are replaced with the save and cancel icons.

Note: The Roles page can be navigated away from while the workspace is in edit mode. No changes will be saved/applied until the Administrator navigates back to the Roles page and clicks the save icon. All changes made prior to the navigation will remain available for saving until the browser session is closed.

Name

Each Role must have a unique name that identifies the particular Role.

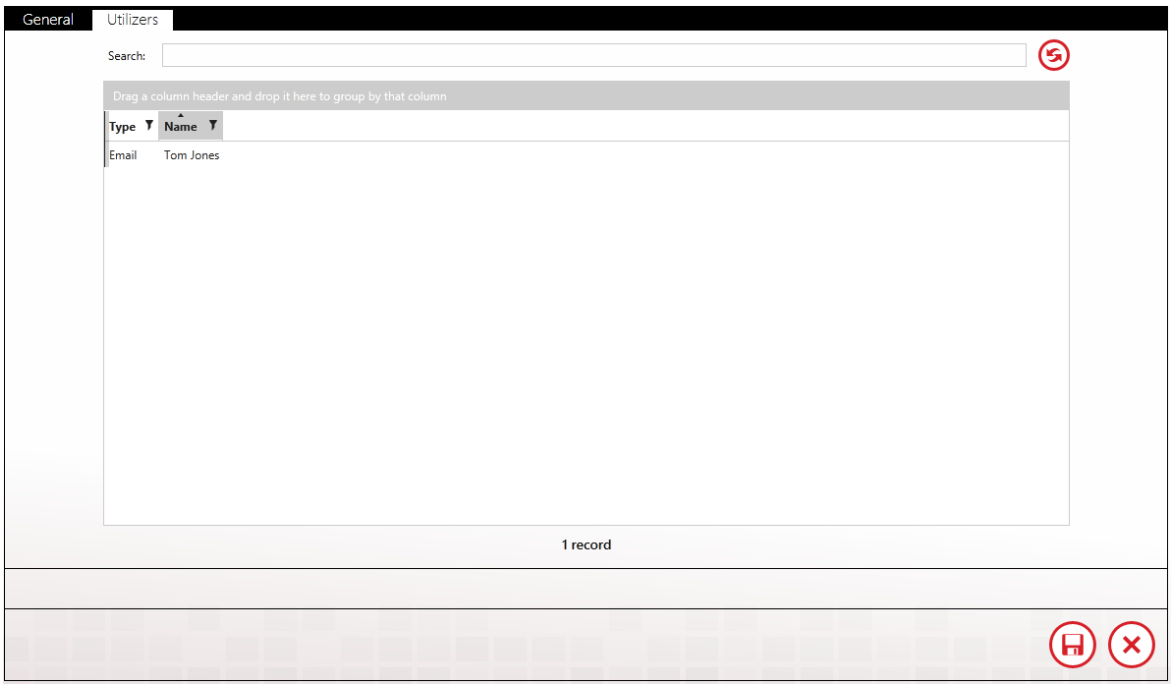
Description

An extra text field for organization and administration purposes, similar to a code comment.

Colors

Each role will You have a color pattern to help visually organize the connections. The WIN-911 Administrator can select a background and foreground (text) color for each role. The color picker for the foreground and background colors are invoked by clicking the associated red icon next to the left of the color to be edited. He/She can preview the current selections with the "what-you-see-is-what-get" presentation of the role provided below the color editing tools.

Utilizers

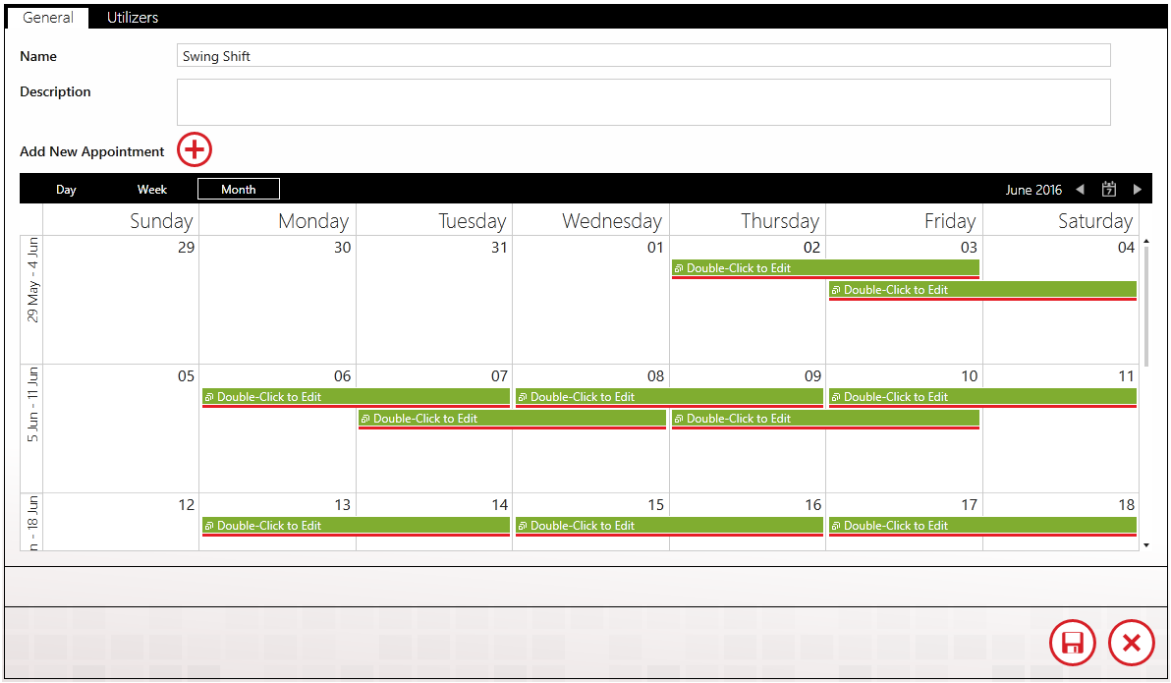


The Utilizers tab is a booking keeping device that lists all of the contacts associated with this role. When utilizers are present WIN-911 prevents the role from being deleted. If you wish to delete the role you will first have to modify the utilizing contacts in a manner that will unlink it from this role. Once all utilizers are cleared, the role can be safely deleted.

Schedules

Schedules define the availability of connections and can be used in a notification tactic to control notifications. They can occupy a single space in time, like an appointment, or be comprised of a pattern of appointments which can recur based on days, weeks, months and even support floating holidays.

WIN-911 provides a suite of predefined common schedules. The default schedule is "Always". These schedules are hard coded and not modifiable. If the specifications of a particular tactic require a different schedule than the ones provided, the WIN-911 administrator can create a custom schedule.



Name

Each schedule must have a unique name that identifies the particular schedule.

Description

An extra text field for organization and administration purposes, similar to a code comment.

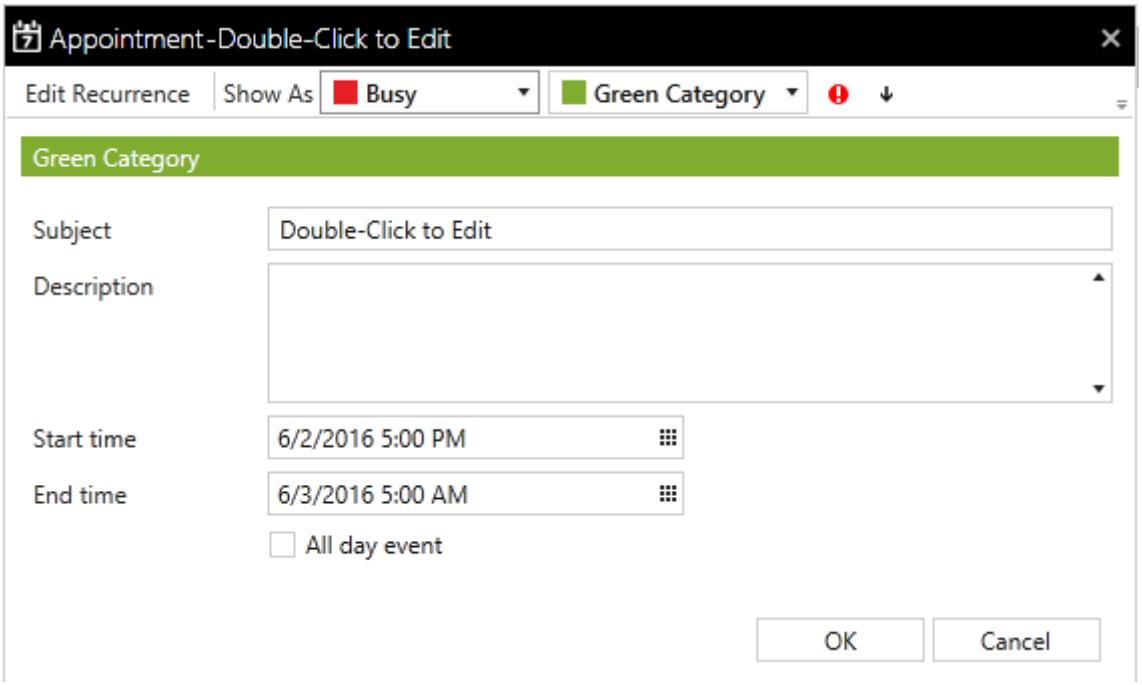
Calendar/Agenda

Beneath the description text box is a color-coded calendar display with three view formats: Day, Week, and Month. The default view is month, which is highlighted on the left side of the black view selector bar across the top of the calendar. The view can be toggled by clicking the desired view name. On the right side of the view selector bar is the currently selected date and time and navigation arrows for advancing the view up or down the date and time selection. In this view, the user can navigate to a particular point in time and examine the schedule definition.

Appointments

Each schedule can be comprised of any number of appointments to meet the users' exact needs. Each appointment can have its own subject, description, start and end times, recurrence pattern, category and priority.

Once in edit mode you can add a new appointment by highlighting the date and clicking the "Add New Appointment" icon, followed by "Double-click to Edit". If the appointment is part of a series, the appointment editor asks if you wish to modify this single instance or carry the modification throughout the series.

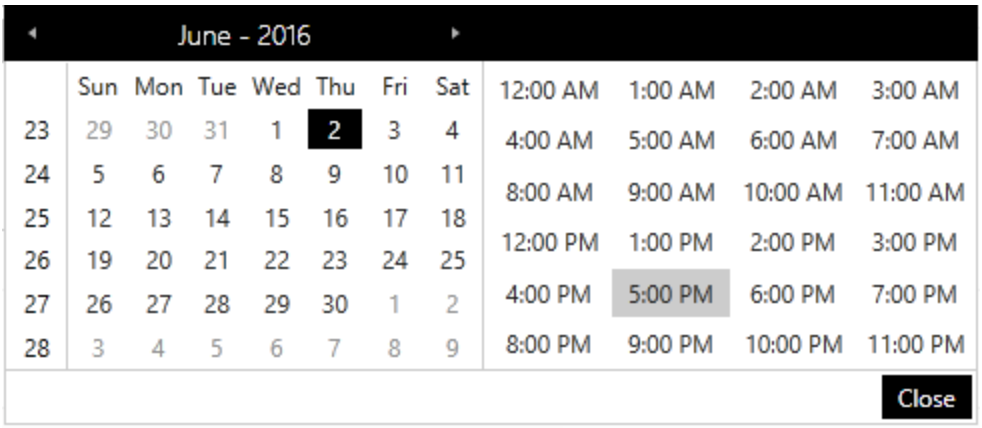


Subject

Each appointment may have a subject/title that identifies the particular appointment. This subject need not be unique.

Start/End time

Input fields to select the beginning and end of a block of time the appointment occupies. The time and date can be entered manually following the provided format by clicking the calendar icon in the right corner of the entry field to bring up a time and date selection dialog box. The dialog only provides start and end times that begin on the hour or half-hour. If you need a finer resolution you will have to enter it manually.

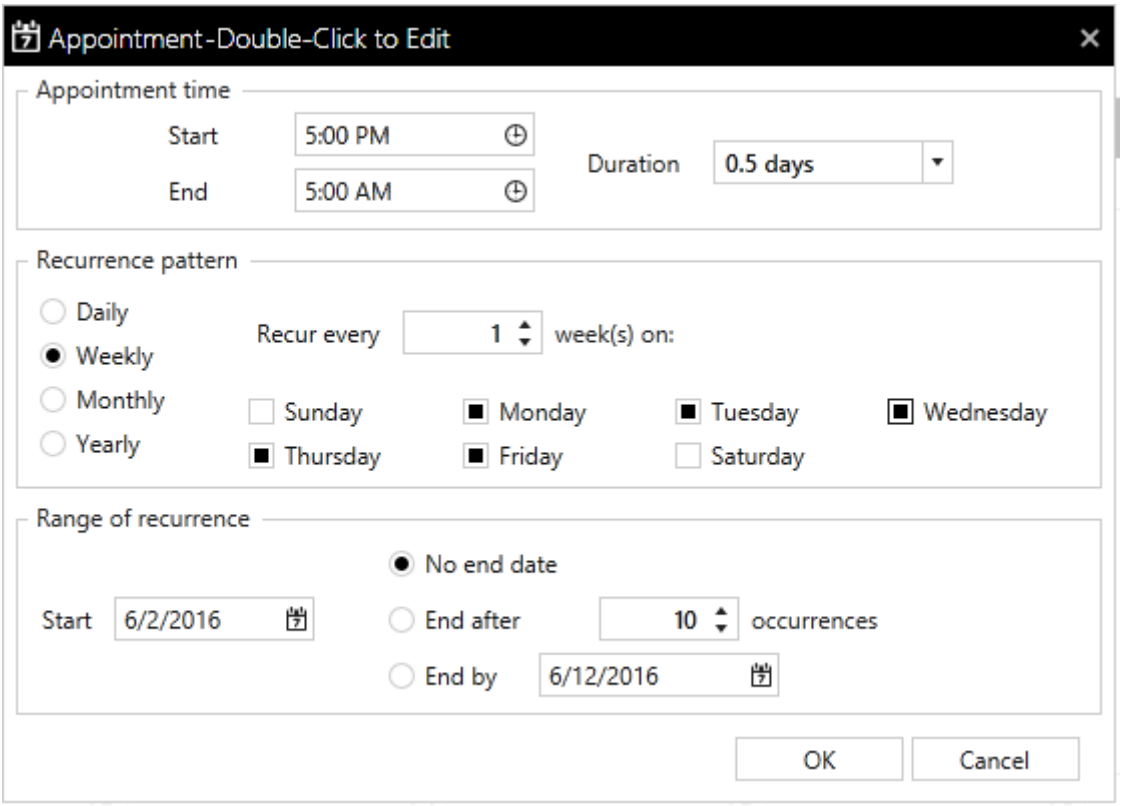


All day event

Check this box to select the entire 24-hour period of the selected day.

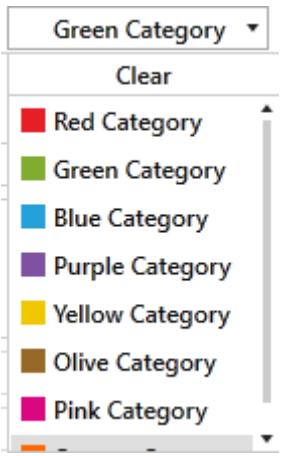
Edit Recurrence

If the selected appointment is to be a repeating series or part of a pattern click the edit recurrence button to bring up the recurrence dialogic box. From this window, you can edit the appointment time, establish a recurrence pattern designate the span of time the pattern is to honored.



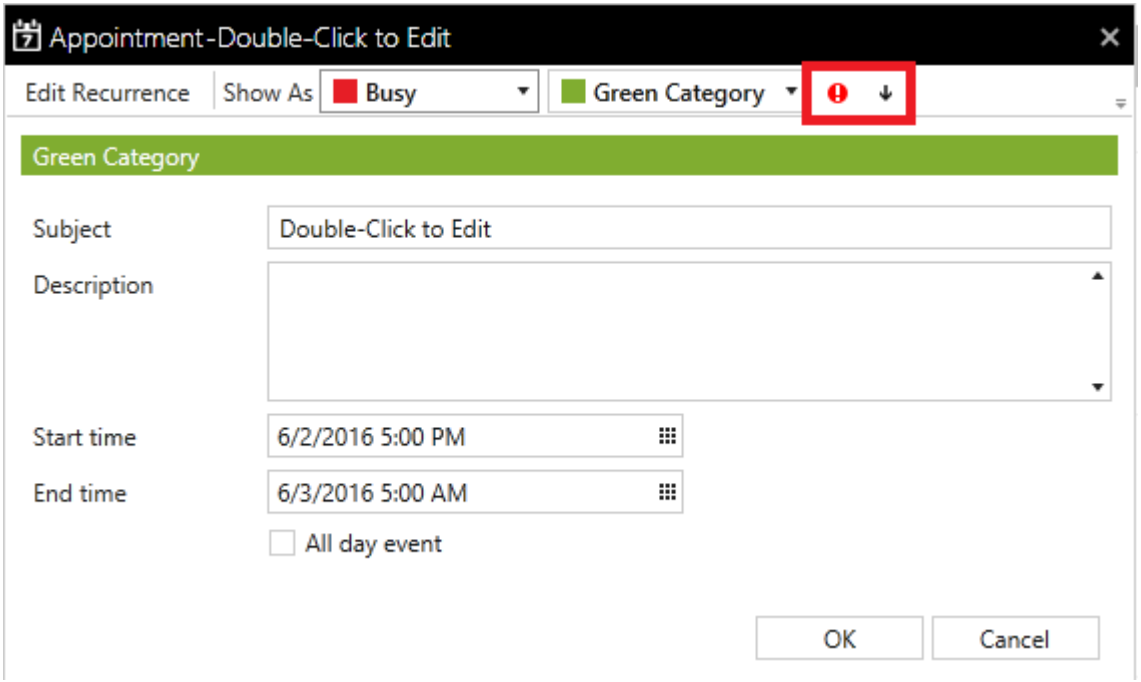
Categorize

Color-coded attributes that help the administrator visually organize schedules.



Priority

Priority is an optional attribute that designates the appointment as high (red exclamation point) or low (down arrow). Higher priorities take precedence over lower priority appointments.



Notification

Define how alarm notification should take place. Create and manage schedules and design custom notification strategies.

Design Basic Tactics

Basic Tactics makes it easy to define a list of connections for notification.

Design Advanced Tactics

The Advanced Tactics Workspace provides the WIN-911 administrator an easy to use, intuitive development environment that allows him/her to create anything from simple, single-step notification routines to complex logical flowcharts capable of circumstantial decisions and user interaction.

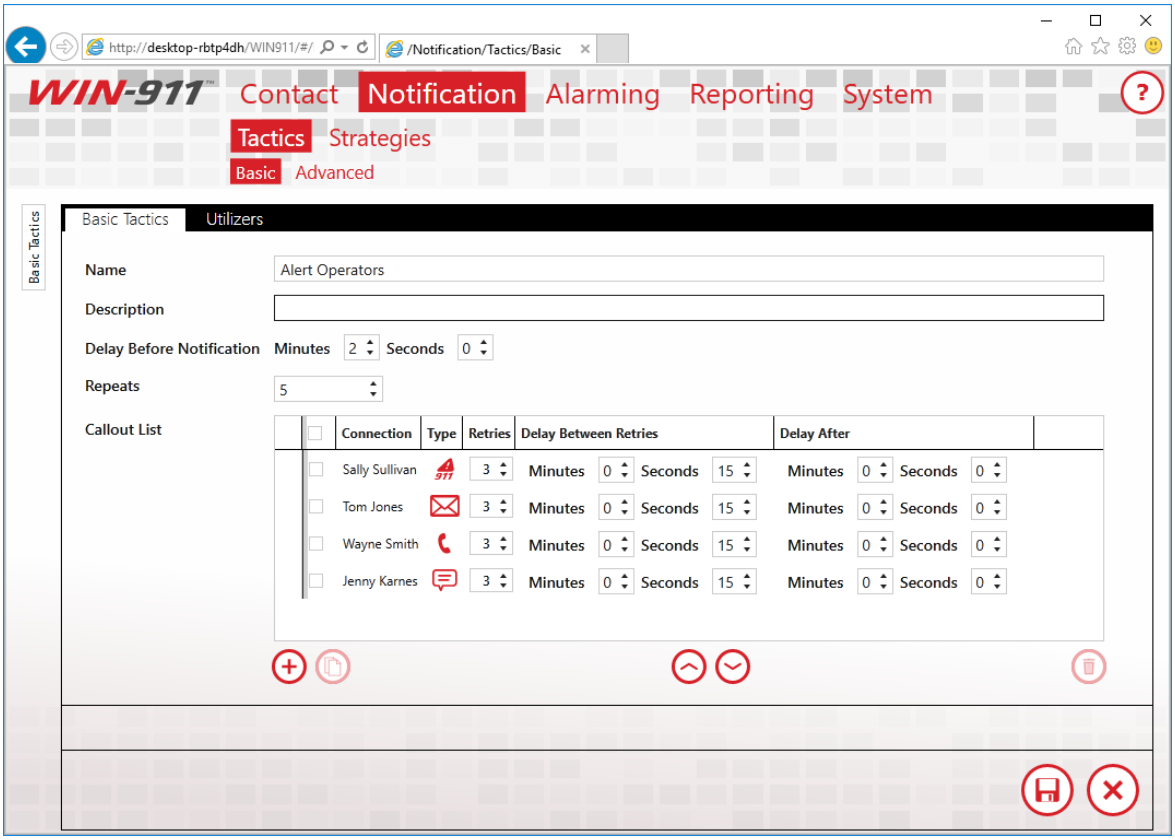
Manage Strategies

The Strategies Workspace provides the administrator with an easy to use, intuitive form for developing policies that invoke and regulate the tactics developed in the previous workspace based on alarm events and user input.

Basic Tactics

Overview

Basic Tactics are simple callout lists which deliver alarm notifications to the Connections listed within them. When a Basic Tactic is started, the list of connections is processed in the order they appear. Notifications are sent only to connections which are on duty at the time the notification attempt is made. Also, notifications are processed synchronously, that is, WIN-911 waits for each notification attempt to be completed before it continues on to its next action. In the event of a failure to send a notification to a connection, additional attempts may be configured. Delays may be placed between attempts to notify a connection and between different connections.



Name

Each Tactic, both Basic and Advanced, must have a unique name.

Description

An optional text field which provides additional context for the Tactic.

Delay Before Notification

The amount of time that should elapse before the list is processed. Use this to build in a delay for nuisance alarms. If the Tactic is stopped before the time period defined in this field has elapsed, no notification will occur.

Repeats

The number of times the callout list will be repeated, until it is stopped by a Strategy Policy. Set this to zero, if you wish the list to be processed once. The maximum number of Repeats is 99.

Callout List

This is the list of connections that will be notified and their order. Connections may be listed multiple times, scheduled for retires and spaced out using delays. Use the plus icon to add new connections to your list. The arrows will reorder connections within your list. The trashcan icon will remove entries from your list. Use the copy icon to duplicate an entry.

Connection	The name of the connection to be notified.
Type	This icon indicates the type of the connection to be notified.
Retries	The number of additional attempts that should be made to notify the connection, should failures occur.
Delay Between Retries	The amount of time to wait between attempts to notify the connection.
Delay After	The amount of time to wait after the connection has been notified before moving on to the next entry in the list.

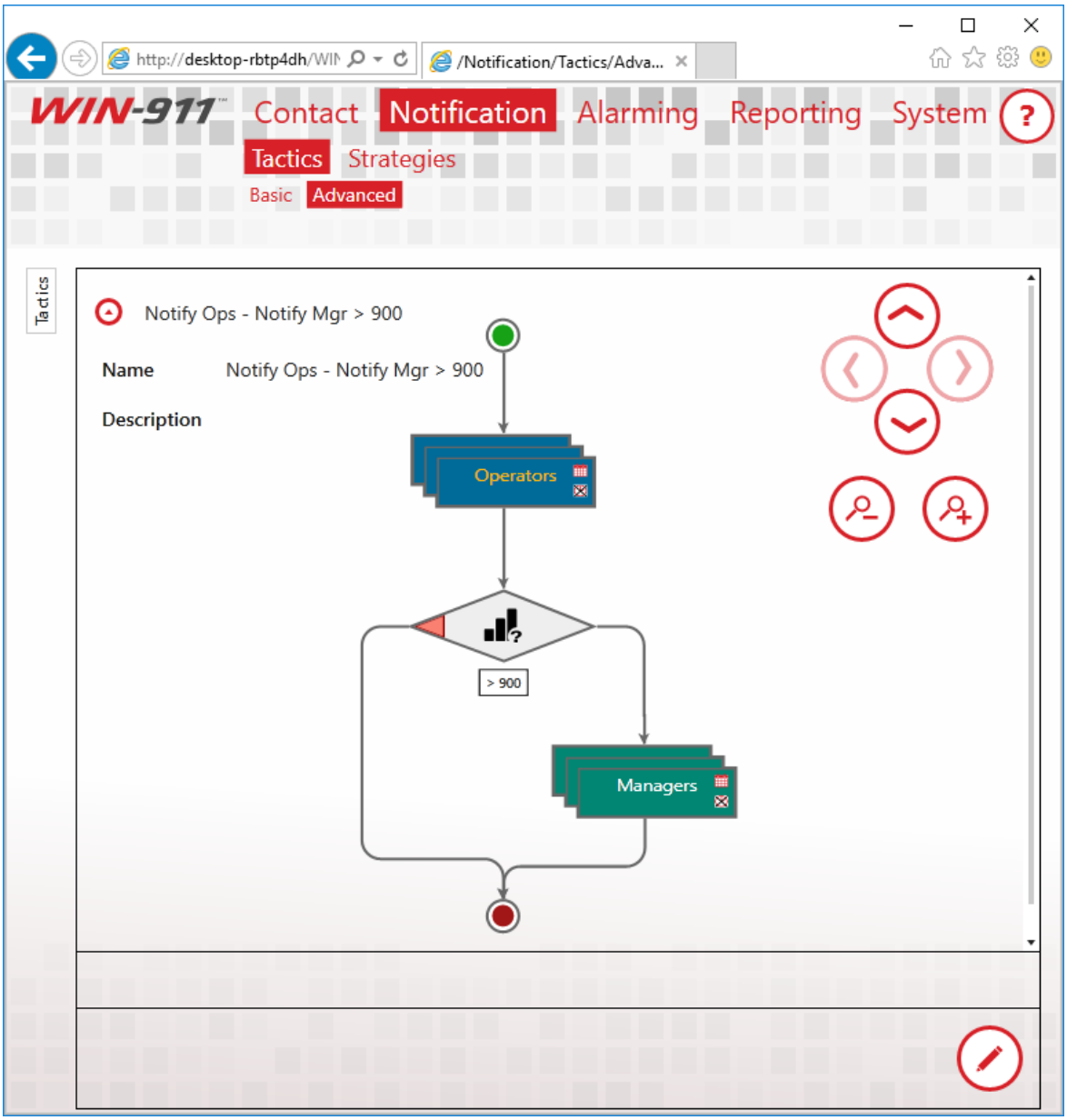
Utilizers

Tactics are referenced by Strategies. Tactics which are in use by a Strategy may not be deleted. Use the Utilizers tab to determine where a Tactic is used.

