WIN-911 Quick Start