Advanced Tactics

Overview

An Advanced Tactic is a workflow, which may be started by a Strategy. Use these flowcharts to send alarm messages, reports, and acknowledge alarms. A tactic is constructed by dragging and dropping in various blocks into the chart. The following image depicts a tactic, which will send alarm messages to Connections tagged with the "Operators" Role, and, if the alarm has a Severity greater than 900, it will also send a message to Connections tagged with the "Managers" Role.



Blocks

There are a variety of blocks available to construct a tactic; each instructs WIN-911 to undertake a different action. Most of the blocks you will use are Notification Blocks, which allow you to send alarm or report messages to connections. There are also Decision Blocks, which enable your Tactic to branch based on the properties of the alarm that triggered the Tactic.

Notification Block

Sends the current alarm to the specified Connection.

Notify All Block

Sends the current alarm to all Connections tagged with the specified Role. If you do not specify a Role, the alarm is sent to Connection within the system.

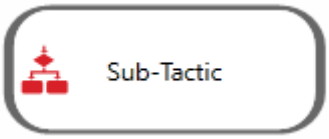
Report Block

Sends a Report to the specified Connection.

Report All Block

Sends a Report to all Connections tagged with the specified Role. If you do not specify a Role, the Report is sent to every Connection within the system.

Sub-Tactic



Starts another Tactic. Nesting Tactics recursively is not supported.

Ack-Decision

Branches the Tactic flow based on the acknowledgement state of the current alarm. If the alarm is acknowledged, the right path is taken. If the alarm is unacknowledged, the left path is taken.

Active-Decision

Branches the Tactic flow based on the active state of the current alarm. If the alarm is active, the right path is taken. If the alarm is inactive, the left path is taken.

Label-Decision

Branches the Tactic flow based on the Labels attached to the current alarm. If the specified Label is attached to the alarm, the right path is taken. If the Label is not attached, the left path is taken.

Severity-Decision

Branches the Tactic flow based on the severity attached

to the current alarm. If the severity of the alarm is greater than the value specified, the right path is taken. If the severity is less than or equal to the value specified, the left path is taken.

Timespan-Decision

Branches the Tactic Flow based on the amount of time that has passed since a specified event occurred and the time that the block is executed. The options for the initial event time are: the initial alarm time, the last time the alarm changed state, or the time at which the Tactic was started.

Delay Block

Delays Tactic execution for a specified period.

Ack Block

Acknowledges the current alarm when the block is executed. You may provide an acknowledgement comment. If your Data Source supports it, the comment will be passed along with the acknowledgement.

Loop Block

Loops the blocks placed within the loop for the number of times specified. The maximum is ninety-nine. It's a good idea to pair a Loop Block with a Decision Block so that a specific action can be repeated until some condition exists.

Notification Blocks

Synchronous vs. Asynchronous Notification

Notification Blocks can be configured to execute asynchronously or synchronously. When a block is asynchronous, the alarm message will be dispatched and the next block will be executed immediately. When a block is configured synchronously, the message is dispatched and the dispatcher waits to hear a response from the notifier which handles the message. If notification fails, another attempt, if

configured, may be made. Delays may be placed between notification attempts as well as between connections. Check the “Wait for Notification to Complete” checkbox on the Notification Block to make it synchronous.

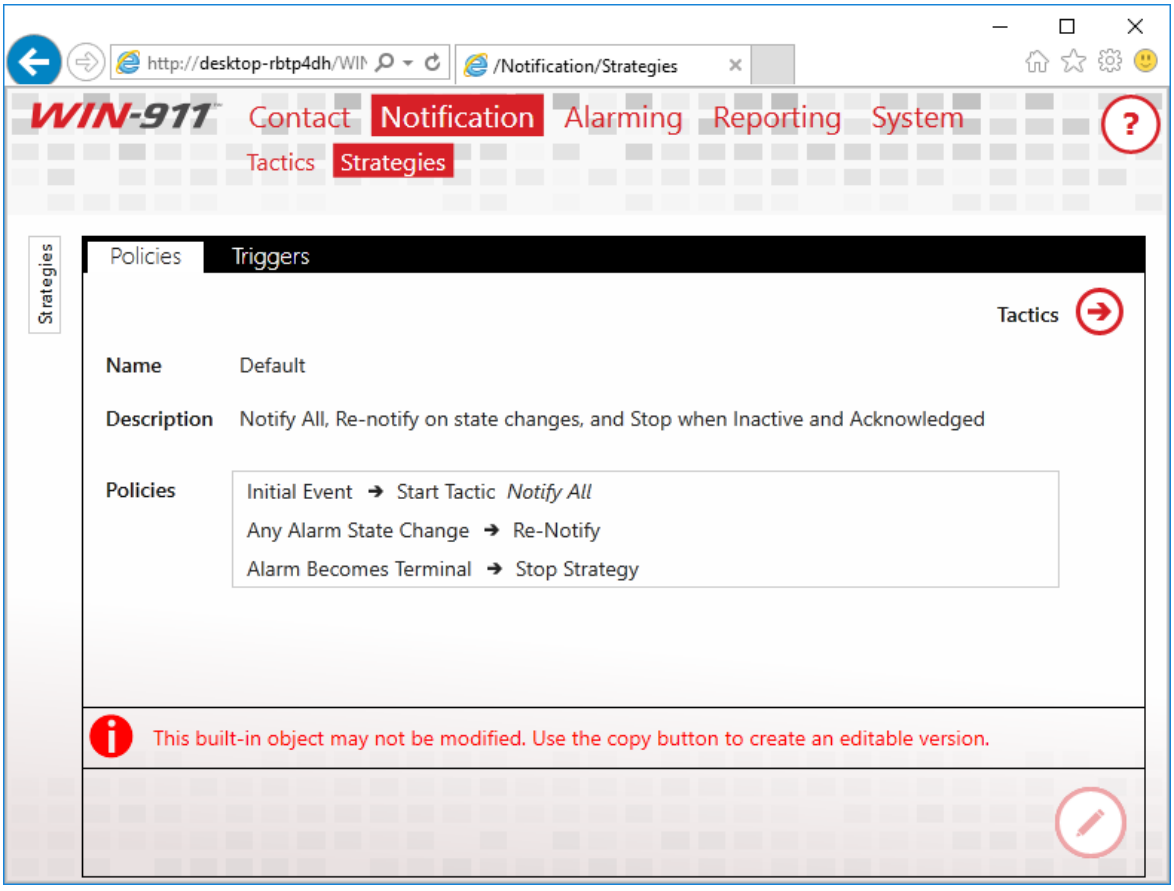
Schedules

Schedules determine when a Connection is available to receive alarms. This is a property of the Connection and is not specified within the Tactic. You may, however, ignore a Connection’s schedule, by checking the “Ignore Schedules” checkbox on a Notification Block. If the option is enabled, the notification will always be sent. Use this option for extremely important messages.

Strategies

Overview

Strategies define the set of actions to undertake when an alarm event is received. The condition that triggers the action and the action itself are referred to as a Strategy Policy. Alarms pass events into Strategies and the Strategy Policy list determines how WIN-911 will handle your system's alarm.



The Default Strategy, pictured above, has three policies. The first specifies that when the initial alarm event is received, a Tactic should be started called "Notify All." This Tactic is configured to notify

everyone in your WIN-911 system. The second policy specifies that when any update regarding the alarm is received, WIN-911 should send an updated notification to everyone who has previously received a message for the alarm. The final policy states that when the alarm becomes terminal, that is, when it is inactive and unacknowledged, the Strategy should stop executing.

To reiterate, alarms send events to Strategies, and, if the event matches a specified condition, action is taken by WIN-911. This action is, generally, to start or stop a Tactic. Tactics specify the details regarding the actual notification.

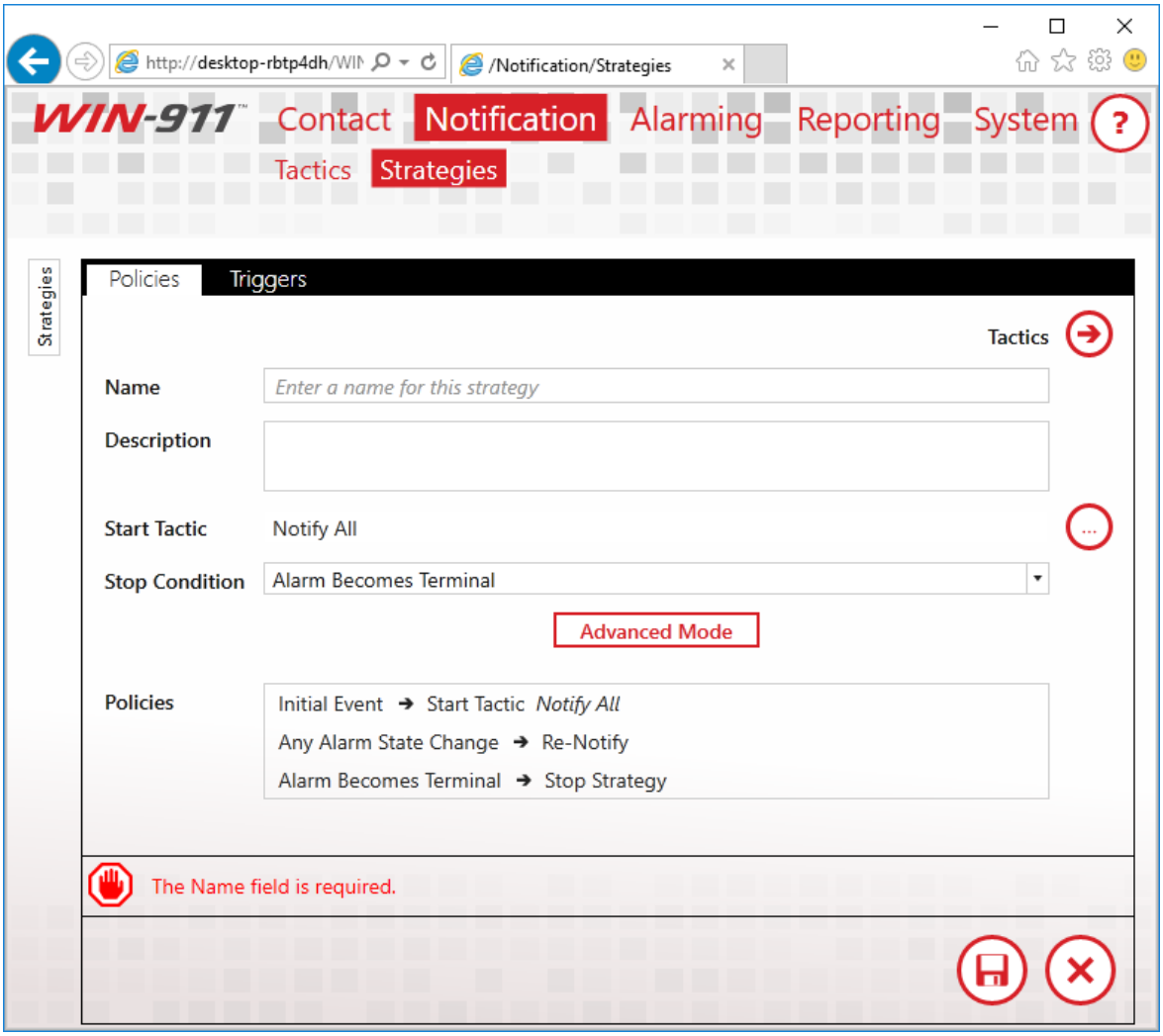
Name

Use this field to provide a unique and informative name for your Strategy. This name will be displayed in your logs and is also displayed in the list of Strategies.

Description

Use this field to provide additional context for your Strategy.

Basic Strategies and Advanced Strategies



All new Strategies begin as Basic Strategies. This is done to aid new users as they learn how Strategies function. A Basic Strategy has three policies, only two of which are configurable. The initial event must always start a Tactic, which you must select. Any alarm state change must always notify previously notified connections. Lastly, the Stop Condition is selectable. If a Basic Strategy does not meet your needs, simply click the Advanced Mode button and the full range of configuration will be unlocked. Once you press the Advanced Mode button, you cannot revert the Strategy to Basic Mode.

Policy Condition

Policy Conditions are used to determine when WIN-911 should take action regarding your alarm. When an event regarding your alarm is received that matches one of the Conditions you've specified some action may be taken. The list of available Conditions can be found in the table below.

Initial Event	The initial event for the alarm. This represents the first time the alarm is reported as being active.
Any Alarm State Change	The alarm's active or inactive state has changed.
Alarm Becomes Active	The alarm has gone into the active state.
Alarm Becomes Inactive	The alarm has gone into the inactive state.
Alarm Becomes Acknowledged	The alarm has been acknowledged.
Alarm Becomes Unacknowledged	The alarm has gone into the unacknowledged state.
Any Condition Change	The alarm's condition has changed. At this time, this is useful only for iFIX alarms.
Event Quality Changes	The quality, as reported by your SCADA or OPC server, has changed. This could mean the quality has changed from good to bad or from bad to good.
Upon Timer	A timer will be started when the strategy begins its execution. After the period you specify has elapsed, the action you specify will be triggered. This event will occur only once and the timer will be canceled, if the Strategy is stopped.
Upon Repeating Timer	A timer will be started when the strategy begins its execution. After the period you specify has elapsed, the action you specify will be triggered. This timer will be repeated until the Strategy stops.

Alarm Becomes Terminal	The alarm has gone into the Inactive and Acknowledged state.

Policy Actions

The actions which may be taken after a matching event is received are listed below.

Start Tactic	Start the specified Tactic. Use this action to start a Tactic and begin the notification process.
Restart Active Tactic	If the specified Tactic is executing, stop it and start it from the beginning.
Re-notify	Send an updated notification to all Connections which have previously received a notification regarding the current alarm.
Stop Tactic	Stop the specified Tactic.
Stop All Tactics	Stop all Tactics launched by this Strategy.
Stop Strategy	Stop this Strategy and all Tactics launched by this Strategy. This will stop all Policy evaluation, including all Timers.

Triggers

The list of alarms and filters which are associated with the Strategy are displayed on this tab. Strategies which are in use may not be deleted. Use this tab to track down where a Strategy is referenced, so that you may delete it.

Alarming

Create, manage, and organize the alarms monitored by WIN-911.

OPC DA Settings

Setup your OPC DA Sources by defining connection settings and alarm conditions.

FactoryTalk A&E Settings

Setup your FactoryTalk Alarm and Event Sources by defining connection settings and alarm subscriptions.

Cimplicity Settings

Setup a direct connect with your CIMPLICITY Projects.

iFIX Settings

Setup your iFIX Source by defining Connection Settings and Alarm Conditions.

InTouch Setting

Setup remote and local connections to InTouch applications for alarm and data monitoring.

Organize with Labels

Labels represent a label for organizing alarms based on location, device, functions, severity, or other logical grouping. Labels can be used in a notification tactic to control notification.

OPC DA Overview

The OPC DA data connection allows WIN-911 to connect to a wide variety of HMI/SCADA systems by using a generic data exchange medium, OPC DA server. WIN-911 serves as a generic OPC DA client. WIN-911 only supports Data Access (DA) servers not Alarm and Event (A&E) servers. WIN-911 is capable of browsing tags in an OPC DA server and importing them into the WIN-911 configuration, where tag browsing is available.

If at any time WIN-911 loses connection to the OPC server, WIN-911 will attempt to re-establish its connection and continue to do so until the server is back online and the data is restored.

The OPC DA server passes raw values, or "Items", to WIN-911 on a pass-by-exception basis. Alarm events are derived from set-points (e.g. "On", "Off", "50 >", "4 <", etc.) that you enter and which WIN-911 will compare to the Items. When an Item meets or exceeds the set-point an alarm event is triggered by WIN-911.

The OPC DA connection also supports watchdog alarms. Watchdog alarms are based on an item's value NOT changing within a specified period of time. This type of alarm is useful for monitoring the operational status of a server/device. OPC DA servers only update clients when item value's change. If a server stops responding the client can only assume that the data has not changed but is still valid. Watchdog's are provided to guard against this by triggering an alarm event when an item's value fails to change within a specified amount of time.

WIN-911 can monitor an item's changing value by setting the timeout value greater

The OPC DA Conversation

There are three parts to an OPC DA Address: The Machine Name or IP Address, Server Class, and the ItemID. The Machine Name specifies the network node that the server resides on, the Server Class specifies the server that contains the data, and the ItemID is the specific data point within the server.

Preparing Your Computer for Remote OPC DA

Setup DCOM

Run the DCOM configuration utility by selecting Start and typing *dcomcnfg* in the *Search Programs and Files* text entry box. Highlight Component Services, then Computers, then right-click My Computer and select Properties which will bring up the Component Services dialog. Select the Default Properties tab and check Enable Distributed COM on this computer. In addition, make sure that the Default Authorization Level shows Connect and the Default Impersonation Level is set to Identify. Uncheck the additional security for reference tracking box (match the settings below). Set default security right by selecting the Default Security tab.

Configure Access Permissions for the computer's DCOM via the Default COM Security tab. On the Access Permission window you can add individual users and groups to grant access to this particular computer on the DCOM level. Make sure you select the correct domain or workgroup user list from the pull-down menu. Here you

select your computer's domain or workgroup. For initial test purposes include Everyone in the Grant Access list.

Configure OPC DA Sources

Specify how to connect to your OPC DA sources.

Name

Each data source must have a unique name that distinguishes it from the others.

Description

An optional text field for providing the user with context. Such information can contain location data (like Lift Station 22), or an explanation of the event that conveys useful information to the user that is not provided elsewhere.

Single Source Definition vs. Group of Redundant Sources

Single Source Definition is the default OPC DA source type which interfaces a single server. If the source is an array of redundant servers you will need to use to specify each server that is part of the Group.

Machine Name

Select the computer that hosts your OPC DA server. You can use the browse button to the right to browse for your server. Type "localhost" if the OPC DA server in on the same machine as WIN-911.

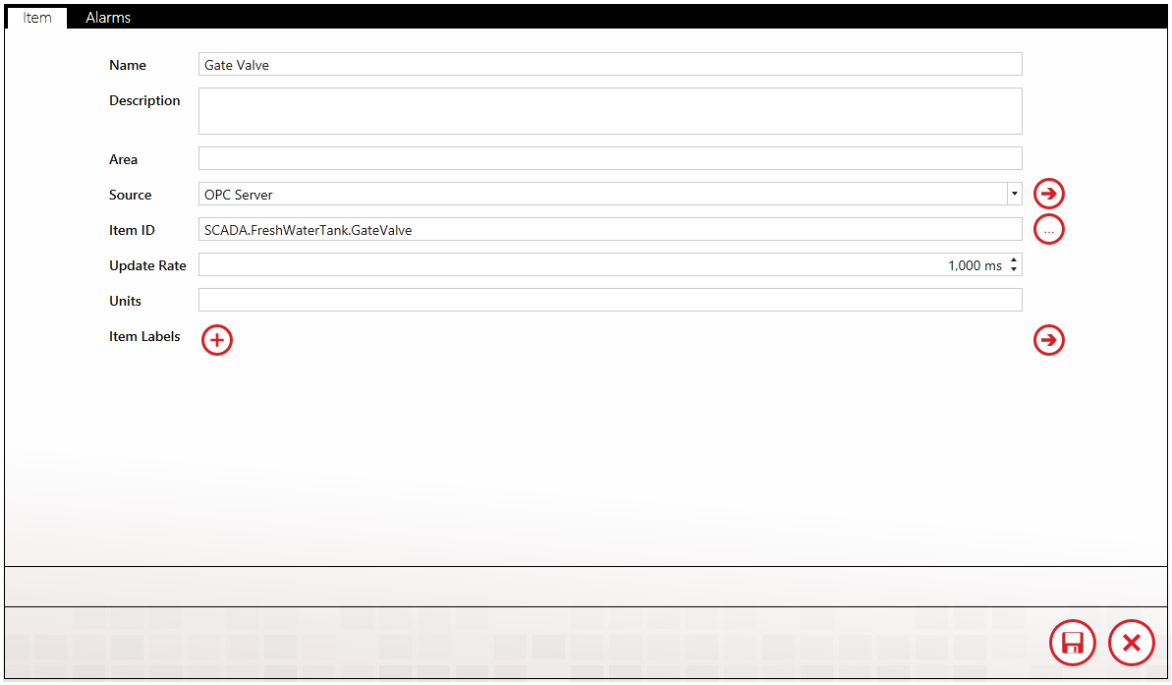
Server Class

Enter the OPC DA server name. You can type the name manually or you can use the browse button to the right to select the server you wish to connect to.

Configure OPC DA Alarms

Configure alarm conditions on data provided by an OPC DA source. Alarms represent specific alarm conditions such as a tank level exceeding a high limit or a valve being opened that would normally be closed and require an alarm responder to be notified. Alarms trigger a notification strategy.

Item



Name

Each item must have a unique name. When WIN-911 delivers alarm messages, this is the name it will use. The name can be independent of the Item ID, which must match the syntax of the OPC DA server and is often cryptic.

Description

An extra text field for organization and administration purposes. It is intended to allow for elaboration on the information concerning the alarm/item. Such information can contain location data (like Lift Station 22), or a description of the data that provides additional context.

Area

The area is an optional attribute that can be assigned to help identify the item in environments that may have multiple sections with similar functions, such as a waste water treatment plant with multiple lift stations. An area example would be "Lift Station 22". When importing from WIN-911 Version 7, the grouping name will be imported as the area.

Source

Select the OPC DA server name.

ItemID

The "ItemID" is the name of the tag as it exists within the OPC DA server and is the name that WIN-911 uses to communicate with the server. You can type the name in manually using the text entry box provided, but it is highly recommended that you use the browse button to the right and select the ItemID directly from the server for the sake of convenience and the prevention of errors.

Update Rate

You can set the update rate at which the OPC DA data source module refreshes its data. The default value is 1.000 ms.

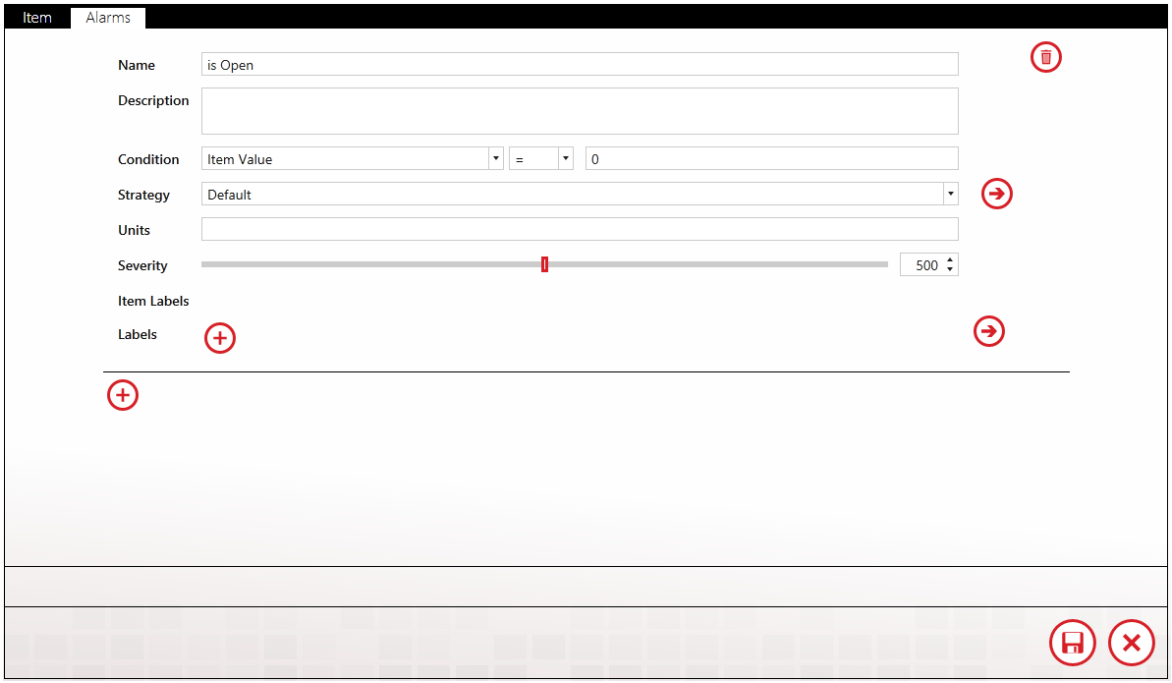
Units

The Units field is optional. Use it to add engineering units. to your notifications.

Item Labels (for use by Advanced Tactics)

The "Item Labels" are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements. See Labels.

Alarms



Note: Each individual item can be assigned any number of alarm conditions.

Name

Each alarm must have a unique name. When WIN-911 delivers alarm messages, this is the name it will use.

Description

An optional text field for providing the user with context. Such information can contain location data (like Lift Station 22), or an explanation of the event that conveys useful information to the user that is not provided elsewhere.

Condition

The value or state of the OPC DA item that defines the alarm condition.

Item Value: Alarm based on the item's value. The relationship can be equal to, not equal to, greater than, less than, or a combination thereof.
Quality: Alarm based on the OPC DA item's attribute.
Watchdog: Alarm based on an item's value NOT changing within a specified period of time. This type of alarm is useful for monitoring the operational status of a server/device. OPC DA only updates clients when value's change. If a server stops responding the client can only assume that the data has not changed but is still valid. Watchdog's are provided to guard against this by creating an alarm event when an item's value fails to change within a specified amount of time.

Strategy

The strategy that WIN-911 invokes when the alarm event occurs.

Severity

A number from 1 to 1000 that designates that urgency of an alarm event. It can be used as an organizational tool and be used in a tactic to determine how an alarm is dispatched. The default severity is 500.

Units

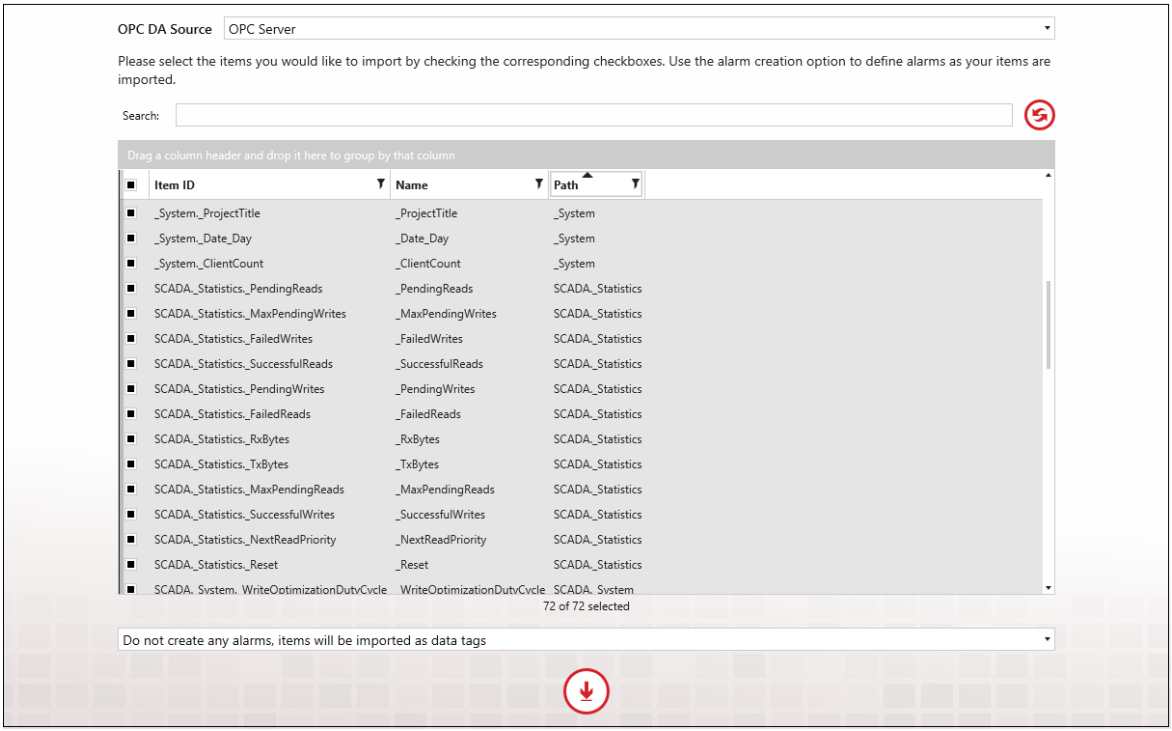
The Units field is optional. Use it to add engineering units. to your notifications.

Alarm Labels

The "Alarm Labels" are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements. See Labels.

Import from OPC DA Server

Import items from an OPC DA server on your local network. The OPC DA server should be configured as a source before it can be browsed for items to import.



OPC DA Source

Use the pull-down list to select the OPC DA server that you would like to conduct the import from. If there are no servers in the list, you will have to create one in the OPC DA Sources workspace.

See Configure OPC DA Sources.

OPC DA Item Import

If the OPC DA server supports browsing then the OPC DA module will generate a list of all items available for importing. Select the items you would like to import by checking the corresponding checkboxes. You can also create alarms on selected items while importing.

Import Item List

In the center of the import items workspace is a master list of all importable items. Each import item object contains three properties, the Name, ItemID, and Path, that are displayed in columnar format. These properties can be used to sort and filter import items using tools provided within the form. The active sorting column is indicated by a black triangle in the middle of the column header.

Selecting Import Items

The import item(s) is selected by clicking the check box to the left of the import item's properties. Multiple import items can be selected per import.

Sorting

When the name column header has a black triangle pointing down, the import items will be arranged by name in descending alphabetical order. Clicking on the triangle will reverse the list and cause it to be arranged in ascending order. A third click on the triangle will deselect the column. Any property column can be sorted.

Search

The search field will filter the import items collection selector list by suppressing the display of import items that do not contain the character string entered. Any property column can be searched. The search field will be highlighted yellow while the search filter is in session.

Filtering

On the right side of the property column heading is a black filter symbol. Clicking it causes a custom filter design form to appear. This form provides several options the WIN-911 administrator can use to exclude unwanted import items from being listed in the collection selector. "And/Or" expressions can be created that key on the selected property data for inclusion or exclusion. The selected property (Name or Description) column header will be highlighted yellow while the custom filter is applied. Any property column can be filtered.

Grouping

Dragging and dropping a property column header into the grey area above the import items list will cause the collection selector to group the import items accordingly. The collection selector now lists the title of the selected object in bold font with a drop-down arrow to the left. Click on the drop-down arrow and the collection selector will drop a list of all the import items that contain a particular object title. Groups can be compounded by dragging another object into the "Group by" field. Grouping can be removed by hovering over the group title and clicking the "X" that appears to the right of the title. Any property can be grouped.

Select Import Alarm Condition

Each import can be configured to automatically set an alarm condition, that will be assigned to each of the selected items by using the pull-down selector beneath the import item selection list. The alarm condition will be assigned the Default (Notify All) strategy. The alarm condition options are as follows:

- Do not create any alarms, items will be imported as data tags (default selection).
- Create an alarm on value = 0
- Create an alarm on value = 1
- Create an alarm on value "not equal to" 0
- Create quality alarm

Note: Caution should be used when automatically assigning alarm types to bulk imports. Upon completion of the import all new alarms will immediately go live and any that are in alarm condition will be subject to the default strategy "Notify All".

What is FactoryTalk Alarms and Events?

FactoryTalk A&E Overview

The FactoryTalk Alarm and Events source/direct connection provides a means of connecting to Rockwell's FactoryTalk Services. The WIN-911 direct connect interface to FactoryTalk provides access to alarms generated by FactoryTalk Alarm and Events.

Multiple data sources can be configured for FactoryTalk Alarms and Events. This allows the user to connect to multiple applications. FactoryTalk Alarms and Events supports the ability to reconnect to FactoryTalk Services if it ever loses its connection.

Note: The FactoryTalk Alarms and Events does not provide access to tag data.

Note: The FactoryTalk Alarms and Events does not yet support the following: reporting, Bypass, ALARM OFF command, and SUPPRESS command from FactoryTalk View.

FactoryTalk AE supports. Filters allow WIN-911 to subscribe to alarm events according a filter created by the WIN-911 administrator. The FactoryTalk filters based on Alarm Name, Alarm Class, and Severity. This expedites the WIN-911 alarm configuration process.

The FactoryTalk Alarms and Events tag properties are configured at the device level making all properties dynamic with respect to WIN-911. This means that a tag can be modified in FactoryTalk and those changes are automatically reflected in WIN-911.

FactoryTalk assigns one of four Priorities to Alarms: Urgent, High, Medium, and Low. WIN-911 can subscribe to FactoryTalk alarms based on the Priority. Priorities are configured at the data source level.

FactoryTalk A&E Subscriptions

The FactoryTalk Alarm & Event Source uses Subscriptions to access alarms from FactoryTalk.Subscriptions can be created to match against FactoryTalk names, classes, and/or severities. Subscriptions may be used across multiple servers to fetch existing alarms within. By default, a Subscription named 'All Alarms' is included.

Subscription

By default, Subscriptions will match all alarms when first created. Users can click the radio buttons to modify the filtering criteria. In the example below, specific Names and Severities are being targeted.

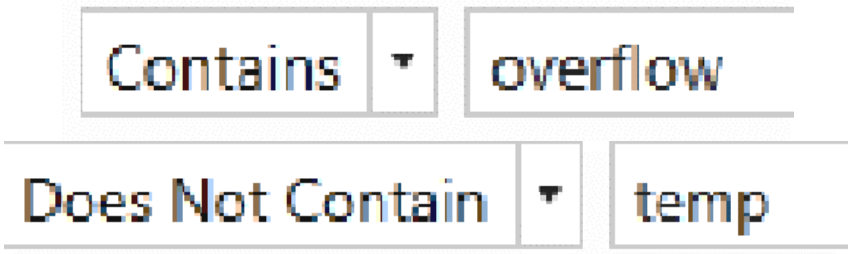
String Filters

Four types of string filters exist. They can be used to match against FactoryTalk Names and the Classes that your FactoryTalk Tags are assigned to in FactoryTalk Alarm & Events. String filters are case-sensitive.

The first and, easiest to use is the wildcard filter. Enter any string literal to match it exactly. Enter an asterisk to match any character any number of times. Enter a question mark to match any character one time.

- "Tank" will only match the string "Tank"
- "*tank" will match any string that ends with "tank." E.g. "Watertank," "Brite tank."
- "z?g" will match any string that begins with "z," ends with "g," and has one and only one letter between them. E.g. "zig," "zag."

Regular expressions can be used. Regular expressions are an advanced method of pattern matching. There are many resources available online that document their use.



'Contains' will match any string that contains the substring you enter exactly. 'Does Not Contain' will match the opposite.

Click the 'Add' button to create a new string filter under the respective category (e.g. tagname) with default values. Multiple filters in a category will be logically AND'ed.

Click the 'Delete' button to delete the selected string filter under the respective category.

Severity Filters

Severity filters are supported for FactoryTalk Alarm & Events. They can be created to match an inclusive range.

They can also be created to match a specific Severity.

Labels

Click the 'Add' button to the right of 'Labels' to add new Labels to this Subscription. At runtime, alarms matching the Subscription will have the specified set of Labels attached.

Click the 'Navigate' button to navigate to the Labels workspace. If any changes have been made to the Subscriptions tab, they will persist until the user navigates back to the Subscriptions tab.

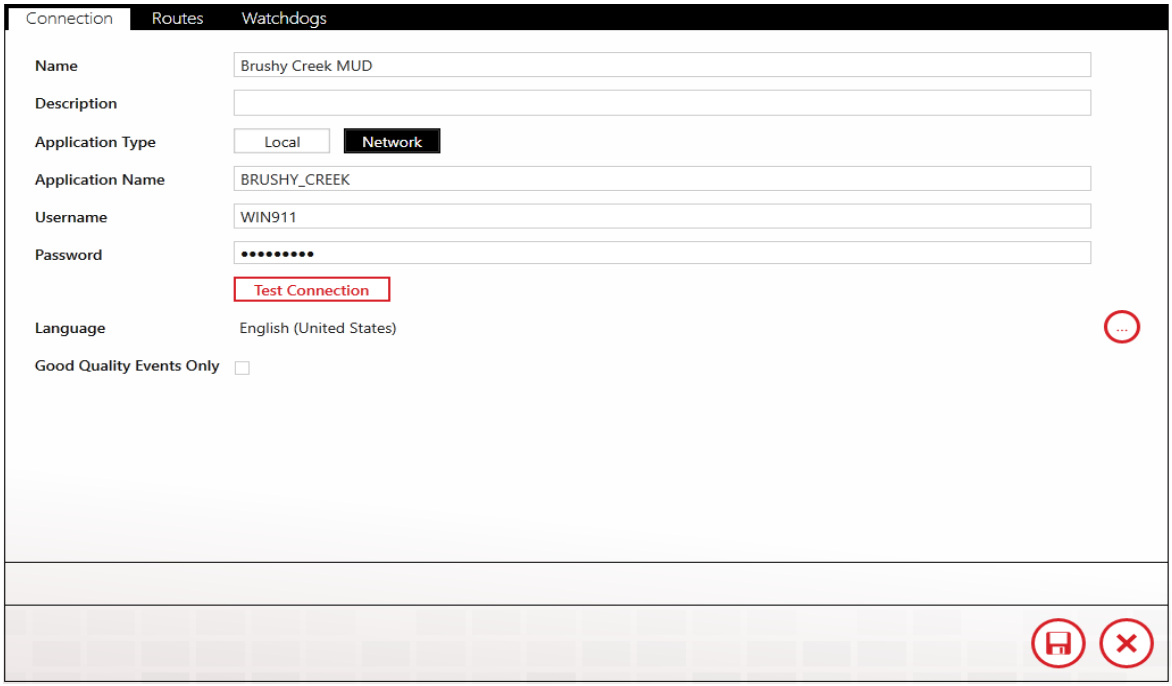
Click the 'Delete Label' button to delete the Label on the left.

Utilizers

This tab simply shows the user which Applications are currently using the Subscription that they are viewing. A Subscription cannot be deleted while in use.

FactoryTalk A&E Applications

Connection



Name

Enter a name for this connection. This name identifies this FTAE connection to WIN-911. It must be unique and should be meaningful and descriptive to the WIN-911 user.

Description

An optional text field for providing the user with context. Such information can contain location data (like Lift Station 22), or an explanation of the connection that conveys useful information to the user that is not provided elsewhere.

Application Type

Match the type of application to that of FactoryTalk. If it is a stand-alone system then select Local, but if FactoryTalk is running as a network application then Network should be selected.

Application Name

Match the FactoryTalk application name (as it appears within FactoryTalk).

Username/Password

Specify a FactoryTalk account user name and password for this application that has permission to access the FactoryTalk A&E Server. You may consider creating one especially one WIN-911.
Note: The password is encrypted.

Test Connection

Use this button to validate the Application, username, and password that was entered above. A success message indicates the connection parameters are correctly entered.

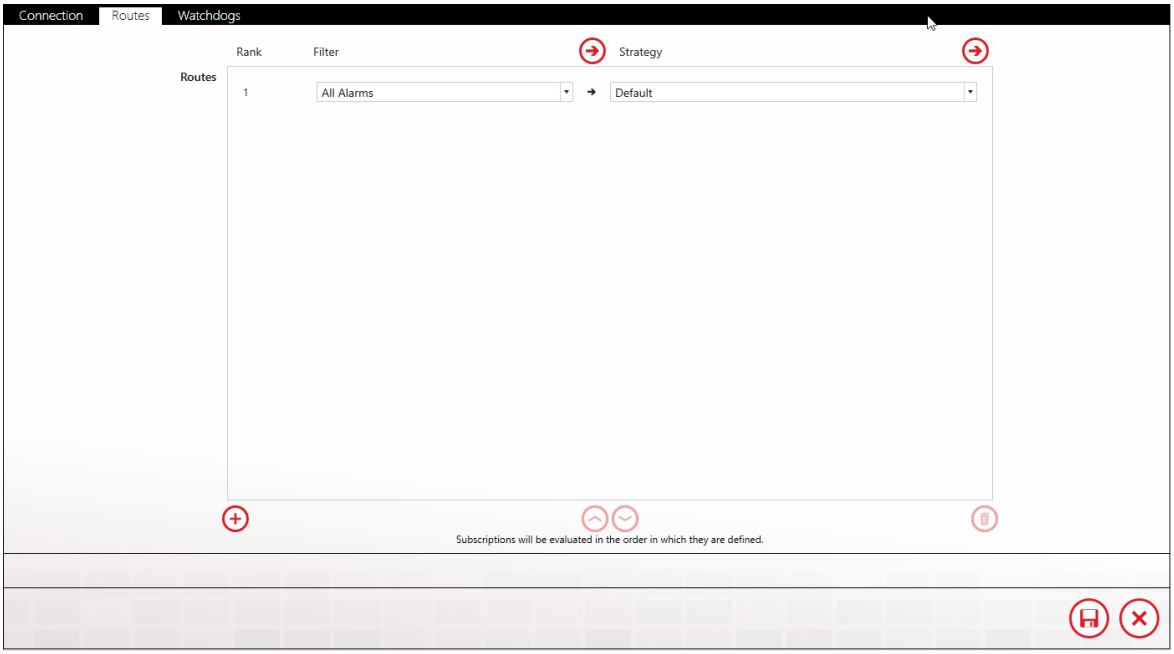
Language

Specify the language WIN-911 is to use when monitoring and dispatching alarms. Use the browse button to the right to select a different language.

Good Quality Events Only

Select this option to ignore bad or uncertain quality alarms.

Routes



Routes forward alarms from a Subscription to a particular Strategy. This feature allows you to use Subscriptions across multiple Applications without redefining Subscription logic. A single alarm will match only one Subscription. Routes are evaluated in the order they are ranked.
See Subscriptions for a detailed explanation of their usage.

Click the 'Navigate' buttons to configure Subscriptions or Strategies.

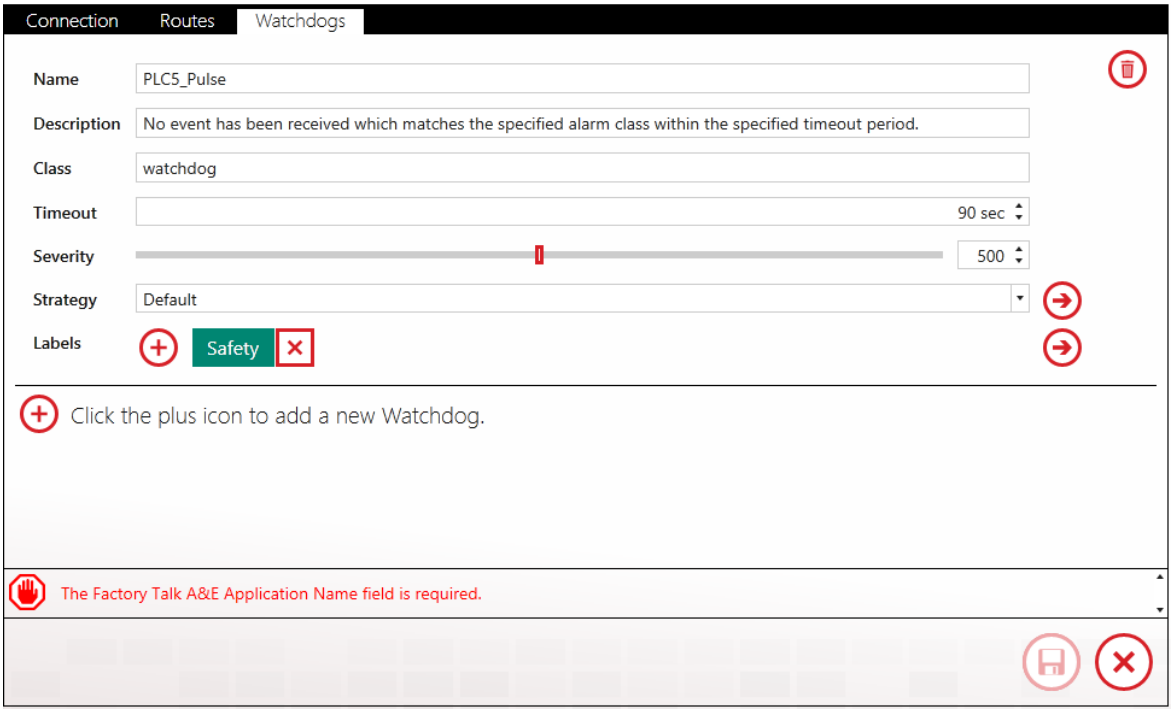
Click the 'Add' button to add a new Route to the Application.

Click the 'Up' button to move the selected Route up a rank.

Click the 'Down' button the move the selected Route down a rank

Click the 'Delete' button to remove the selected Route from the Application.

Watchdog



FactoryTalk A&E supports watchdog timers which may be used to alert users when communications are lost between WIN-911 and FactoryTalk A&E. WIN-911 must monitor a changing alarm condition as opposed to a changing data value. The watchdog timer would then be set to a value greater than the interval of the reoccurring alarm condition.

To use a Watchdog, create a recurring alarm in FactoryTalk A&E with a Class name of "watchdog" (case sensitive).

Name

Enter a name for this watchdog.

Description

An optional text field for providing the user with context. Such information can contain location data (like Lift Station 22), or an explanation of the connection that conveys useful information to the user that is not provided elsewhere.

Class

Defaults to watchdog.

Timeout

Enter time (in seconds) from "5" to "900".

Severity

Select severity level the alarm will be assigned ("0" through "1000").

Strategy

Select defined Strategy (See "Notification" for information on setting up Strategies").

Labels

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements.

Cimplicity Projects

Note: WIN-911 supports Cimplicity versions 8.2 and 9. The installation sets WIN-911, by default, to connect to version 9. If you are integrating WIN-911 with Cimplicity version 8.2 you must make the following modification to properly connect. Change the WIN-911.Source.Cimplicity.Runtime.Adapter from the version 9 to 8.2.

1. *Open your Services via task manager or Control Panel>Administrative Tools and stop the WIN-911 Cimplicity Runtime by right-clicking on it and selection Stop*
2. *Open Explorer and navigate to c:>Program Files (x86)>WIN-911 Enterprise>CIMPLICITY>Adapter82.*
3. *Right-click on the adapter and select Copy.*
4. *Back out of the current folder to the CIMPLICITY folder and Paste the WIN-911.Source.Cimplicity.Runtime.Adapter, allowing it to overwrite the existing file. (If you upgrade CIMPLICITY you still have the original adapter in the Adapter9x folder, with which you can reverse the process.)*
5. *Start the WIN-911 Cimplicity Runtime by right-clicking on it in Services and selecting Start.*

Project

Project Name

Enter the name of the Cimplicity project you wish to monitor. The name is case sensitive and must match the project name as it appears in Cimplicity.

Username/Password

Cimplicity users can be assigned a password to enhance operational security. If a password is configured for the WIN-911 username enter it here, otherwise leave this field empty.

Health Alarm

The health alarm monitors WIN-911's connection with the project. If the project connection is lost WIN-911 will trigger an alarm that can be dispatched an alarm notifier

Description

Enter the text of the alarm message you wish to be dispatched on the event of a data source connection loss.

Strategy

Select the strategy you wish WIN-911 to use when dispatching the health alarm notification.

Severity

A numeric attribute from 1 to 1000 that designates that urgency of an alarm event. It can be used as an organizational tool and be used in a tactic to determine how an alarm is dispatched and which alarm has priority over another. The default severity is 500.

Labels (for use by Advanced Tactics)

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements. (See Labels)

Filters

WIN-911 provides the Cimplicity user with two methods of alarm monitoring: Filters, and Points. Filters allow WIN-911 to subscribe to a range of possible alarm events based on criteria the user defines Here.

The advantage of using alarm points over filters is that individual points are subject to having its alarm criteria modified which may cause a previously defined alarm filter to reject the new alarm. In situations where a point and a filter both match an alarm event, the point setting will take priority over the filter and dispatch the alarm.

Filters specify which Cimplicity alarm events will be handled by WIN-911 and which strategy will be utilized when handling them (See "Tactics" and "Strategies" in the Notification section). The user is able to create subscriptions for All Alarms, or subscribe based on Point ID, Class Names, or Class Orders.

If more than one subscription is set up for an alarm event, the event will be handled based on the first matching filter defined. If all properties of the filter are not satisfied by an alarm event, WIN-911 will move on to the next filter until a matching filter is found. The filter workspace also allows the user to attach Labels to the alarms.

All Alarms

If All Alarms is selected (default), all Cimplicity alarm event messages for this filter will match the subscription and will be sent to WIN-911 for remote notification as per the selected strategy.

Point ID

Each point in a Cimplicity project has a unique Point ID.

Your filter can be set to allow all Point IDs or you can restrict certain events base on criteria you specify here. When defining specific Point ID criteria you have the option to use a "Wildcard" to include certain events based on your input, or a "RegEx" to exclude certain names. For example, "T*" would match all alarm events with an alarm name that starts with "T" while "*pump*" would match all events containing the string "pump" in their name. Any alarm event that does not meet this criterion will cause the event to be rejected by the filter.

Class Names

Alarm Classes are a group of alarms with similar characteristic. Class names (Class ID) can be up to 5 characters in length, must be unique, and cannot include the $ or | characters.

Your filter can be set to allow all class names or you can restrict certain events base on criteria you specify here. When defining specific Class Name criteria, you have the option to use a "Wildcard" to include certain events based on your input, or a "RegEx" to exclude certain names. For example, a wildcard with criteria of "T*" would match all alarm events with a class name that starts with "T" while "*pump*" would match all events containing the string "pump" in their name.

Any alarm event that does not meet this criterion will cause the event to be rejected by the filter.

Resource IDs

Your filter can be set to allow all Resource IDs or you can restrict certain events base on criteria you specify here.

Class Orders

An alarm Class Order is a numeric priority that ranges from 0 to 9999, where 0 is the highest priority and 9999 is the lowest.

You can select an order range (e.g. 200-400) or a specific order value (e.g. 800). Any alarm event that does not meet this criterion will cause the event to be rejected by the filter.

Combinations

The filters are evaluated based on the sum total of all criteria specified. For example, a filter with a specified class order of "700-900" and a Point ID of "T" would match all alarm events with a class order range of "700-900" and a Point ID that starts with "T". Since the Class Name was not specified no alarm event would be rejected based on Class Name.

Strategy

Select defined Strategy to dispatch alarms for this filter.

Labels

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project's alarming requirements. (See Labels)

Watchdogs

Cimplicity supports watchdog timers which may be used to alert users when communications are lost between WIN-911 and Cimplicity. WIN-911 must monitor an alarm condition that cycles in and out of alarm on a specified time interval. The watchdog timer would then be set to a value greater than the interval. If the timer expires prior to the change of alarm state, WIN-911 with trigger the watchdog.

Name

Enter a name for this watchdog.

Description

An extra text field for context concerning the Watchdog Alarm.

Point ID

Each Point ID can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see Cimplicity documentation for these).

Timeout

Specify the timeout interval that WIN-911 will wait for an alarm condition change to occur before triggering the Watchdog. Enter time (in seconds) from "5" to "900".

Severity

Select severity level the alarm will be assigned ("0" through "1000").

Strategy

Select defined Strategy (See "Notification" for information on setting up Strategies").

Cimplicity Points

WIN-911 provides the Cimplicity user with two methods of alarm monitoring: 1) Filters, and 2) Points. Filters allow WIN-911 to subscribe to a range of possible alarm events based on criteria the user defines in the Cimplicity Filters Workspace (see Cimplicity Projects>Filters). The advantage of using alarm points is that individual points are subject to having its criteria modified which may cause a previously defined WIN-911 filter to reject the new alarm event. In the case where a filter is set that matches the Points configuration, the Points configuration takes priority over the Filter and will process the alarm rather than producing two alarm events, one for the filter and on for point.

Point

Name

The "Name" field is a unique WIN-911 property that can be associated with the Cimplicity point Its purpose is to make the point name easier to read if the Cimplicity Point ID is cryptic.. This name must be unique and is independent of Cimplicity's Point ID.

Description

An optional text field for providing the user with context. Such information can contain location data (like Lift Station 22), or an explanation of the event that conveys useful information to the user that is not provided elsewhere.

Project

Select the Cimplicity project that contains this point.

Point ID

Each Point ID can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see Cimplicity documentation for these).

Strategy

Select the strategy you wish WIN-911 to use when dispatching the health alarm notification.

Labels (for use by Advanced Tactics)

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements.

Conditions

You may optionally define conditions in order to provide condition specific labels and description.

Condition

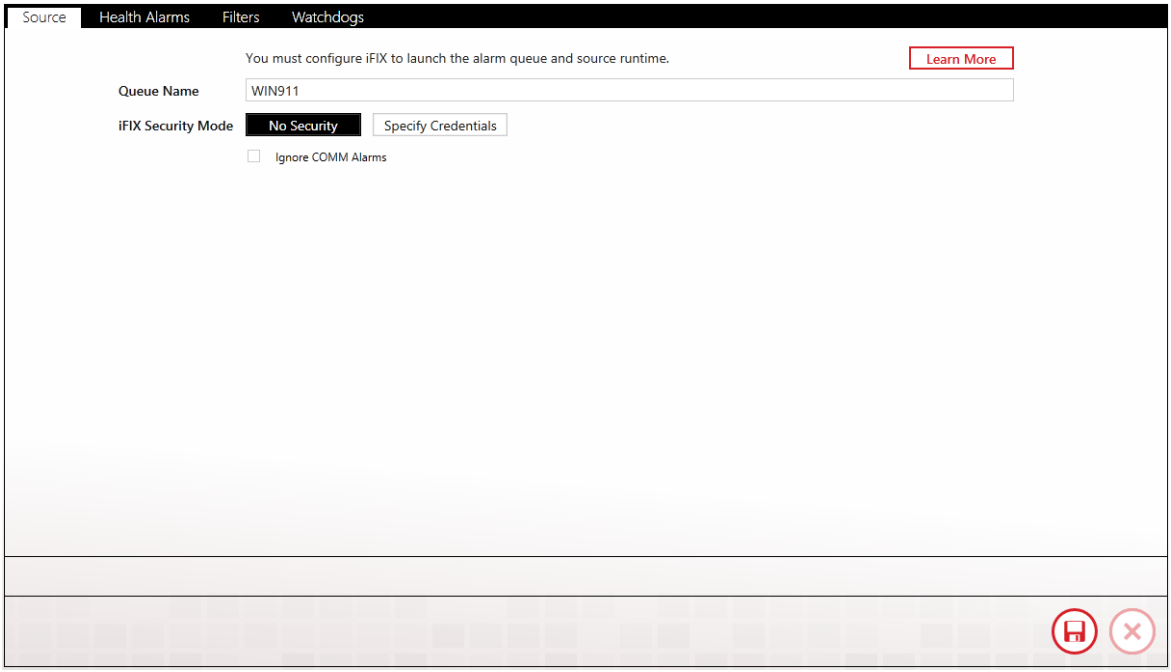
The value or state of the Cimplicity point that constitutes and alarm event. The state can be selected from the following options: Lo, LoLo, Normal, Hi, and HiHi.

Description

Enter the text of the alarm message you wish to be dispatched on the event of a data source connection loss.

iFIX Sources

Source



You must configure iFIX to launch the alarm queue and source at runtime.

Queue Name

To integrate WIN-911 with iFIX you must configure the iFIX System Configuration Utility (SCU) to start two executables as part of as part of the iFIX startup sequence: the alarm queue and the WIN-911 iFIX runtime source. The queue must be started before the runtime source. The two applications must be launched before WIN-911 may import blocks from iFIX and are also required for remote alarm notification. Follow the instructions below to make sure that iFIX launches both of these applications at start up, and in the proper order.

1. *Open the iFIX SCU.*
2. *Open the Configure > Tasks...*
3. *Click the browse button to the right of the Filename text box.*
4. *Browse to the WIN-911 iFIX runtime source path. By default, the path is : "C:\Program Files (x86)\WIN-911 Software\WIN-911 Enterprise\iFIX." and select "AlmUserQ.exe."*
5. *In the command line text box enter"/nWIN911 /s6000" without quotations. (Take note that there is no space between "/n" and "WIN911" or between "/s" and "6000.")*
6. *Set the start up mode to "background."*
7. *Click the add button.*
8. *Once again, click the Filename browse button and navigate to the WIN-911 iFIX runtime source path.*
9. *Select "WIN911_Source_iFIX_Runtime_WPFHost.exe."*
10. *Leave the Command Line field blank (see note below) and set the start up mode to "background."*
11. *Click the "add" button.*
12. *Click the "OK" button at the bottom of Task Configuration page.*
13. *Save the changes you've made in the SCU with the File > Save menu option.*

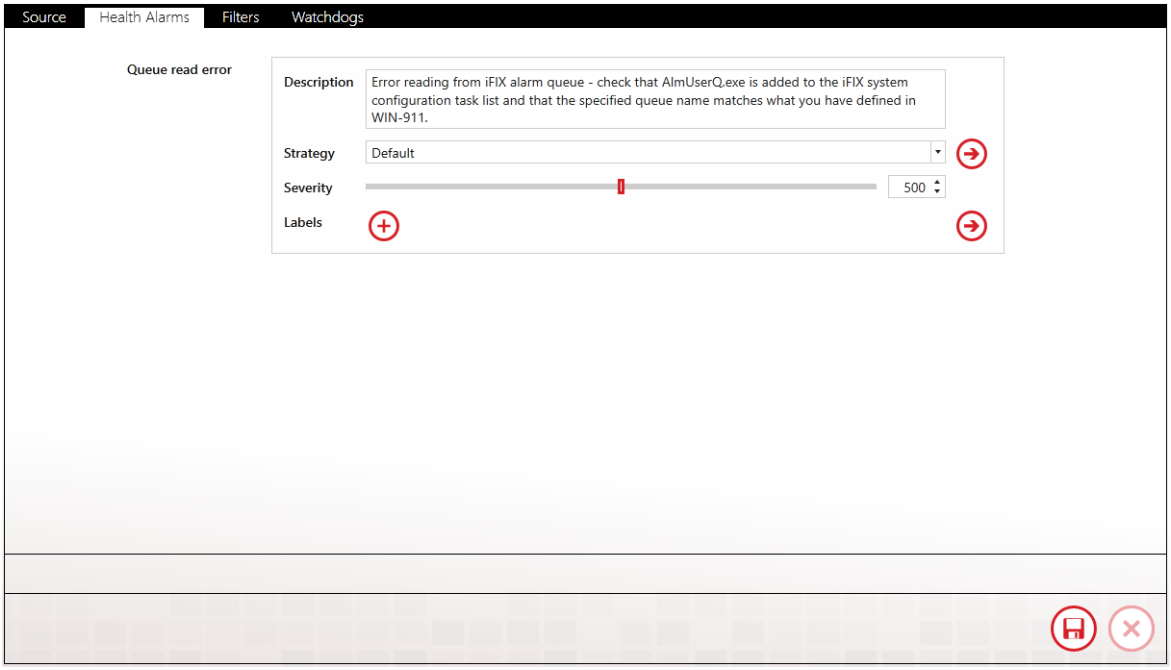
iFIX Security Mode

iFIX can be configured to require security credentials for access to their SCADA. When iFIX is configured for security WIN-911 will require valid credentials in the form of a username and password. See your network administrator for obtaining credentials for your WIN-911 system.

Test Credentials

The iFIX Runtime credentials can be verified by clicking Test Credentials button. If the test fails try reentering the credentials or contact your network administrator.

Health Alarms



Queue Read Error

Description

The text of the health alarm can be modified by the WIN-911 Administrator by editing the contents of the description text entry box.

Strategy

The strategy selector pull-down list assigns the strategy that WIN-911 will use to dispatch health alarm messages.

Severity

You can select a specific severity value (e.g. 800) to associate with Health Alarms.

Alarm Priority to Severity Map
Critical: 1000
HiHi: 900
High: 700
Medium: 500
Low: 300
LoLo: 100
Info: 0

Labels (for use by Advanced Tactics)

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements.

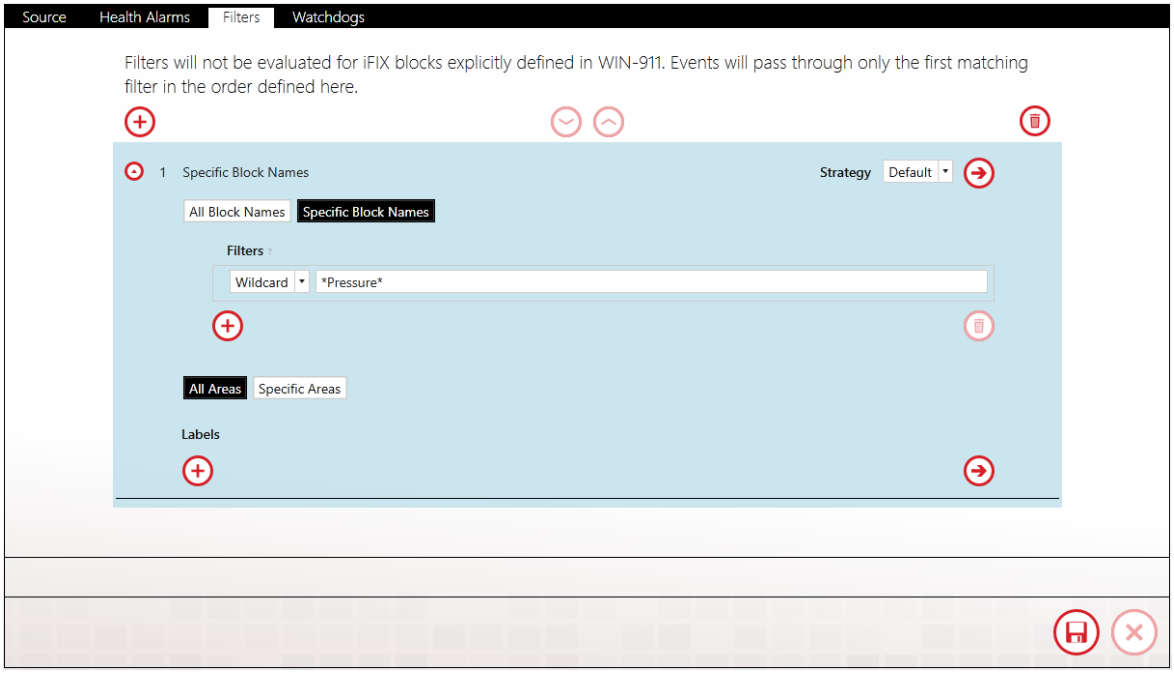
Filters

WIN-911 provides the iFIX user with two methods of alarm monitoring: 1) Filters, and 2) Blocks. Filters allow WIN-911 to subscribe to a range of possible alarm events based on criteria the user defines here. This section focuses on the development of alarm filters.

The advantage of using alarm blocks (rather than filters) is that WIN-911 will synchronize alarm states upon startup; however, this initialization can be very time consuming. In general, filters are preferred. Filters consume fewer resources and are easier to maintain. In the case where a filter is set that matches an alarm block configuration, the block configuration takes priority over the filter and will process the alarm rather than dispatching two alarm events, one for the filter and on for the block.

Filters specify which iFIX alarm events will be handled by WIN-911 and which strategy will be utilized when handling them (See "Tactics" and "Strategies" in the Notification section). The user is able to create subscriptions for All Alarms (default), or selections based on Block Names, or Specific Areas.

If more than one filter is set up for an alarm event, the event will be handled based on the first matching filter defined. If all properties of the filter are not satisfied by an alarm event, WIN-911 will move on to the next filter until a matching filter is found. The filter workspace also allows the user to attach Labels to the alarms matching the filter.



All Block Names

If All Block Names is selected (default), all iFIX alarm event messages for this filter will match the subscription and will be sent to WIN-911 for remote notification as per the selected strategy.

Specific Block Names

Each block in an iFIX project has a unique block name that identifies it. It can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see iFIX documentation for these).

Your filter can be set to allow all block names or you can restrict certain events base on criteria you specify here. When defining specific block name criteria, you have the option to use a "Wildcard" to include certain events based on your input, or a "RegEx" (regular expression) to exclude certain names. In a wildcard search, "T*" would match all alarm events with an alarm name that starts with "T" while

"*pump*" would match all events containing the string "pump" in their name. Any alarm event that does not meet this criterion will cause the event to be rejected by the filter. If more than one filter criterion is specified, the alarm is considered to match the filter if any criterion is matched.

All Areas

If All Areas is selected (default), all iFIX alarm event messages for this filter will match the subscription and will be sent to WIN-911 for remote notification as per the selected strategy.

Specific Areas

Each Area in an iFIX project has a unique area name that identifies it. Each area name can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see iFIX documentation for these).

Labels

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project's alarming requirements.

Combinations

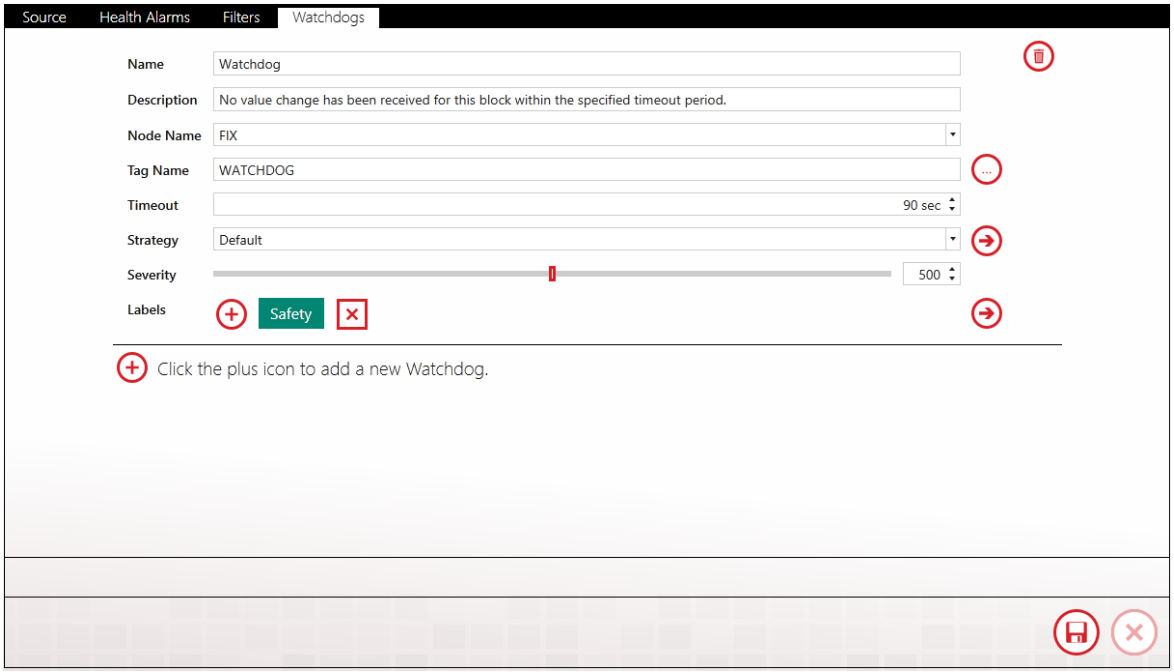
The filters are evaluated based on all criteria specified. For example, a filter with a specified block name WASTEWATER and an alarm area that contains the letter "T" would match only alarm events with a block name of WASTEWATER and an alarm area that contains the letter "T".

Strategy

Select defined Strategy (See "Notification" for information on setting up Strategies").

Watchdog

WIN-911 provides watchdog timers which may be used to alert users when communications are lost between WIN-911 and an iFIX tag. WIN-911 will monitor the specified tag, expecting an alarm event or value change message to appear in the queue within a specified period of time. When the value or alarm state fails to change within the specified period of time the Watchdog alarm will become active.



Name

Enter a name for this watchdog.

Description

An extra text field communicated with the alarm event notification.

Node Name

The node of the block to be monitored. Each can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see iFIX documentation for these).

Tag Name

The tagname of the block to be monitored. Each can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see iFIX documentation for these).

Timeout

Enter time (in seconds) from "5" to "900".

Strategy

Select defined Strategy (See "Notification" for information on setting up Strategies").

Severity

Select severity level the alarm will be assigned ("0" through "1000").

WIN911

Alarm Priority to Severity Map

Critical: 1000
HiHi: 900
High: 700
Medium: 500
Low: 300
LoLo: 100
Info: 0

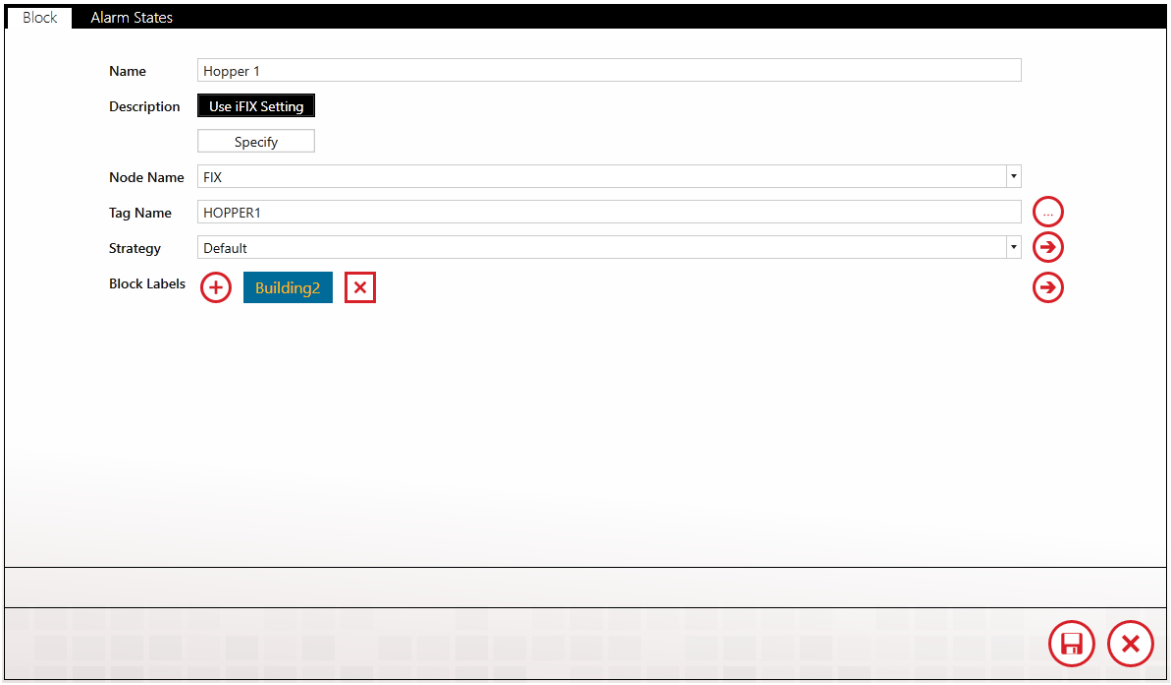
Labels

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project's alarming requirements.

iFIX Blocks

WIN-911 provides the iFIX user with two methods of alarm monitoring: 1) Filters, and 2) Blocks. Filters are the preferred option as they allow WIN-911 to subscribe to a range of possible alarm events based on criteria the user defines in the iFIX Filters Workspace (see iFIX>Source>Filters). This section focus on the development of individual iFIX Blocks.

Block



Name

The "Name" field is a unique WIN-911 property that can be associated with the iFIX Blocks. Its purpose is to make the block name easier to consume if the iFIX block name is cryptic. This name must be unique

but is independent of iFIX Tag Name and only used when dispatching alarm notifications.

Description

Enter the text of the alarm message you wish to be dispatched with alarm events for this block. The user can opt to use the iFIX description or can specify a custom description for use by WIN-911.

Node Name

Select the iFIX node that contains this block. The name is case sensitive and must match the node name as it appears in iFIX.

Tag Name

Each block in an iFIX configuration has a unique tag name that identifies it. Each can have up to 32 characters, any combination of upper-case letters and numbers, and special characters, with some restriction (see iFIX documentation for these).

Strategy

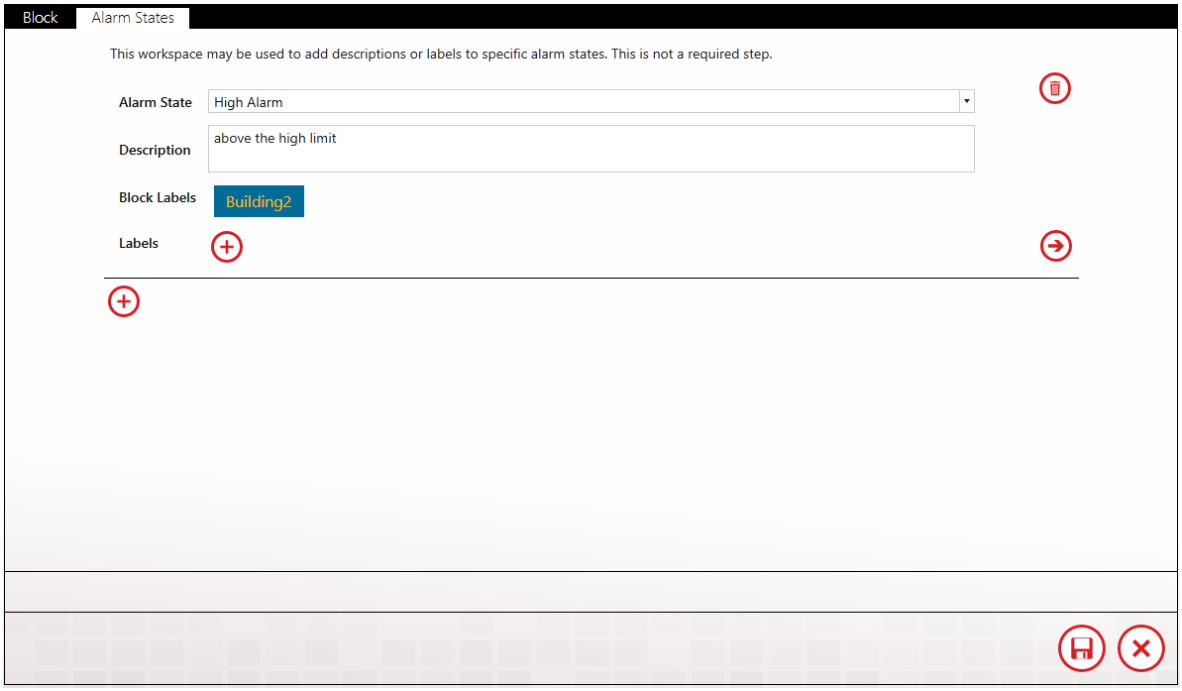
Select the strategy you wish WIN-911 to use when dispatching alarm events for this block. (See Strategies)

Block Labels (for use by Advanced Tactics)

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements. (See Labels)

Alarm States

You may optionally define alarm states in order to provide alarm state specific labels and descriptions.



Alarm State

The state on which to provide customer labels and/or descriptions. The state can be selected from the following options: Lo, LoLo, Normal, Hi, and HiHi.

Description

Enter the text of the alarm message you wish for alarm events with this state.

Block Labels (for use by Advanced Tactics)

Labels are optional attributes for organizing alarms in a logical manner. They can represent function, location, severity, or other such category that serves the project requirements. (See Labels)

iFIX Imports

Logical Node and Attribute Selection

Import blocks from an iFIX database on your network.

The iFIX client on the WIN-911 host and all applicable iFIX SCADA servers must be running in order to conduct a block import.

You must define a strategy other than the default strategy before importing iFIX blocks. This is required in order to ensure a large number of blocks are not accidentally imported and immediately dispatched to everyone in the WIN-911 contact library. You may still conduct the import and assign all blocks to the Default strategy. This requirement is merely a safeguard to force verification of your intent.

All Logical Nodes

This selection will allow the selection of blocks from all logical nodes on your iFIX network.

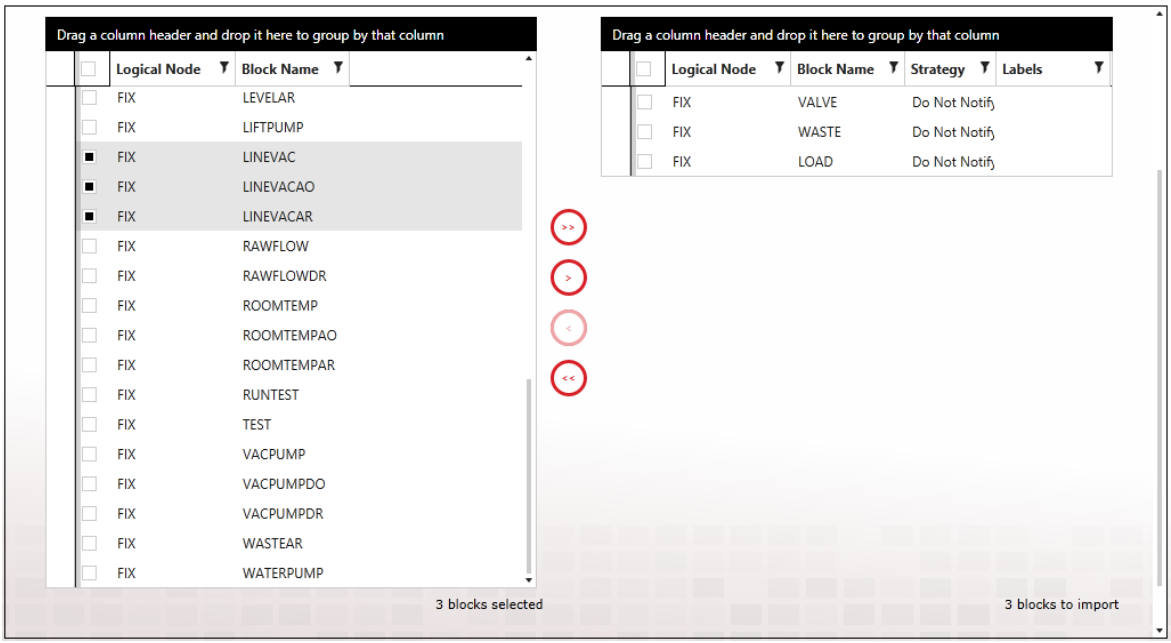
Specific Logical Nodes

This selection filters the available block list to blocks residing on specified logical nodes. The nodes may then be selected from the available nodes list on the right.

Additional information can be gathered to help organize and refine the import process. This can include block types (AA, AD, DI, etc.). alarm descriptions, and whether or not alarming has been enabled. Please note that these options will slow down the loading process.

Once your nodes and additional information are selected, click next to proceed to block selection page by clicking the Next button on the bottom right. You can always return to this page by clicking the previous button on the bottom left.

Block Selection



The block selection page provides the WIN-911 Administrator with a powerful tool to quickly and accurately import mass data, apply labels and assign strategies with as few steps as possible.

Start by selecting the strategy you want to assign to all of the blocks collected in this section. You can repeat any portion of the import to gather different blocks to assign to other strategies. Once a block has been imported it will no longer show up in the available blocks list. Thus, everything shown in the available blocks list is NOT currently a part of your WIN-911 configuration. Once a block (or list of multiple blocks are selected they are moved to the selected blocks list on the right by click the red arrows on the column between the two lists.

Once your selection is complete you can execute the import by clicking the finish button on the bottom right. Until that button is clicked no blocks are imported.

Import Results

After the import is complete WIN-911 presents a report detailing the result of the process. From this page, the use can continue with further block imports by clicking the Import More button provided on the bottom right, or navigate to the iFIX Blocks tab by clicking the red arrow under the results report.

InTouch Subscriptions

The InTouch Source uses Subscriptions to access alarms from InTouch. Subscriptions can be created to match against InTouch tagnames, groups, and/or priorities. Subscriptions may be used across multiple Applications to fetch existing alarms within. By default, a Subscription named 'All Alarms' is included.

Navigate to the Subscription workspace under Alarming > InTouch > Subscriptions to get started.

Subscription

By default, Subscriptions will match all alarms when first created. Users can click the radio buttons to modify the filtering criteria. In the example below, specific Tagnames and Priorities are being targeted.

String Filters

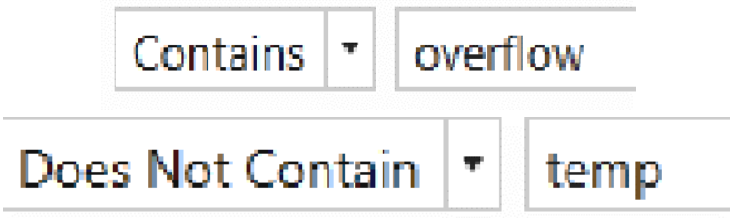
Four types of string filters exist. They can be used to match against InTouch Tagnames and the Groups that your InTouch Tags are assigned to in InTouch. String filters are case-sensitive.

The first and, easiest to use is the wildcard filter. Enter any string literal to match it exactly. Enter an asterisk to match any character any number of times. Enter a question mark to match any character one time.

- Tank" will only match the string "Tank"
- "*tank" will match any string that ends with "tank." E.g. "Watertank," "Brite tank."
- "z?g" will match any string that begins with "z," ends with "g," and has one and only one letter between them. E.g. "zig," "zag."

Regular expressions can be used. Regular expressions are an advanced method of

pattern matching. There are many resources available online that document their use.



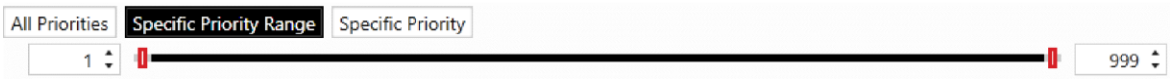
'Contains' will match any string that contains the substring you enter exactly. 'Does Not Contain' will match the opposite.


Click the 'Add' button to create a new string filter under the respective category (e.g. tagname) with default values. Multiple filters in a category will be logically AND'ed.


Click the 'Delete' button to delete the selected string filter under the respective category.

Priority Filters

Priority filters are supported for InTouch. They can be created to match an inclusive range.



They can also be created to match a specific Priority.

Labels

Click the 'Add' button to the right of 'Labels' to add new Labels to this Subscription. At runtime, alarms matching the Subscription will have the specified set of Labels attached.

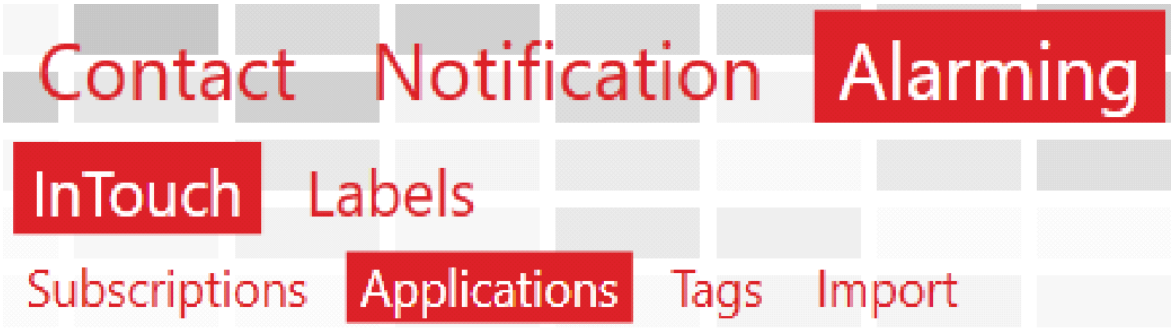
Click the 'Navigate' button to navigate to the Labels workspace. If any changes have been made to the Subscriptions tab, they will persist until the user navigates back to the Subscriptions tab.

Click the 'Delete Label' button to delete the Label on the left.

Utilizers

This tab simply shows the user which Applications are currently using the Subscription that they are viewing. A Subscription cannot be deleted while in use.

InTouch Applications



Application

WIN-911 is capable of connecting to multiple local or remote InTouch Applications. Specify the connection criteria in the Applications tab.

Name

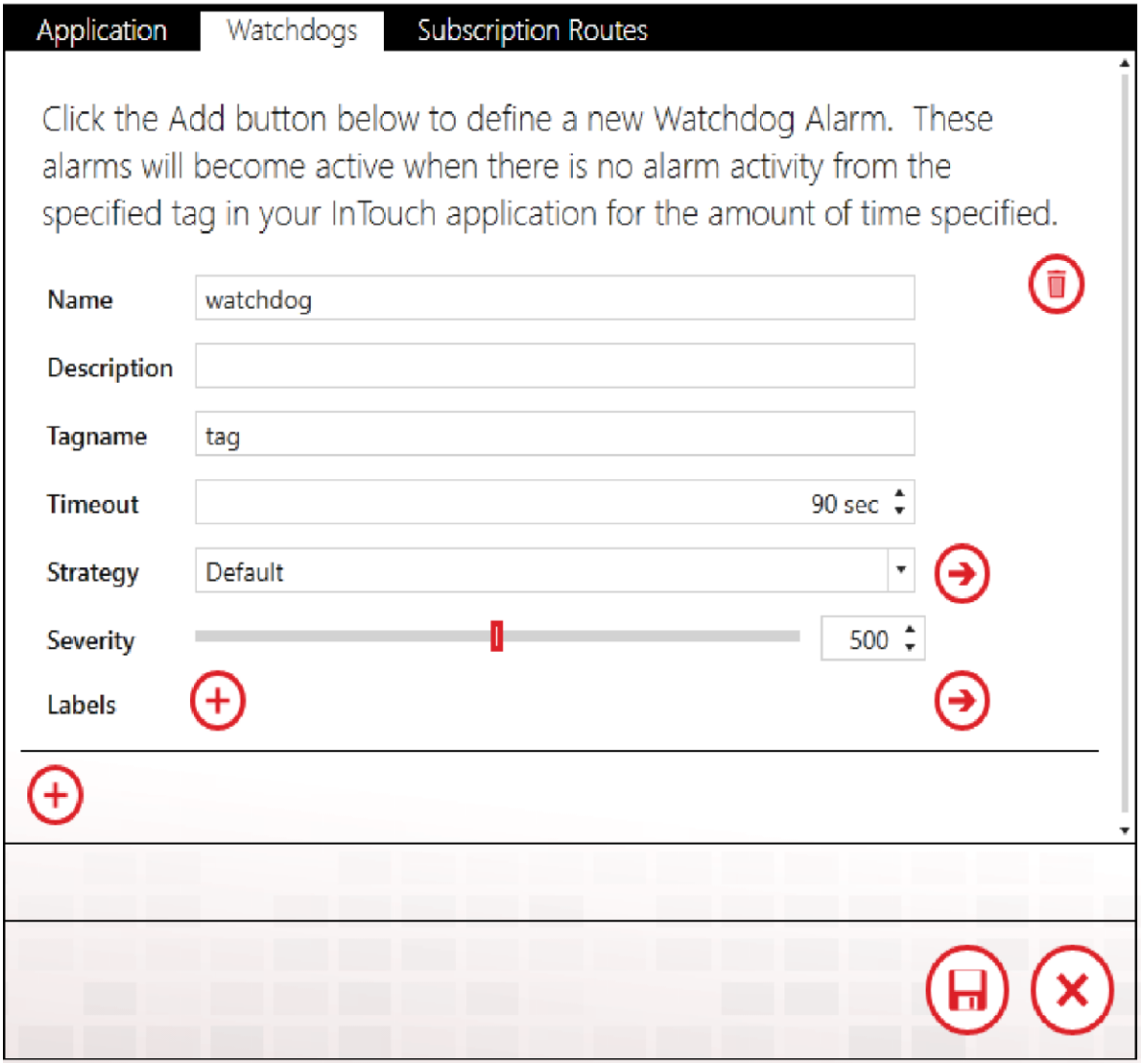
Enter a unique name for your Application.

Node Name

WIN-911 will connect to the single running Application on this specified Node. If your Application is running on the local machine, use “localhost.” Otherwise, enter its host name or IP address. The IP address should be static; if using a dynamic address, the user will have to update the address each time the IP changes.

You may browse for machines by clicking the Browse button.

Watchdogs



WIN-911's InTouch Source supports Watchdog alarms. They monitor a changing value (or changing alarm state) within your Application. If an update is not received within the specified Timeout period, the watchdog will become an active alarm. Watchdogs can thus be used to monitor the operation and connectivity of critical devices.

Watchdogs have a configurable Severity from 0 – 1000 inclusively and may also have Labels attached. Watchdogs are associated with a Strategy for alarm escalation.

Click the 'Add' button at the bottom of the Watchdog collection to add a new Watchdog configuration to the Application.

Each Watchdog will have the following configuration:

* indicates required fields.

***Name:** the friendly name for this Watchdog configuration. Provide a user-friendly name here, as this is the name that will be most prominently displayed in alarm notifications.

Description: a description for this configuration.

***Tagname:** InTouch Tag that WIN-911 will monitor for a changing value (or changing alarm state). This field must match the name of the tag as it is configured in InTouch.

***Timeout:** the elapsed time (seconds) when WIN-911 will periodically check the tag for a changed value.

***Strategy:** the strategy to execute when the Watchdog alarm activates.

Click the 'Navigate' button to the right of the 'Strategy' combo box to go to the Strategies workspace in order to configure Strategies.

***Severity:** the severity associated with this Watchdog alarm.
Labels: the list of Labels associated with this Watchdog.

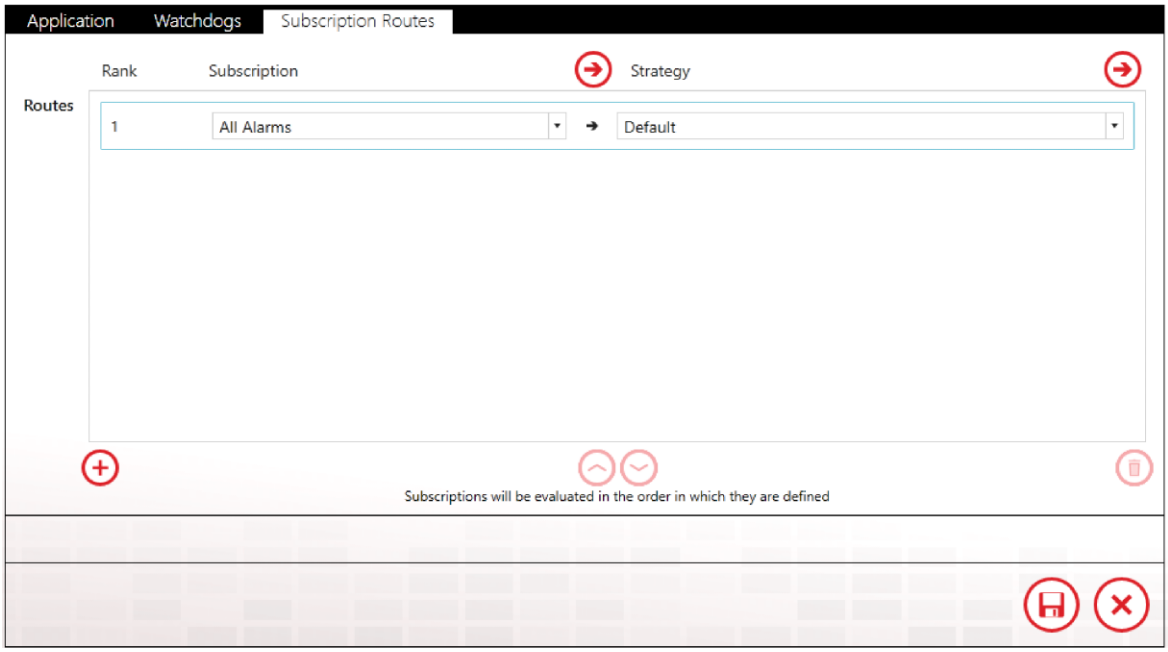

Click the 'Add' button to the right of 'Labels' to attach Labels to the Watchdog.


Click the 'Navigate' button to the right of the Label collection to configure Labels in the Labels workspace.


Click the 'delete' button at the top-right corner to remove the Watchdog from the Application.


Click the 'X' button to the right of an attached Label to remove it from the Watchdog.

Subscription Routes



Subscription Routes forward alarms from a Subscription to a particular Strategy. This feature allows you to use Subscriptions across multiple Applications without redefining Subscription logic. A single alarm will

match only one Subscription. Routes are evaluated in the order they are ranked.
Subscriptions are the preferred method of configuration for fetching alarms from InTouch Applications. See the Subscriptions for a detailed explanation of their usage.


Click the 'Navigate' buttons to configure Subscriptions or Strategies.


Click the 'Add' button to add a new Route to the Application.


Click the 'Up' button to move the selected Route up a rank.


Click the 'Down' button the move the selected Route down a rank

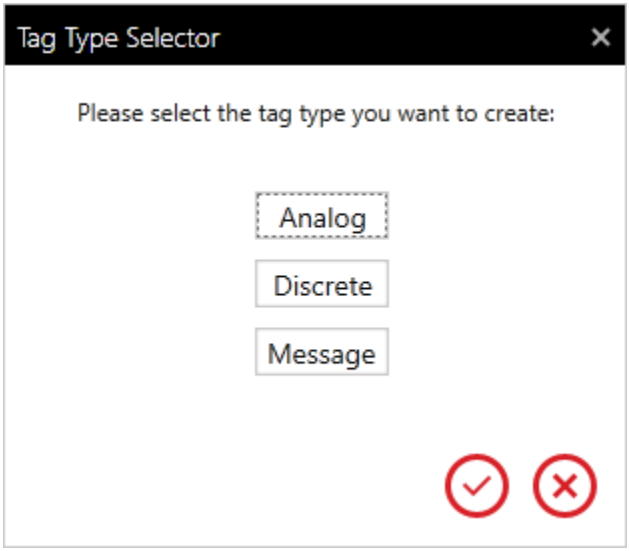

Click the 'Delete' button to remove the selected Route from the Application.

InTouch Tags

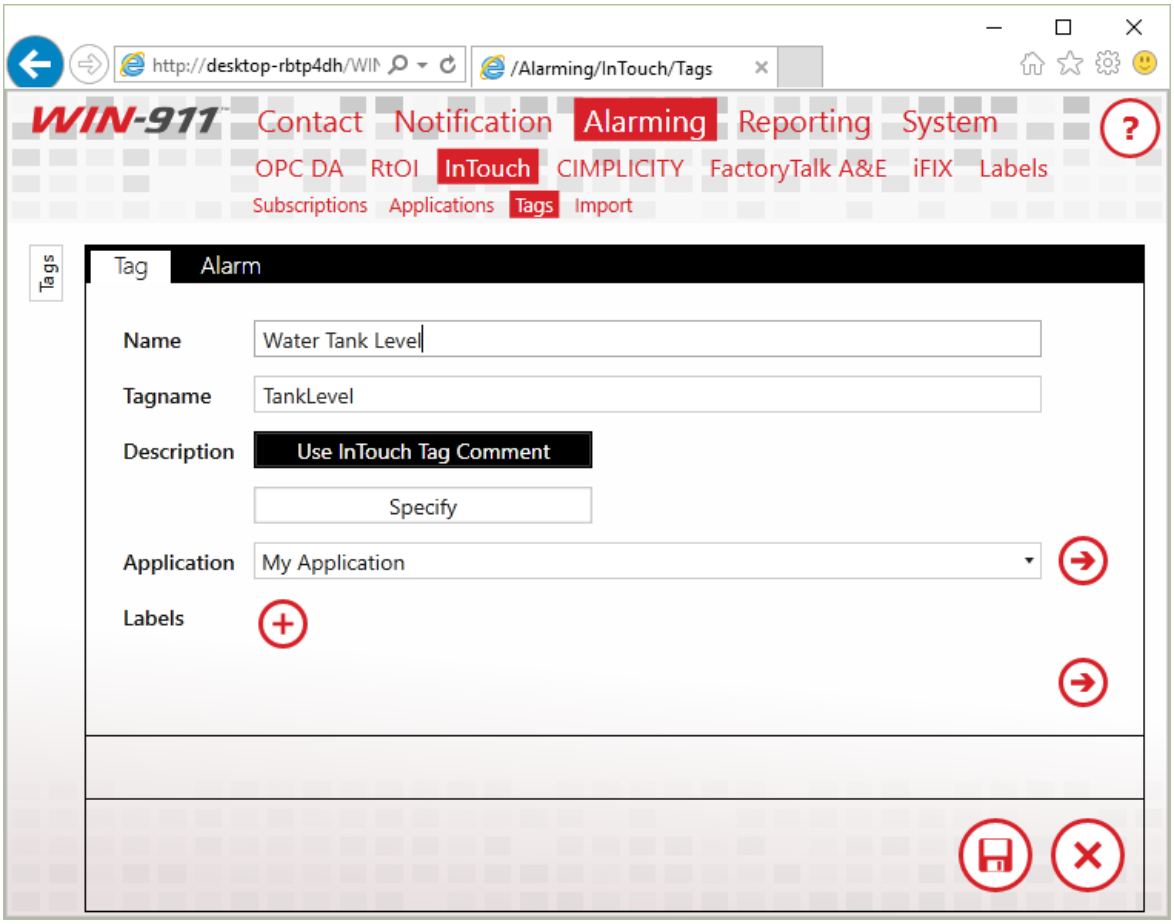
WIN-911 supports Subscriptions for InTouch alarms, which provide an easy to configure means of subscribing to alarms. As they require less maintenance, we recommend you use Subscriptions over tag definitions. You must, however, use Tag definitions to support reporting.

WIN-911 can connect to all types of InTouch Tags. Alarms are supported for both Discrete and Analog Tags. Message Tag support is included for reporting purposes.

Tags may be imported from an InTouch DBDump. They may also be created manually. When manually creating a Tag in WIN-911, you must first specify the Tag type. Once the Tag type has been set, it cannot be changed. If you wish to change the Tag type, simply delete the Tag and recreate it as the desired type.



General



Name

The Name field serves as a unique identifier for InTouch Tags. This field is user defined and may be independent of the InTouch Tagname. Provide a user-friendly name here, as this is the name that will be most prominently displayed in alarm notifications.

Tagname

The Tagname field must match the tagname of the Tag as it appears within InTouch. Tagnames must be unique within an Application. Comparison is case-sensitive.

Application

Select the Application which hosts the Tag you've created.

Labels

Attach Labels to your Tag as a means of organization. See the Labels for more information regarding Labels.

Alarm

WIN-911 supports four types of alarms for tags: level, rate of change, deviation and discrete. Level, rate of change, and deviation alarms belong to analog Tags, and discrete alarms belong to discrete Tags.

For the sake of brevity, only the discrete alarm condition will be discussed. For analog tags: level alarms have four conditions: HiHi, Hi, Lo, and LoLo; deviation alarms have two: Major Deviation and Minor Deviation; rate of change alarms have only one condition, just like discrete alarms. Each alarm condition has the following configuration:

Strategy

Select the Strategy that will dispatch this alarm.

Click the 'Navigate' button on the right to configure Strategies in the Strategies workspace.

'Alarm' Enabled

Enable the alarm by checking this box. Any alarm may be independently disabled. For instance, it is possible to define an analog tag with a rate of change alarm, while the level alarm is disabled.

Description

You may provide an alarm description to add additional context to your alarms. If you leave the description field blank, your alarm description will match your InTouch alarm comment.

Labels may be attached to any alarm condition. See the Labels for more information regarding labels.

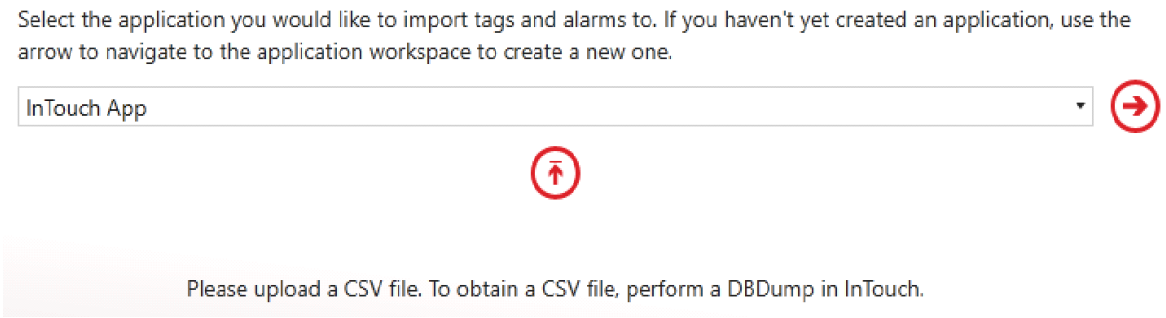
Click the 'Add' button to attach Labels to the associated condition.

Click the 'X' button to delete the Label to the left.

Click the 'Navigate' button on the right to configure Labels in the Labels workspace.

InTouch Import

Select Application



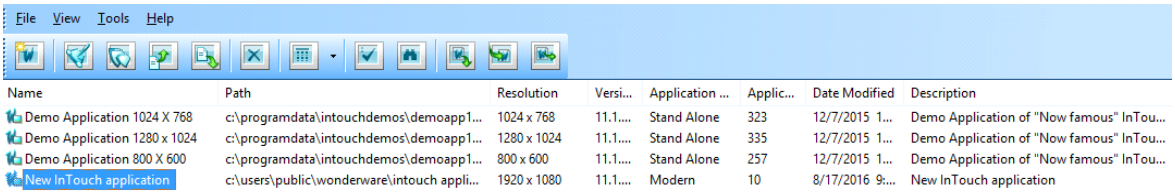
Before proceeding, you must have an InTouch Application defined.

Click the Navigation button to go to the Applications workspace and configure an InTouch Application to WIN-911.

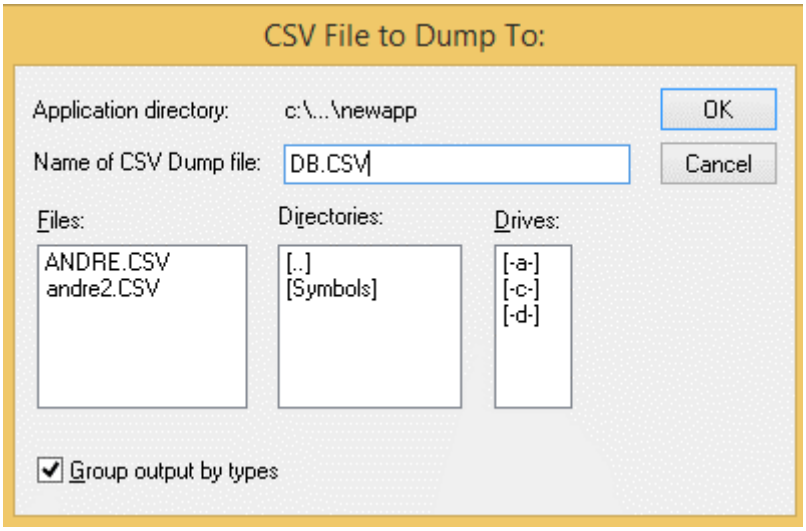
You will also need to upload a CSV file that contains Tag definitions.

DBDump

To perform a DBDump in InTouch, start the InTouch Application Manager (by default located at '**C:\Program Files (x86)\Wonderware\InTouch**') and select one of your defined Applications.

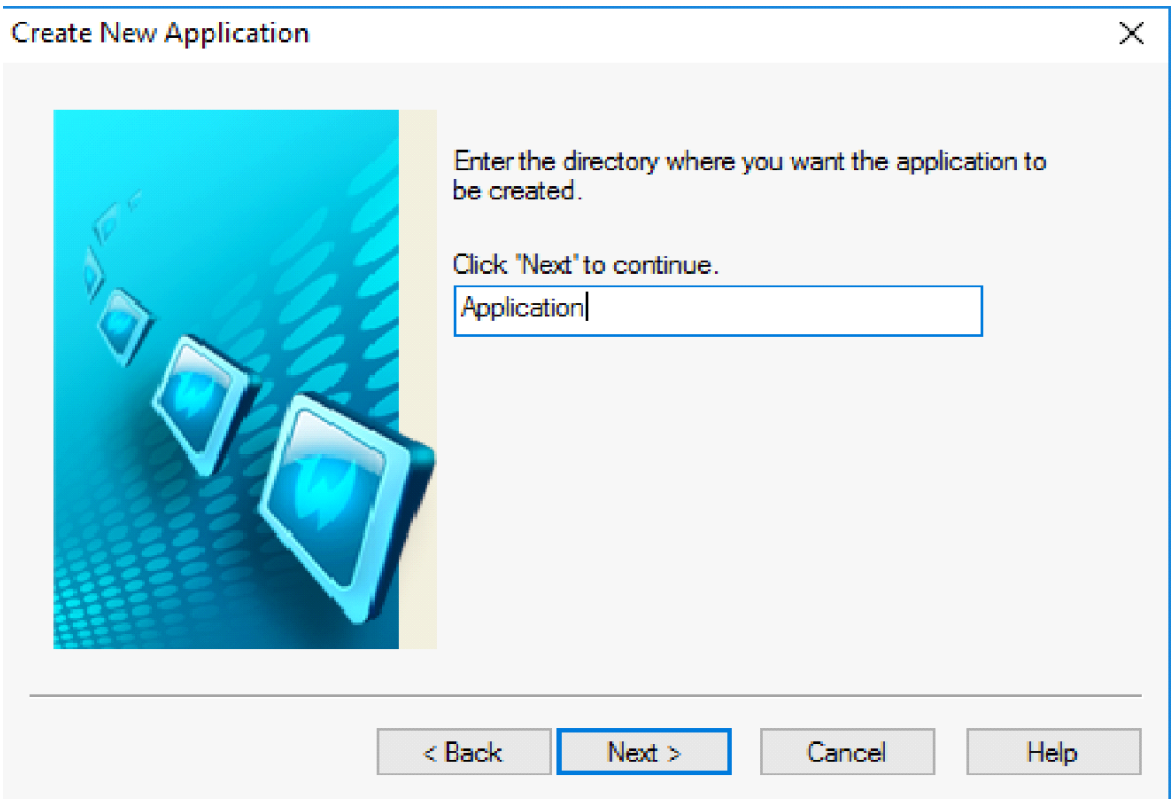


After that, go to 'File' -> 'DBDump'. Make sure you have an Application selected, or this option will be disabled. You will see the following dialog:



Hit 'OK', then the dump file will be saved under '**C:\Users\Public\Wonderware\Intouch Applications\[Name of selected Application's directory]***'.

*Refers to the directory name you specified when you first created the Application:



Back on the Import workspace, click on this Upload button to open File Explorer. Navigate to '**C:\Users\Public\Wonderware\Intouch Applications\[Name of selected Application's directory]**', then open the CSV dump file you just created. Once the file is uploaded, the workspace will tell you how many Tags are defined in the file.

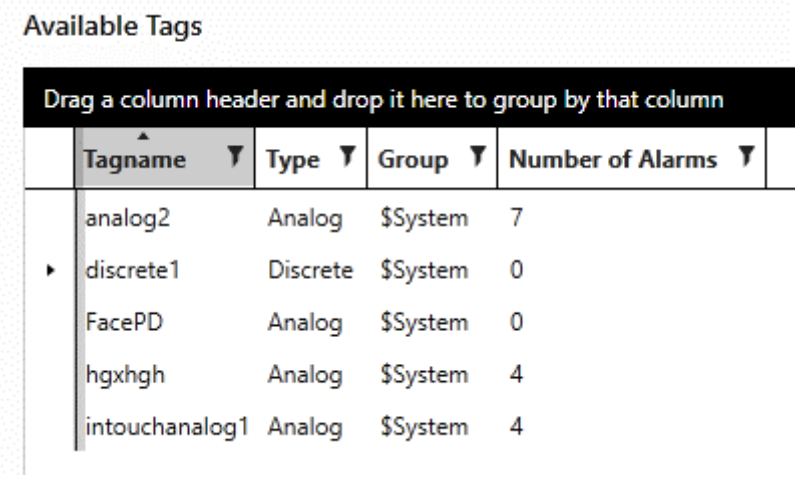
If any of the Tags have already been configured under the selected Application, the workspace will let you know about this, too. Tag definitions must be unique within Applications; the same Tagname can be defined multiple times across your entire InTouch system, as long as each definition is inside a different Application.

If the CSV file contains at least one Tag to import to the selected Application, the Next button will enable. Click on it to enter the Tag selection

phase.

Select Tags

The available Tags will appear on the left grid:

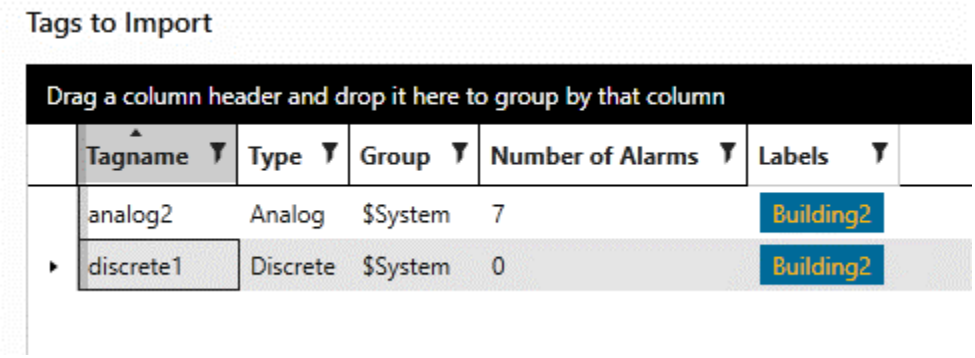


Labels may be attached to any Tag. See the Labels for more information regarding Labels.

Click the 'Add' button to attach Labels to the selected Tags.

Click the 'X' button to delete the Label to the left.

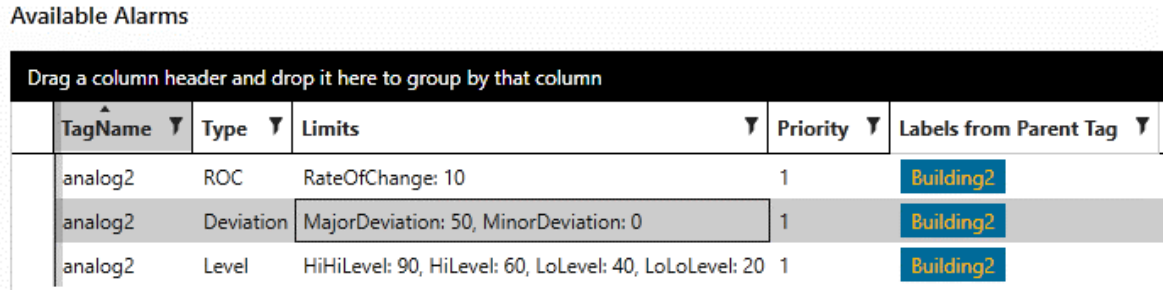
Click the 'Navigate' button on the right to configure Labels in the Labels workspace.



The Next button will enable once you have at least one Tag under 'Tags to Import'. Click 'Next' to advance to the Alarm selection phase.

Select Alarms

You'll see the same type of screen here. This time, you will select the alarms from the Tags you chose from the previous step.



Each limit under 'Limits' refers to a different alarm. They are separated by commas. For each distinct Tag, the total number of limits should equal the 'Number of Alarms' from the previous grid.

Click this button to move all available alarms to the 'Alarms to Import' grid and attach the selected Strategy plus additional Label(s) to them.

Click this button to move the selected alarms from 'Available Alarms' to 'Alarms to Import' and attach the selected Strategy plus additional Label(s) to them.

Click this button to remove the selected alarms from 'Alarms to Import' back to 'Available Alarms'.

Click this button to remove all 'Alarms to Import' back to 'Available Alarms'.

Labels

Labels may be attached to any Tag. See the Labels for more information regarding Labels.

Click the 'Add' button to attach Labels to the selected Tags.

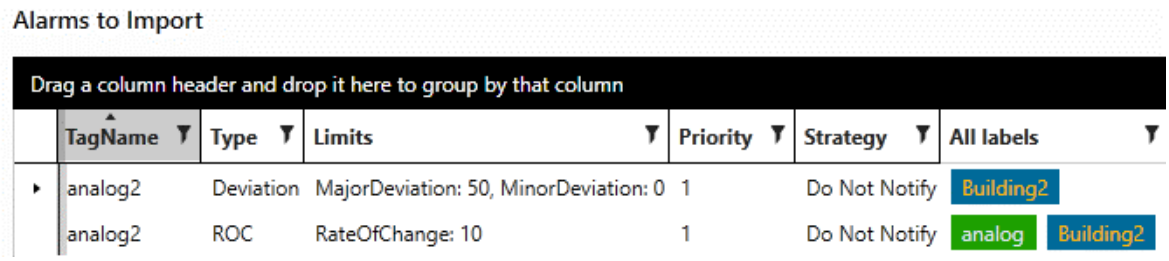
Click the 'X' button to delete the Label to the left.

Click the 'Navigate' button on the right to configure Labels in the Labels workspace.

Strategies

Select the Strategy that will dispatch the selected alarms.

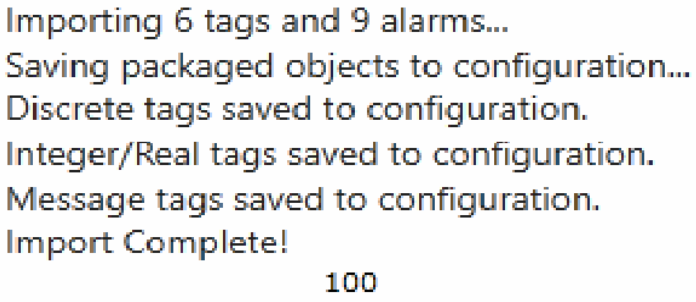
Click the 'Navigate' button on the right to configure Strategies in the Strategies workspace.



Once you have at least one alarm under 'Alarms to Import', click 'Next' to import the selected tags and alarms into your WIN-911 configuration.

Import Progress

Upon a successful import, the workspace will say 'Import Complete!' at the end of the message:



If any errors occur during this process, the progress message will reflect those errors. Import progress for each Tag is independent from progress of the others. Thus, if one Tag fails to import, the others should still continue. The number at the bottom indicates the real-time percentage of the import that is complete.

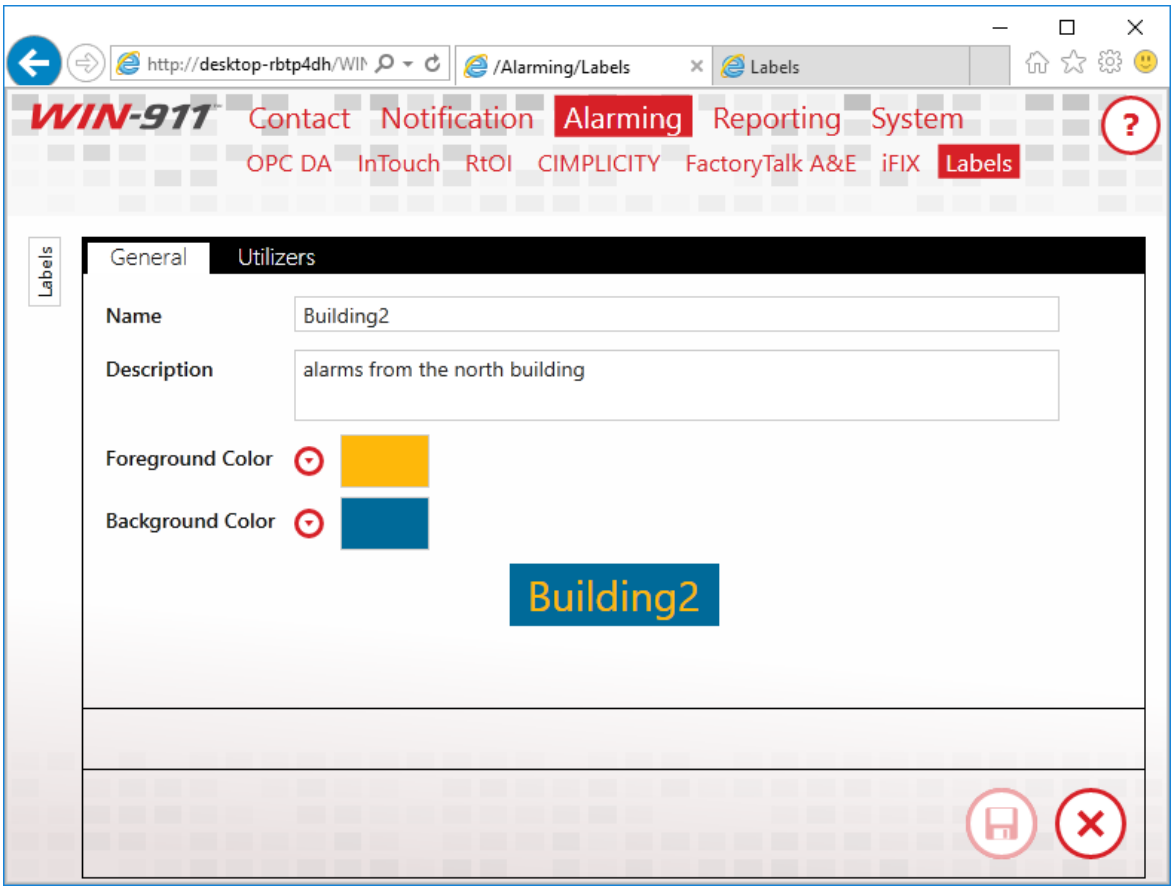
InTouch Runtime

To begin monitoring InTouch alarm events, WIN-911 must connect to a running HMI via the WIN-911 InTouch module. To do this, first start your InTouch application (WindowViewer), then start WIN-911 InTouch.

Labels

Overview

Labels can be attached to alarms as a method of organization. They can also be used in Advanced Tactics to change the flow of notification.



Name

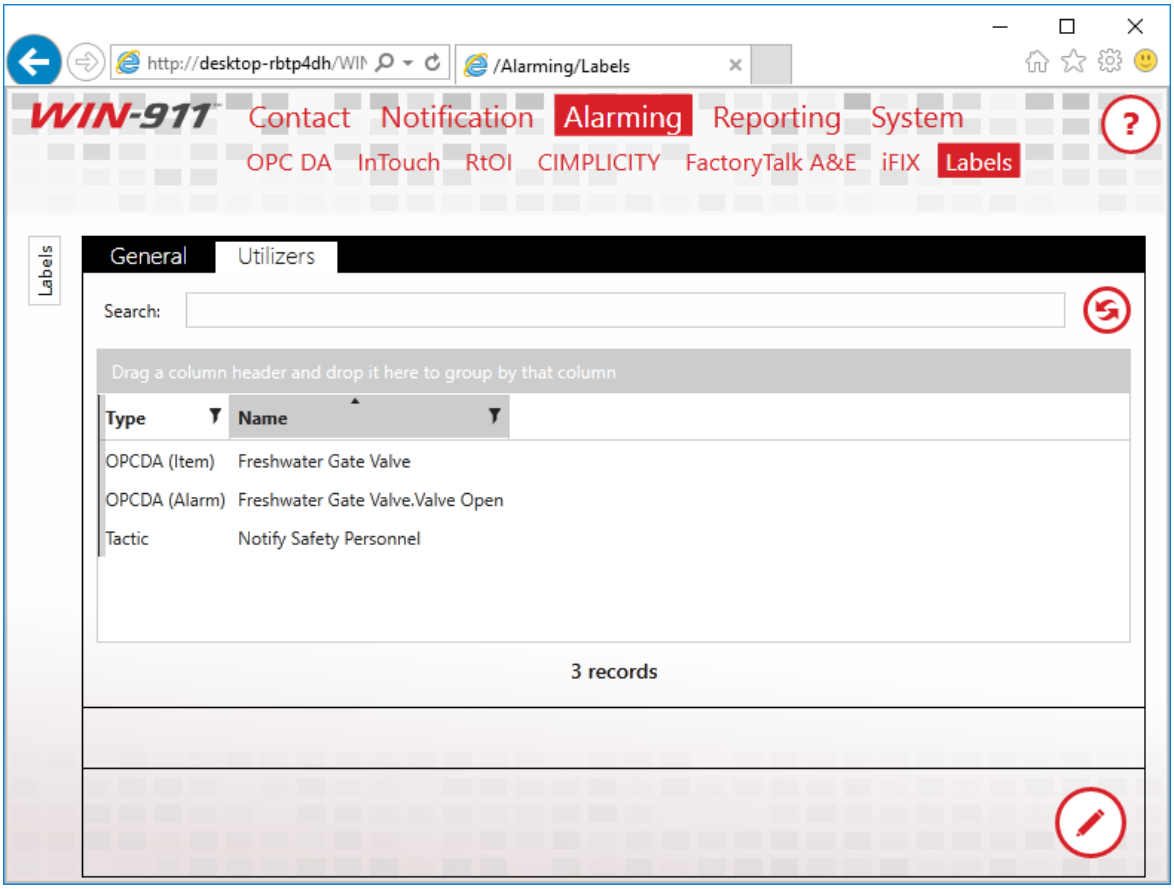
This is a unique identifier for the Label. Make it as descriptive as possible.

Description

The Description adds extra context to your Label. This is an optional field.

Colors

Each Label may be assigned a foreground and a background color. This is a great way to make Labels visually distinctive in Notifiers which can display them, like Email or the Log Viewer.



Utilizers

Labels may be applied to alarms, filters, or data items and referenced in Advanced Tactics by Decision Blocks. The list of items which reference the Label is displayed here. If a Label is in use, it may not be deleted. Use this screen to determine where the current Label is referenced.

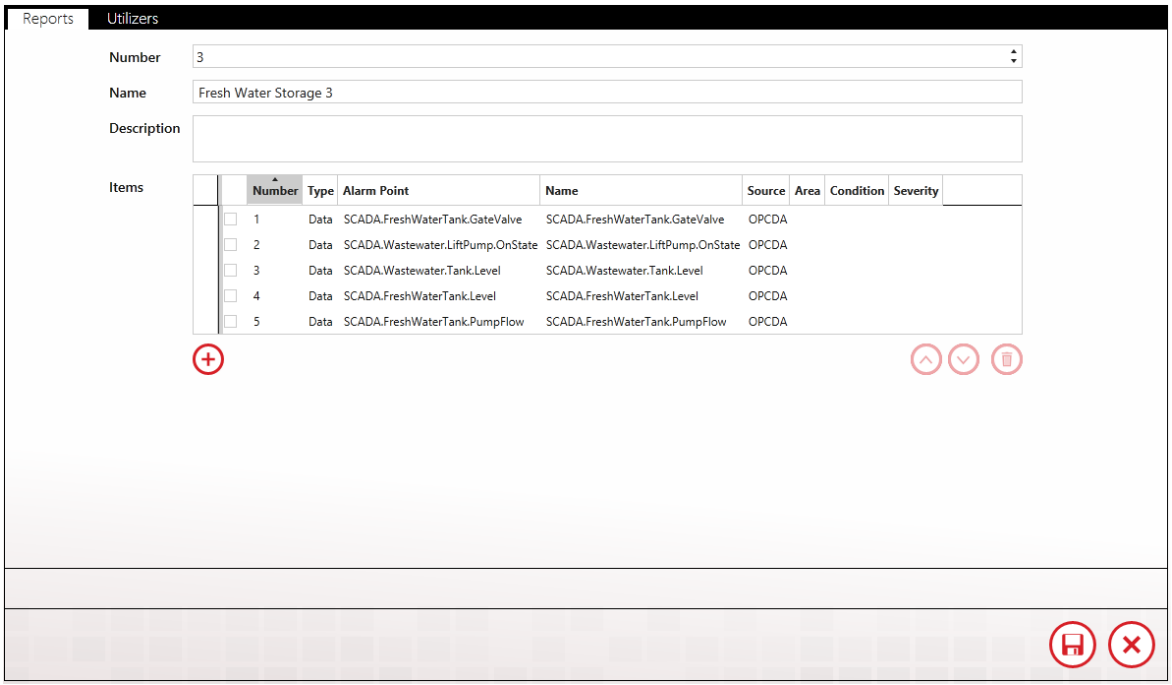
Reporting

Reports provide operational data that is not necessarily associated with alarm conditions. Reports can be dispatched in accordance with a strategy or in response to a query from a remote user.

Reports can be used to:

- query current operating conditions
- provide additional context to alarm events
- organize information

Note: Not all data sources support Reporting.



Number

Each report must have a unique number that distinguishes it from the others. When WIN-911 delivers a report, this number will be used to identify it. This number may also be used to request the report (instead of requesting by name).

Name

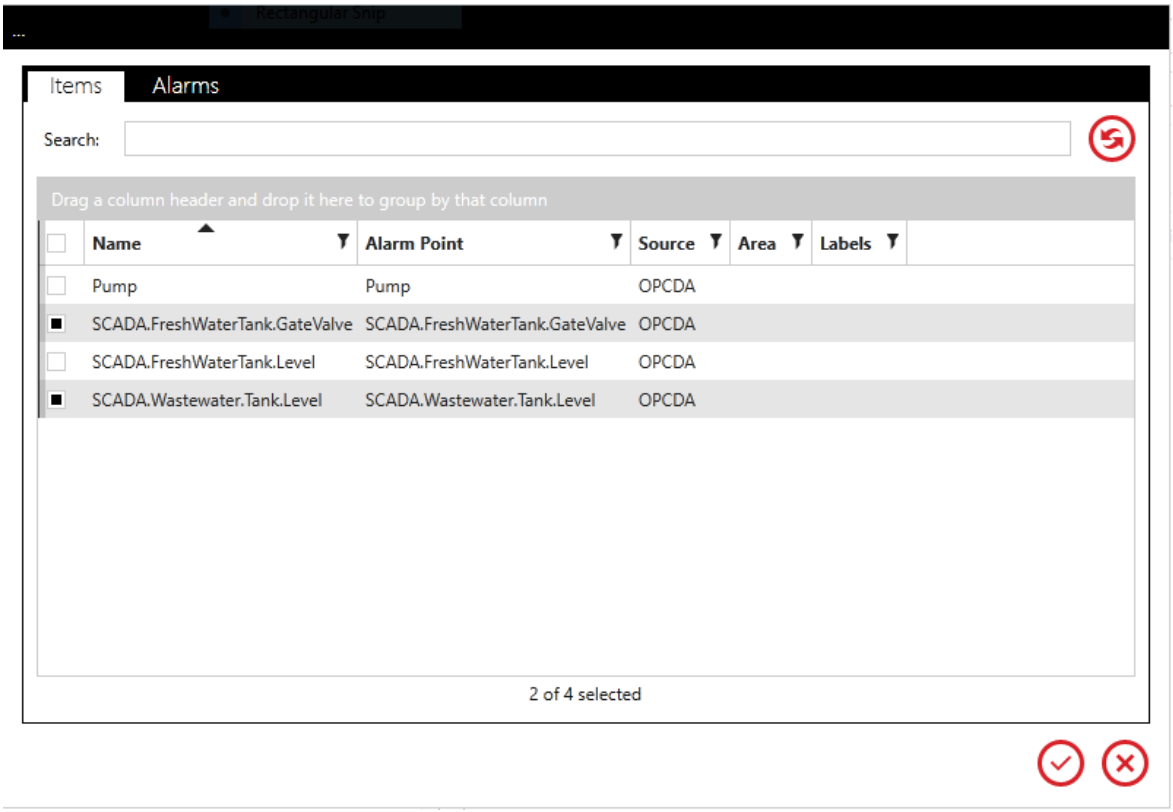
Each report must have a unique name.

Description

An extra text field for organization and administration purposes. The description can contain location data (like Lift Station 22), or a description of the data/alarm that adds additional context.

Items and Alarms

Select the items and/or alarms to be included in a Report. Clicking the  button in edit mode will bring up the Items/Alarms selection form. A search filter is provided at the top of the item list to limit the displayed items based on the selected property and text entered in the search text entry box.


Items
Alarms
Search:
Drag a column header and drop it here to group by that column
Name
Alarm Point
Source
Area
Labels
Pump
Pump
OPCDA
SCADA.FreshWaterTank.GateValve
SCADA.FreshWaterTank.GateValve
OPCDA
SCADA.FreshWaterTank.Level
SCADA.FreshWaterTank.Level
OPCDA
SCADA.Wastewater.Tank.Level
SCADA.Wastewater.Tank.Level
OPCDA
2 of 4 selected

System

Info

Serial Number

This number specifies information about the software which may be required when contacting WIN-911 Software.

Support Code

The support code identifies what support services this product is entitled to. It may be required when contacting WIN-911 Software for support.

Standby, Activate WIN-911

WIN-911 can be put into "Standby", which stops WIN-911 from conducting alarm notifications. From "Standby" WIN-911 can then be activated by clicking the "Activate" button, causing the remote notifications to resume.

Tech Support

You can contact WIN-911 Tech Support at Support@WIN-911.com or call (800) 331-8740 between the hours of 8:00 AM and 5:00 PM Central, Monday through Friday.

WIN911 Administration

WIN-911 Log Viewer

WIN-911 activity can be monitored using the *WIN-911 Log Viewer*. This tool displays log entries written to the operating system's Event Viewer in a convenient format that allows the user view, sort, and trace WIN-911 activity. The Log Viewer has two modes of operation Live and Historical. The live mode displays only alarm events that are in progress and updates automatically every 5 seconds. History mode freezes the display and allows you to search back in time for old/expired alarm events. The user can acknowledge individual alarms locally when an alarm event is focused.

Located in the upper left of the WIN-911 Log Viewer banner is an indicator in parenthesis the displays the operational mode of WIN-911. Valid indications should be Active or Standby.

Live

In live mode, the display will only show active alarms. The Viewer automatically refreshes every five seconds ensuring the user a near-live experience of WIN-911 activity.

Historical

This mode displays all alarm events, current and expired. It allows the user to look back in time at by using the *Display Events From* date/time brackets.

Settings

The user can customize the display by selecting which columns of data to include. Click on the gear icon located on the upper-right. From the selection list, you can choose to include columns by checking the box to the right of the option. The available columns include:

- Select: Check-box that selects the associated alarm event.
- State: Icon indicating Active/Inactive, Acknowledged/Unacknowledged
- Most Recent Event: Date and time of the most recent activity concerning the associated alarm event.
- AlarmLifetimeId: WIN-911 assigns each alarm event an internal GUID that identifies it. This GUID is referred to as AlarmLifetimeId and is included as an option for display.
- Alarm Point: Tagname of point name of the individual alarm
- Condition: High, HiHi, Low, LoLo, Opened, Closed, etc.
- Source Type: The type of data source or SCADA (HMI) that the alarm event originates from.
- Source: Specific data server that the alarm event originates from.
- Strategy: the name of the strategy that the alarm event is assigned.
- Initial: Date/Time when the alarm event is triggered.
- Labels: Label assigned to the alarm event for organization and remote notification processing.

WIN-911 Log Viewer Collection Selector List

Alarm event entries can be grouped, filtered, and sorted using the tools located across the top of the view window. The black bar running across the top is a grouping workspace where column headers can be dragged and dropped. In the column headers is a filtering tool to right of the column titles. This combination of tools allows the user a virtually unlimited array of ways to focus the view window to meet his/her specific needs.

Sorting

When the name column header has a black triangle pointing down, the alarm events will be arranged by name in descending alphabetical order. Clicking on the triangle will reverse the list and cause it to be arranged in ascending order. A third click on the triangle will deselect the column. Select, State, and Labels are the only columns that cannot be filtered.

Filtering

On the right side of the property column heading is a black filter symbol. Clicking it causes a custom filter design form to appear. This form provides several options the WIN-911 administrator can use to exclude unwanted alarm events from being listed in the collection selector. "And/Or" expressions can be created that key on the selected property data for inclusion or exclusion. The selected property (Name, Description, Machine Name, or Server Name) column header will be highlighted yellow while the custom filter is applied. Any property column can be filtered.

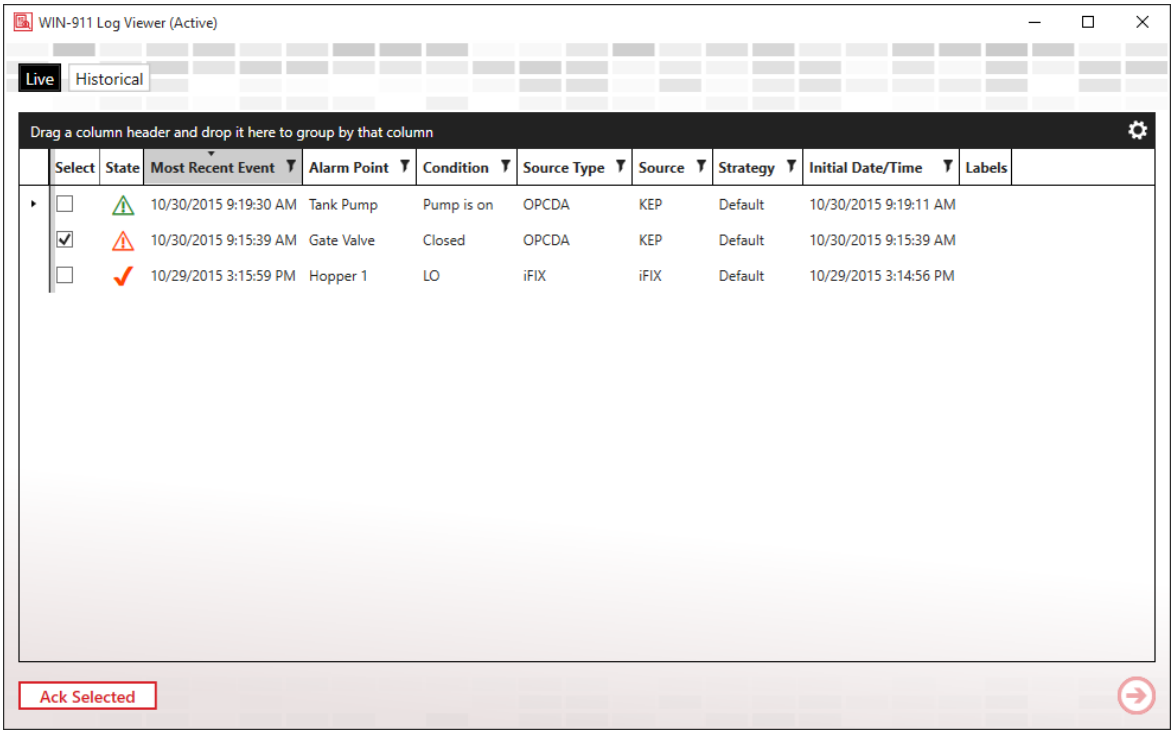
Grouping

Dragging and dropping a property column header into the black area above the alarm event list will cause the collection selector to group the alarm events accordingly. The collection selector now lists the title of the selected object in bold font with a drop-down arrow to the left. Click on the drop-down arrow and the collection selector will drop a list of all the alarm events that contain a particular object title. Groups can be compounded by dragging another object into the "Group by" field. Grouping can be removed by hovering over the group title and clicking the "X" that appears to the right of the title. Any property can be grouped.

WIN-911 Log Viewer Alarm Event List

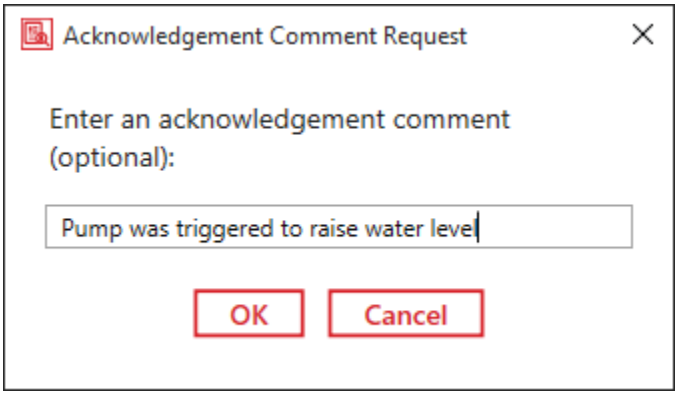
The WIN-911 Log Viewer has two pages that the user can toggle between, the Alarm Event List (default), and the alarm details. The alarm event list displays, in Live mode, displays all current alarm event. In Historical mode, the display lists all alarm events that occurred between the time and brackets selected by the user. The alarm details page expands the focus of the selected alarm event, giving the user a multi-tabbed display that allows the user to drill-down into various details of the alarm event. The tabs include Notification, Acknowledgement, Strategy Execution, Tactic Execution, and State Change.

Live View



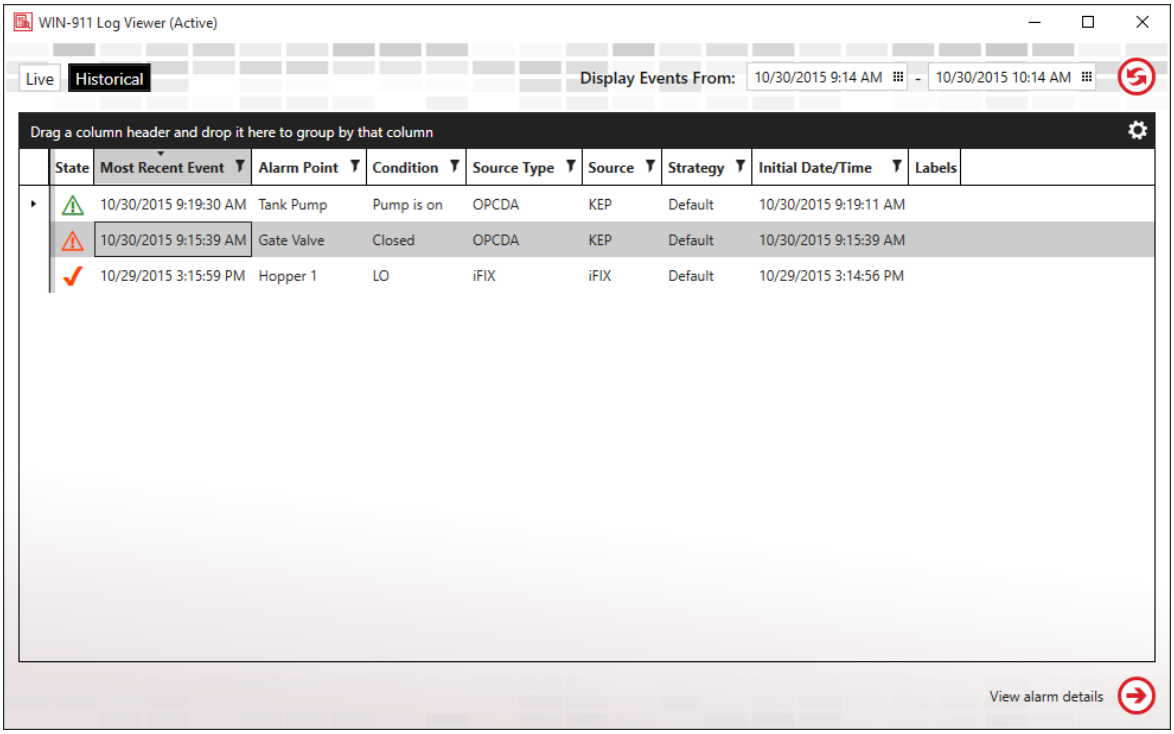
WIN-911 Log Viewer in Live mode. This mode will only show current (in-progress) alarms. The view is automatically refreshed every five seconds. Alarms can be acknowledged by selecting the desired alarms(s) and clicking the Ack Selected button at the lower left corner of the viewer. You can toggle the viewer into alarm details mode by double-clicking the desired alarm event.

When acknowledging an alarm from the WIN-911 Log Viewer, select the desired alarm and click the Ack Selected button.



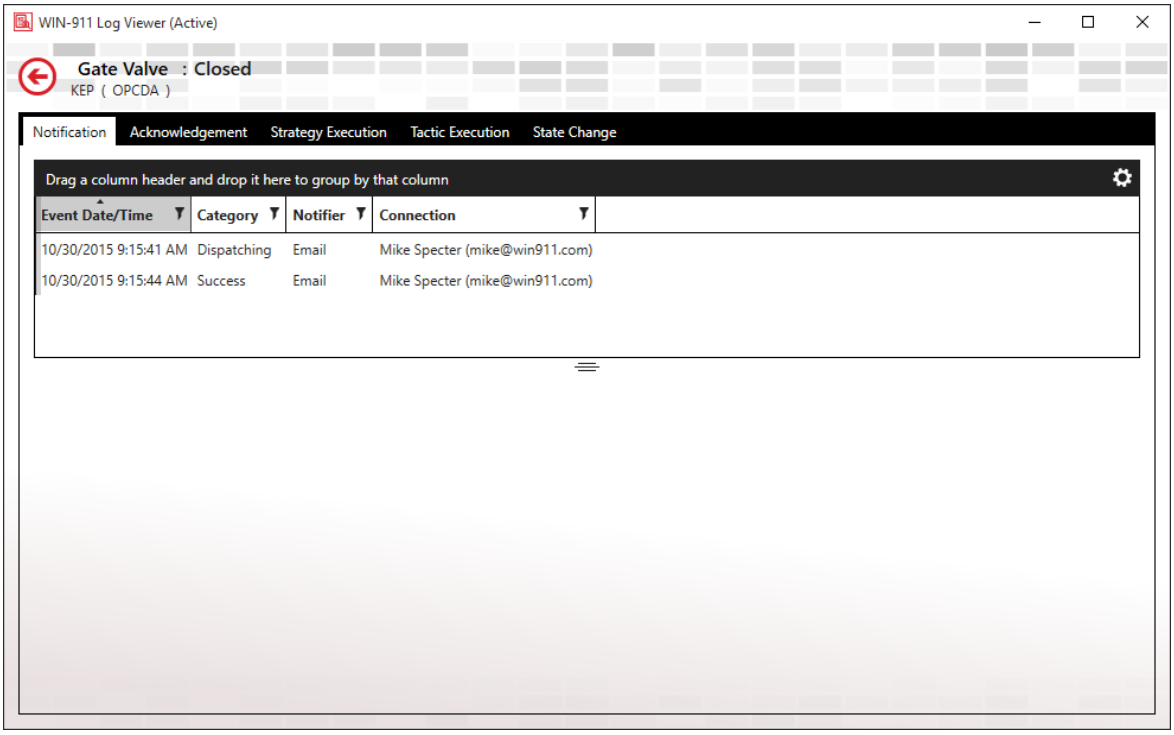
A confirmation pop-up box will appear and present the actor with the option to add a comment. Click OK to process the acknowledgement.

Historical View



WIN-911 Log Viewer in Historical Mode. This mode will display the entire history of the alarm events life cycle (current and expired) that occurred within the selected date and time as specified by user via the input tool located at the upper right. You can toggle into the alarm details page by double-clicking on the desired alarm event.

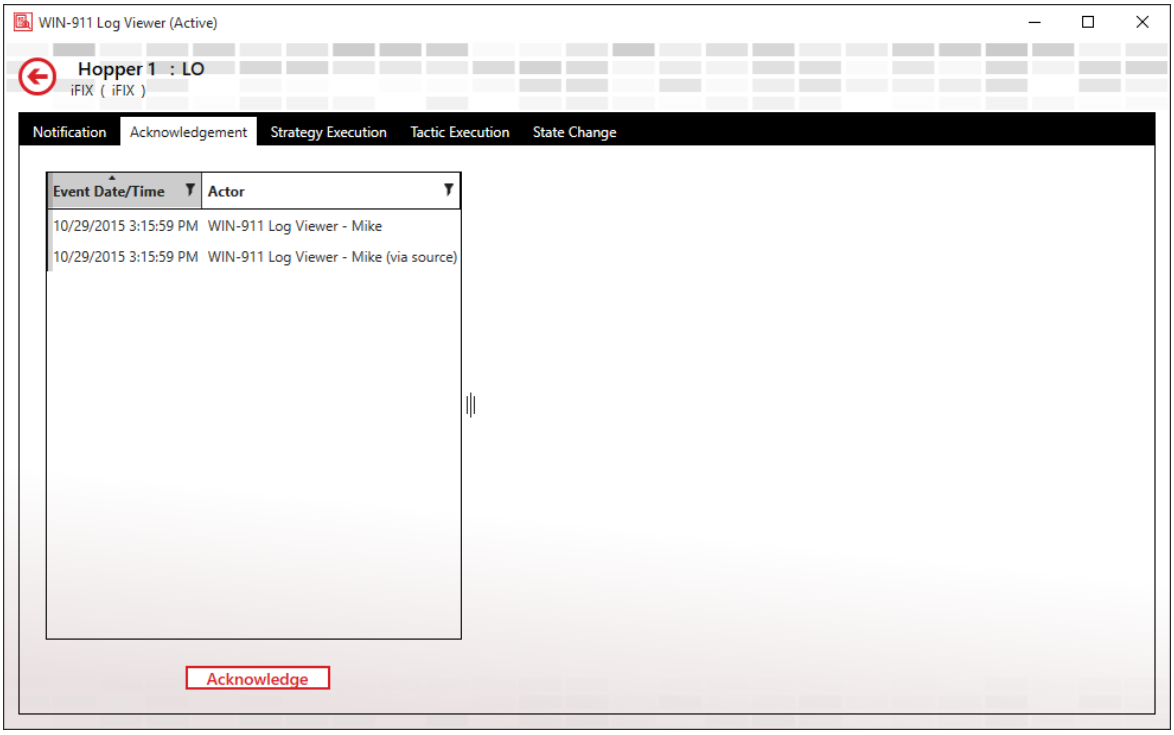
Detailed View, Notification Tab



The Notification tab will list the notification tasks that have been dispatched by the dispatcher and the results of the task as reported back by the notifier module.

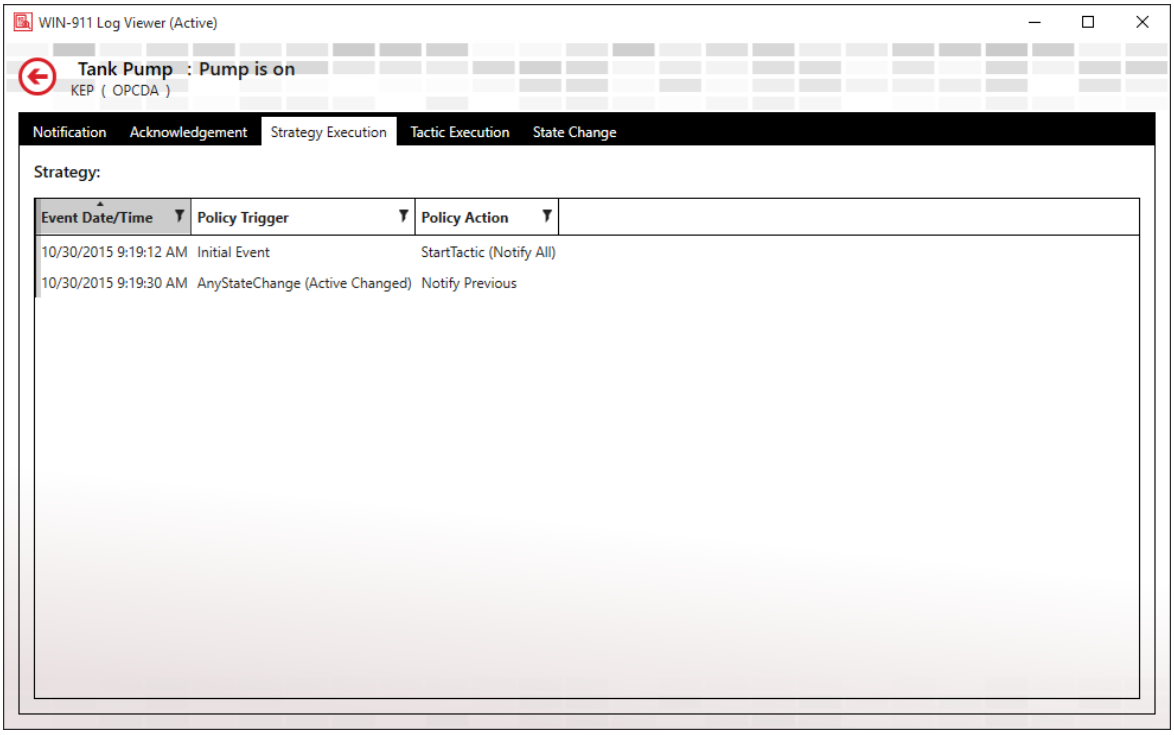
There are handles located on the borders of each viewing window that allows the users to modify the viewing area. When the amount of data exceeds what can be displayed at one time scroll bars appear to the right and bottom that the user can scroll through the full extent of the contents.

Detailed View, Acknowledgement Tab



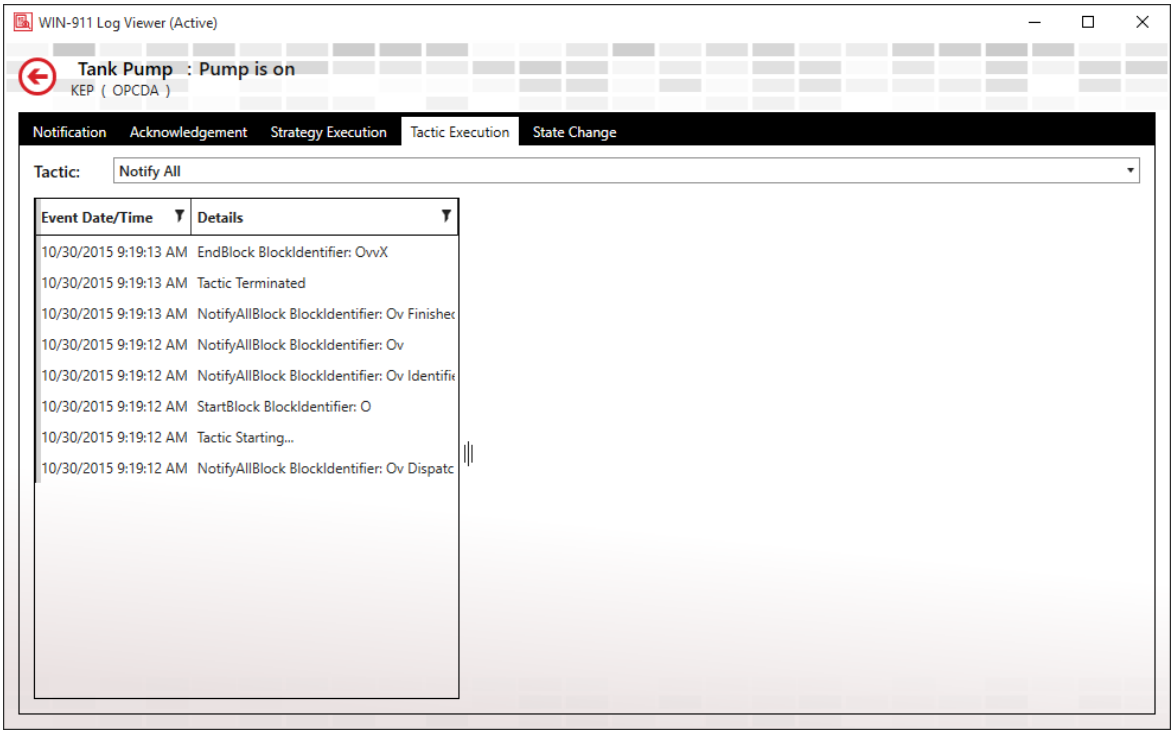
The acknowledgement tab will list all of the acknowledgement activity associated with the selected alarm event. If the alarm is yet unacknowledged then the Acknowledge button will be available at the bottom. The information will include time and date of the activity and the actor.

Detailed View, Strategy Execution Tab



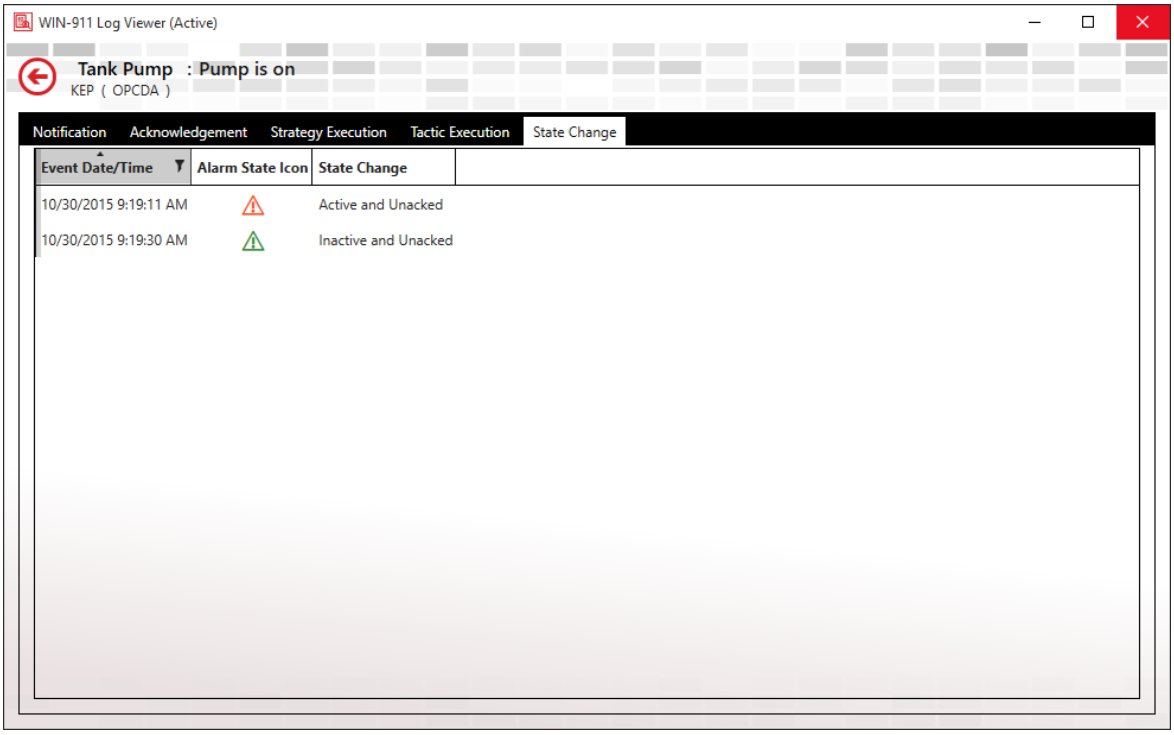
The strategy execution tab lists all of the strategy's activity as processed by the policies triggered. Information includes the time/date, policy trigger, and policy action.

Detailed View, Tactic Execution Tab



The tactic execution tab lists the activities of each of the tactics that have been triggered by the controlling strategy. Information includes event time/date and details.

Detailed View, State Change Tab



The State Change tab lists the states of the alarm event. The information includes event time/date, alarm state icon and state change text.

The various states include:

- Active and unacknowledged
- Inactive and unacknowledged
- Active and acknowledged
- Inactive and acknowledged

Managing Configuration Files

WIN-911 uses a set of Microsoft SQL databases to store and maintain its configuration. The configuration GUI is designed to make all necessary changes without the user needing to interact with the Microsoft SQL Server. However, there are certain "best practices" that can occur in the life of the product that might involve a basic knowledge of SQL Server Configuration Manager. Such situations are detailed below.

Backing Up Your Configuration

Any "best practice" for managing industry software assets includes keeping backups of your production configurations in order to restore your system in the event of a software or hardware failure. This is done using Microsoft SQL Server 2014\Microsoft SQL Server Management Studio.

1. Open *Microsoft SQL Server 2014\Microsoft SQL Server Management Studio*.
2. Select "MyServer"\WIN-911 for your server name, Database Engine is Server type and Authentication will be *Windows Authentication*. Click *Connect*.
3. Open the Databases folder in the Object Explorer tree. There you will find all of your WIN-911 configuration databases.
4. Right-click the first database in the list and select "*Tasks**Back up*..."
5. Confirm the back up by clicking *OK* at the bottom right of the Back Up Database page.
6. Repeat steps 4 and 5 for the remaining databases to complete the configuration back up.

Restoring Your Configuration

To restore your configuration, you must first have backed it up. You must also have a database created in your library with the proper name. For example: you must a database in your library named "MyServer-V8.Default.Dispatcher" (where MyServer is the name of the host computer). If the database does not exist then create one by right-clicking on the Databases folder and selecting New Database. Give it the proper name by following the syntax of the backup file. Typically, a backup file will be located at *C:\Program Files\Microsoft SQL Server\MSSQL 12.WIN-911\MSSQL\Backup\MyServer-V8.Default.Dispatcher.bak*.

1. Open *Microsoft SQL Server 2014\Microsoft SQL Server Management Studio*.
2. Select "MyServer"\WIN-911 for your server name, Database Engine is Server type and Authentication will be *Windows Authentication*. Click *Connect*.
3. Open the Databases folder in the Object Explorer tree. There you will find all of your WIN-911 configuration databases. If they are not, you will need to create them before proceeding.
4. Right-click the first database in the list and select "*Tasks\Restore\Database...*" This will bring up the *Restore Database* page.
5. Ensure the correct database is selected from the drop-down list in the *Source* section.
6. Verify the same is listed in the destination section and click *OK* at the bottom right.
7. Repeat steps 4 - 6 for the remaining databases in your configuration.

Migrating Your Configuration

Note: The Migration of Database Files is NOT supported with Microsoft SQL Server Express. This technique requires a minimum of In order to move your configuration file to a different machine or to mirror your configuration for a redundant setup you will need to use the SQL Server Import and Export Wizard.

1. Open Microsoft *SQL Server 2014\Microsoft SQL Server Management Studio*.
2. Select "MyServer"\WIN-911 for your server name, Database Engine is *Server* type and Authentication will be *Windows Authentication*. Click *Connect*.
3. Open the Databases folder in the Object Explorer tree. There you will find all of your WIN-911 configuration databases.
4. Right-click the first database in the list and select "*Tasks\Export Data...*" This will launch the Export/Import Wizard.
5. Click the *Next* button to bypass the welcome screen.
6. Data Source: Choose the *SQL Server Native Client 11.0* from the drop-down menu.
7. Server Name: Type the name of the SQL Server instance that contains the source data. Example: MyServer\WIN-911 ("MyServer" being your computer name).
8. Authentication: Choose "*Use Windows Authentication.*"
9. Database: Choose the database that contains the source data.
10. Click *Next* to go to "*Choose a Destination*" page.
11. Destination: *Choose SQL Server Native Client 11.0*.
12. Server name: Choose the server to receive the data, or choose a server from the list. The server name shall include the name of the instance that will contain database. For example: a server named Server3 would contain the following: Server3\WIN-911.
13. Authentication: Choose "*Use Windows Authentication*"
14. Database: Click *New...* to create a database on the receiving server for the export to write to. On the *Create Database* page enter the name of the database to be created and click *OK*.
15. On the *Specify Table Copy or Query* choose *Copy data from one or more tables or views* and click *Next*.
16. From the *Select Source Tables and Views*, check all of the sources EXCEPT the 1) *ModuleInformationEntries* and 2) *ServiceInformationEntries*. Then click *Next...*

17. Choose the "*Run immediately*" then click *Next* to advance to the "*Complete the Wizard*" page.
18. Click *Finish*.
19. Repeat steps 4 - 18 for the remaining databases in your configuration.

After all your databases are migrated you will need to run the Endpoint Mapper before using WIN-911 for the first time.

WIN-911 and Redundancy

Any "best practices" method for ensuring operational integrity should include the consideration of redundancy in the event that critical software or hardware fails. WIN-911 should be considered a mission-critical part of your operational nucleus and therefore have a plan for emergency situations where WIN-911 is no longer able to dispatch alarm events.

WIN-911 does not currently have redundancy logic that is able to determine the need for and/or execute a failover. But it does provide the system administrator with tools that can be used by third-party software to evaluate the health of WIN-911 and perform a failover when such a need should arise. These tools can provide information about the state of WIN-911 and change the operational mode of WIN-911 from Standby to Active or Active to Standby.

WIN-911 has two modes of operation, Active and Standby. Active is the default mode and actively monitors alarm events and dispatches remote alarm notifications. Standby is a mode that will suspend all remote notifications but does actively monitor alarm events. The mode of operation can be polled by third-party software and modified based on the results of the poll.

The tools are found in the Standby Activate folder (C:\Program Files (x86)\WIN-911 Software\WIN-911 Enterprise\Standby Activate). There you will find three command-line applications, Activate, IsActive, and Standby.

Activate: this command-line application, upon execution, will change the mode of operation for the local WIN-911 from Standby to Active.

Once the mode is set to active the local WIN-911 will commence remote alarm notifications.

IsActive: this command-line application, upon execution, will query the local WIN-911 instance for its operational mode. There are two valid responses, Active (indicating that it is conducting remote notifications) or Standby (indicating that it is monitoring alarms but not conducting remote notifications). If the application does not receive a valid response from WIN-911 in a timely fashion then the querying application can assume that WIN-911 is not capable of responding.

Standby: this command-line application, upon execution, will change the mode of operation for the local WIN-911 from Active to Standby. Once the mode is set to standby the local WIN-911 will stop all remote alarm notifications while continuing to monitor alarms.

Trouble Shooting

WIN-911 Component's Operational Status

WIN-911 is designed to be an "always on" service that is available for alarm notification tasking and configuration editing at all times. However, components of WIN-911 can be shutdown manually or by the operating system under extraordinary circumstances.

Each module of WIN-911 is composed of an Application Server, which runs in IIS and a runtime executable that runs in the system's services. Thus, the dispatcher module is composed of a dispatcher application server and a dispatcher runtime executable. Each component is capable of running independently of the other. So, the application server can be running in IIS and the runtime service can be stopped (or vice-versa).

If there is any question about the operational status of the WIN-911 system it can be verified by checking Services to ensure all modules labeled "WIN-911" are started and in automatic startup mode. The application servers can likewise be checked in the Internet Information Services (IIS) Manager.

WIN-911 AppServer's Operational Status

View the application server's status by clicking Start and entering *IIS* in the *Search programs and files* field. This will bring up the Internet Information Service (IIS) Manager. In the Connections tree (left pane) highlight Application Pools. This will bring up the list and status of application pools. Check that the following are started:

- WIN-911.Dispatcher
- WIN-911.Notifier.Email
- WIN-911.Source.OpcDa
- WIN-911.Reporting
- NavigationAppPool
- WIN-911.Notifier.Voice
- WIN-911.Notifier.Mobile911
- WIN-911.Source.iFIX
- WIN-911.Source.FTAE
- WIN-911.Source.Cimplicity
- WIN-911.Notifier.SMS
- WIN-911.Source.InTouch.

WIN-911 Services Status

View the services status by clicking *Start* and entering *Services* in the *Search programs and files* field. This will bring up the Services administration window. Scroll to the W section of the list and check that the following are started:

- WIN-911 Dispatcher Runtime
- WIN-911 Email Runtime
- WIN-911 OPC DA Source Runtime
- WIN-911 Reporting Runtime
- WIN-911 Cimplicity Runtime
- WIN-911 FTAE Runtime
- WIN-911 Mobile-911 Runtime
- WIN-911 Navigation Runtime
- WIN-911 Voice Runtime
- WIN-911 SMS Runtime

WIN-911 Diagnostic Information

WIN-911 writes information, error, and warning messages to the event logger within the operating system and these messages can be queried using the Event Viewer and the WIN-911 Dispatcher Diagnostic tool.

There are three modes of detail intensity that the WIN-911 Administrator can choose from while testing and troubleshooting: Default, Debug, and Trace. The default setting logs standard information, warnings and errors, while debug logs finer details concerning the program activity. Trace is the most verbose of the three. These options are set as follows:

1. Stop all WIN-911 AppServers (IIS) and WIN-911 Runtime Services (listed above).
2. Open Windows Explorer and na*vigate to c:\inetpub\wwwroot\Dispatcher*.
3. *Open Web.config with* Notepad and use the *Edit\Find* tool to locate string "*loggingFlags*".
4. Change the *loggingFlags* value from "*Default*" to "*Debug*" (or "*Trace*", case sensitive and including quotation marks).
5. Save this file and close *Notepad*.
6. Navigate back one folder to *wwwroot* and repeat steps 2 through 6 for any other module you are troubleshooting.
7. Start all WIN-911 modules (AppServers and Runtime Services) and conduct troubleshooting.

Once troubleshooting is complete you will want to return your "*loggingFlags*" back to the "*Default*" setting. Use the procedure listed above but replace the words "Debug" and "Trace" with "Default".

Event Viewer

To view system messages click *Start* and enter *Event Viewer* in the *Search programs and files* text box. This will bring up the event viewer. Dispatcher messages are written to the *Windows Logs>Application* log. All other module messages are written to the *Applications and Services Logs>WIN-911*. System messages concerning WIN-911 will

appear in the center pane with options to view general and detailed information about the selected message. These messages can be used to troubleshoot issues and can be attached an Email message that can send to WIN-911 Tech Support for evaluation (Support@WIN-911.com).

Note: Error message generated by Mobile-911 Server are written to Applications and Services Logs>Mobile-911.

WIN-911 Log Viewer

WIN-911 Software developed a convenient tool for viewing system messages concerning the dispatcher module which is the main engine of WIN-911, responsible for executing strategies and tactics. The Log Viewer presents a verbose history of strategies and their related tactics by capturing a snap-shot of events and messages at the time the diagnostics tool was launched. It can be refreshed by relaunching the tool.

Select the event you wish to evaluate. Each event has six properties (Initial Date/Time, Alarm Point, Condition, Source Type, Source, and Strategy) that can be filtered as well as time window with a beginning and end time to constrain the viewer presentation.

Double-click on the desired event to bring up a detailed list of diagnostic information. The data is divided into notification, acknowledgement, strategy and tactics execution groups. A red background on an event indicates the presence of an error that was logged during the event. A yellow background indicates the presence of a warning.

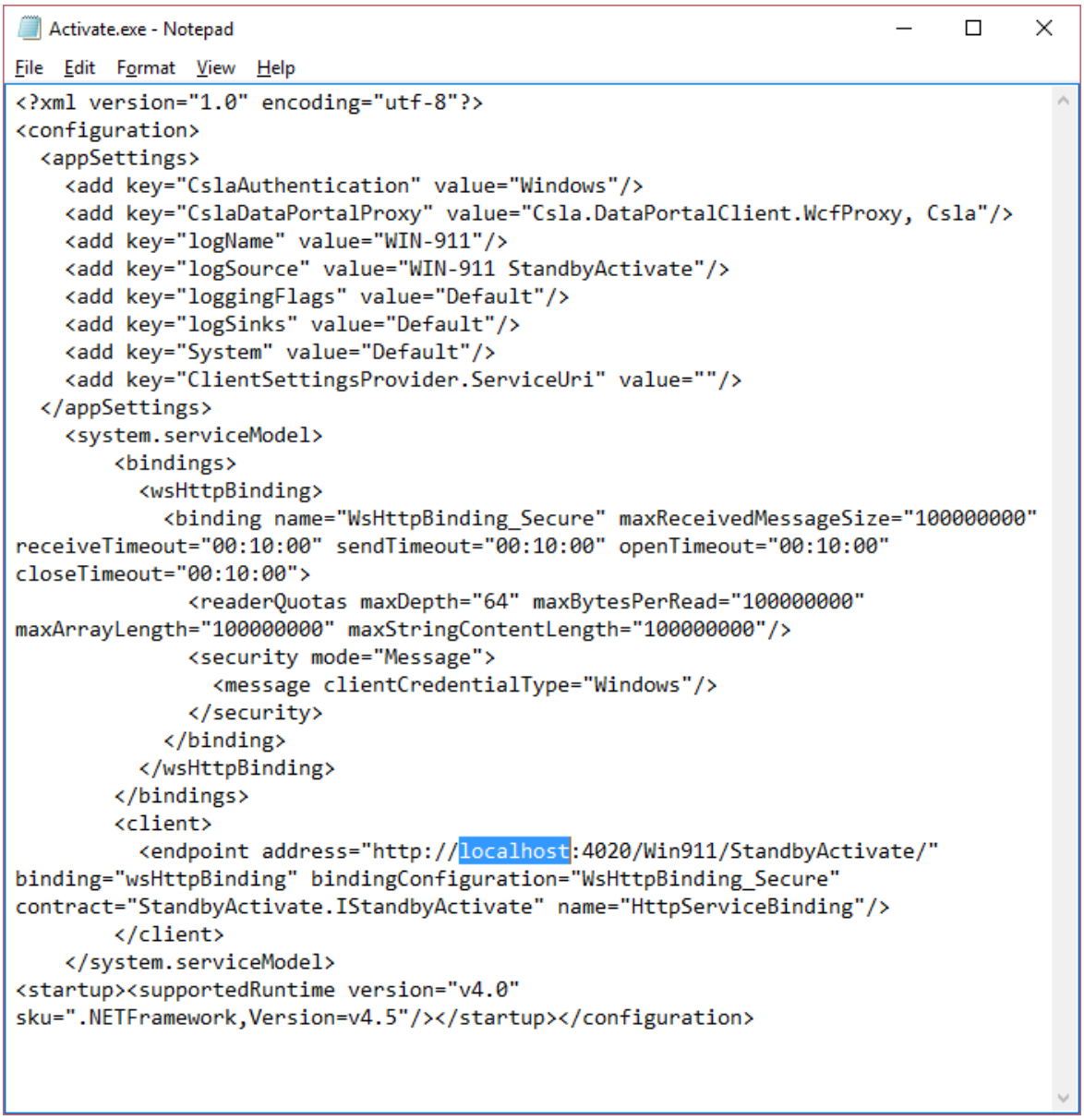
Remote Standby & Activate

Overview

The Standby status of a WIN-911 Dispatcher module can be both accessed and controlled across the network through the utilization of three simple applets. These applets are particularly useful when scripting hot backup failovers within your SCADA system or for displaying the Standby status of one or more WIN-911 systems within your HMI. Details of the applets and their behavior follow.

Target

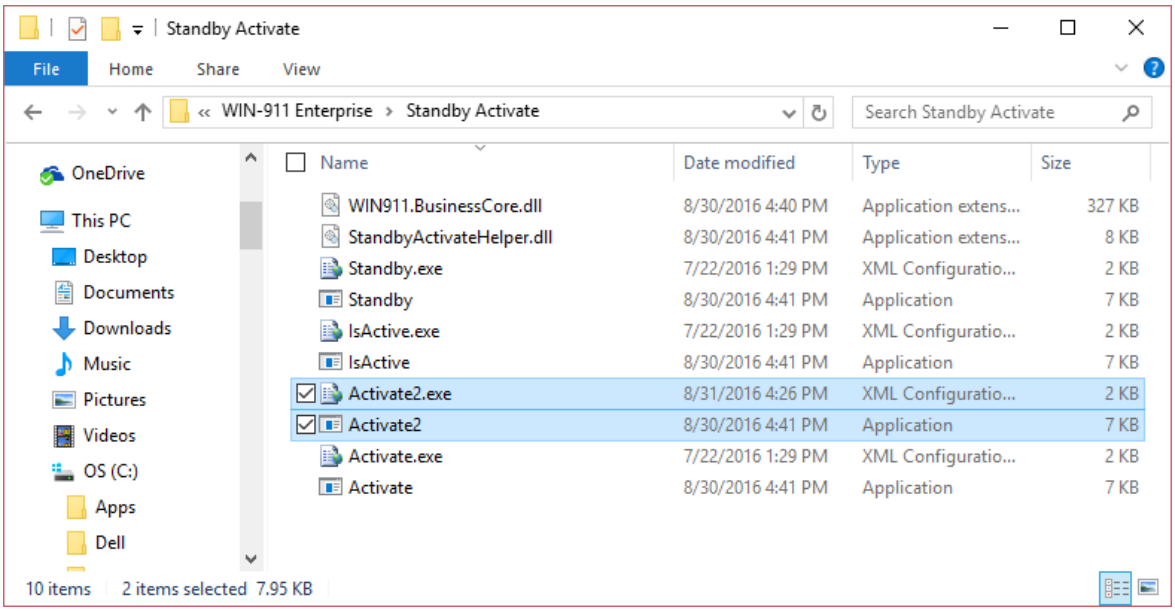
By default, each applet targets the WIN-911 Dispatcher installed on the local computer. This can be easily modified in the .config XML file accompanying each applet. Simply open the appropriate configuration file with a text editor and change the endpoint address (highlighted in the figure below) from localhost to the name or IP address of the target system. Typically, the computer name is recommended as IP addresses can be dynamic.



NOTE: The default install location for these applets is a protected directory and will require elevated priveledges to make configuration file edits. You can run your text editor as Administrator or make a copy of the applets to a more accessible directory.

Applets can be copied onto machines across the network from WIN-911. When copying an applet to another location on the network, be sure to also copy its configuration file and its two DLL dependencies. Copying the utility directory in its entirety is recommended.

Moreover, multiple copies of an applet can be made on a single machine to target different WIN-911 Dispatcher instances. Simply copy both the exe and its configuration file and rename the copies to match one another (e.g. Activate2.exe with Activate2.exe.config or Activate_Secondary.exe with Activate_Secondary.exe.config). You can now edit each configuration file to target different WIN-911 Dispatcher instances.



Network/Security Considerations

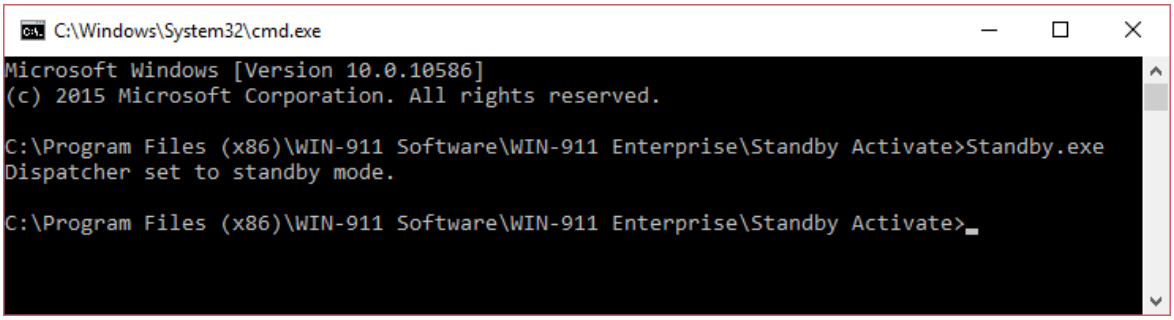
The applets use WCF for communication with the WIN-911 Dispatcher. By default, communications are secured at the message level by Windows and take place over HTTP on TCP port 4020. As such, the account under which the applets are executed must have credentials recognizable to the WIN-911 system (i.e. same domain or same username and password). Additionally, your network domain policy and firewalls should be adjusted to permit communication. These defaults can be changed by your system administrator – see the

following resource for more information:
https://msdn.microsoft.com/en-us/library/ms733027(v=vs.110).aspx

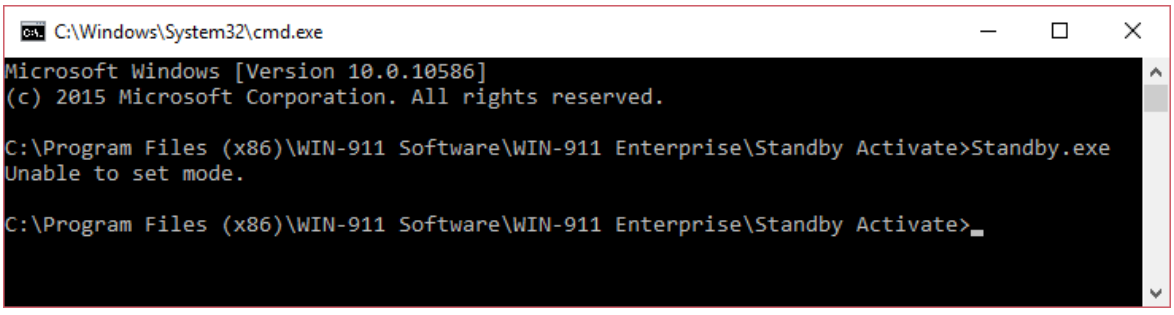
Standby.exe

Description: This applet attempts to place the targeted WIN-911 Dispatcher in standby mode. Note that a Dispatcher already in standby mode will still indicate success when this applet is executed against it.

Success Return Code: 0
Success Console Output: localized string similar to “Dispatcher set to standby mode.”



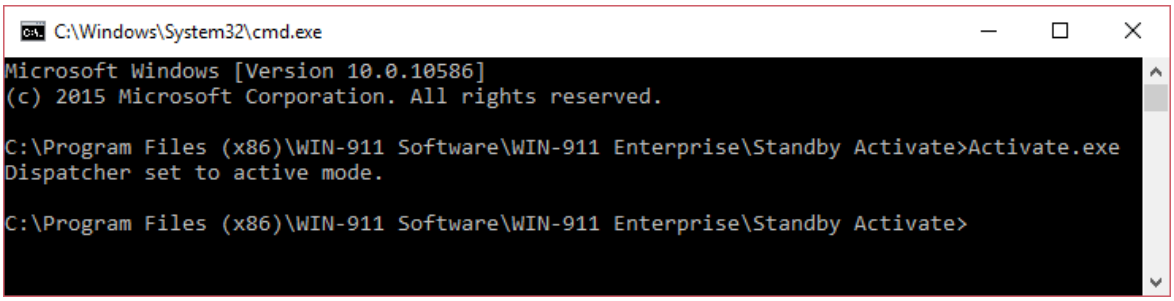
Failure Return Code: 1
Failure Console Output: localized string similar to "Unable to set mode."



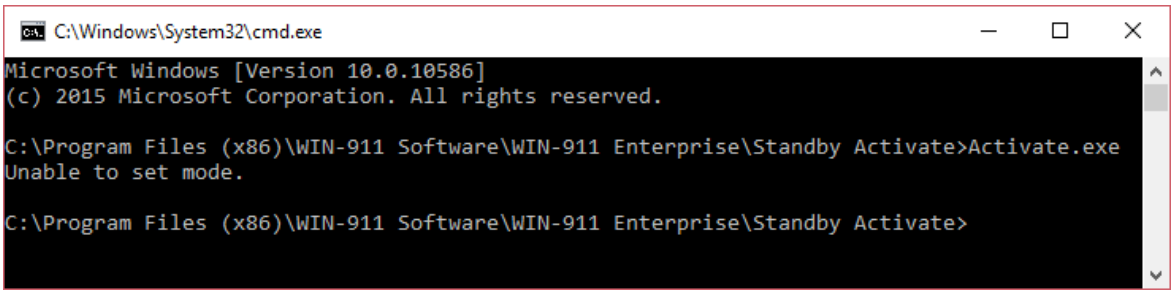
Activate.exe

Description: This applet attempts to place the targeted WIN-911 Dispatcher in active mode. Note that a Dispatcher already in active mode will still indicate success when this applet is executed against it.

Success Return Code: 0
Success Console Output: localized string similar to "Dispatcher set to active mode."



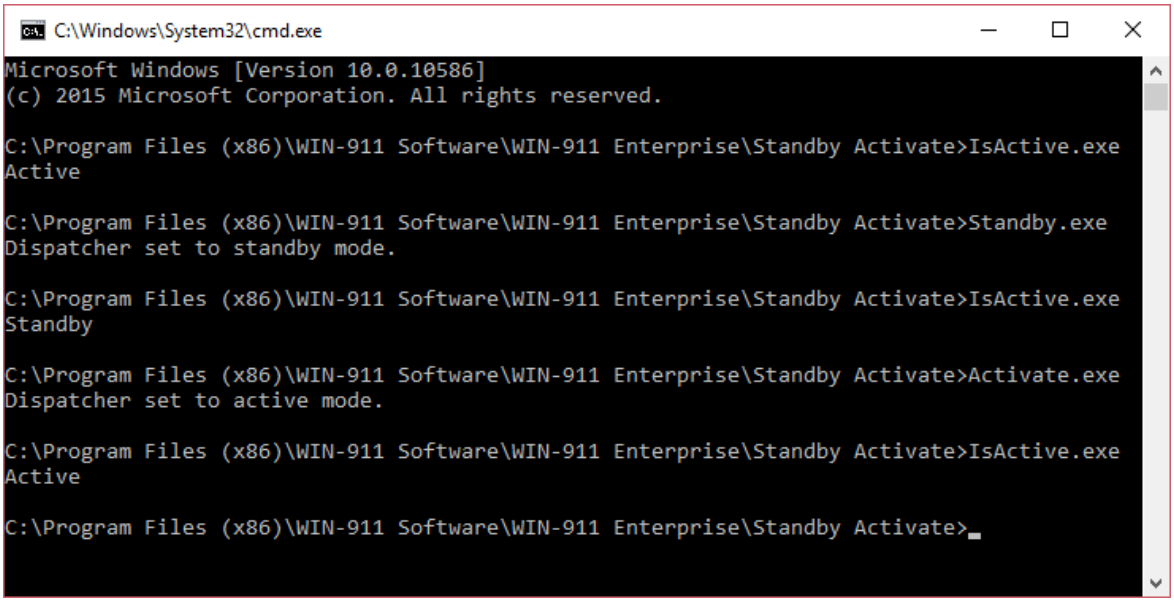
Failure Return Code: 1
Failure Console Output: localized string similar to "Unable to set mode."



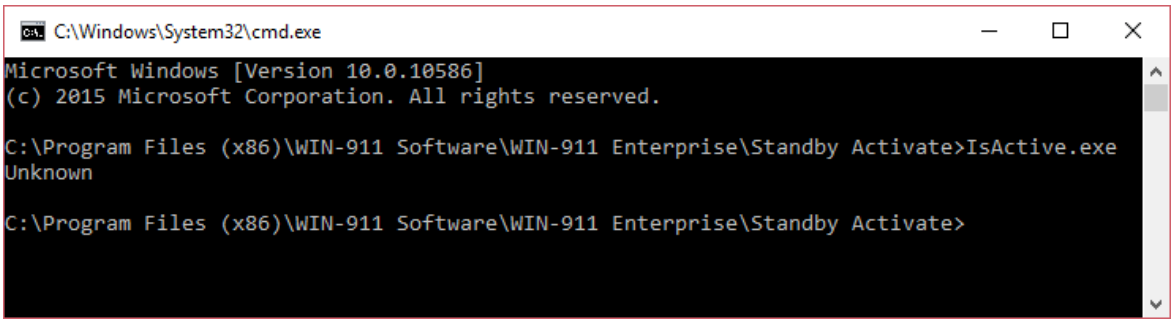
IsActive.exe

Description: This applet attempts to request the current standby status of the targeted WIN-911 Dispatcher.

Success Return Code (Active): 0
Success Console Output (Active): localized string similar to “Active”
Success Return Code (Standby): 1
Success Console Output (Standby): localized string similar to “Standby”



Failure Return Code: -1
Failure Console Output: localized string similar to "Unknown"



Legal Notice

sure to read the release note or README.DOC file before using the product.

TRADEMARKS

WIN-911® and Mobile-911™ are trademarks of WIN-911 Software.

Windows XP®, Server 2003®, Vista®, Server 2008®, Windows 7® , Windows 8®, and Windows Mobile 6® are trademarks of Microsoft Corporation.

Microsoft®, Silverlight®, .NET Framwork®, and MS® are registered trademarks of Microsoft Corporation.

Cepstral® is a registered trademark of Cepstral, LLC

iOS® is a registered trademark of Apple Incorporated

Android® is a registered trademark of Google Incorporated

Blackberry® is a registered trademark of Research In Motion Limited

Dialogic® is a registered trademark of Dialogic Corporation

FactoryTalk® View are registered trademarks of Rockwell Automation, Inc.

Wonderware®, InTouch® and ArchestrA® are trademarks of Wonderware Corporation.

Proficy®, Cimplicity®, Intellution®, Dynamics®, and iFIX® are trademarks of GE.

GoXam™ is a registered trademark of Northwoods Software

Ozeki™ is a registered trademark of Ozeki Informatics Ltd.

CodeMeter™ is a registered trademark of WIBU Systems, AG.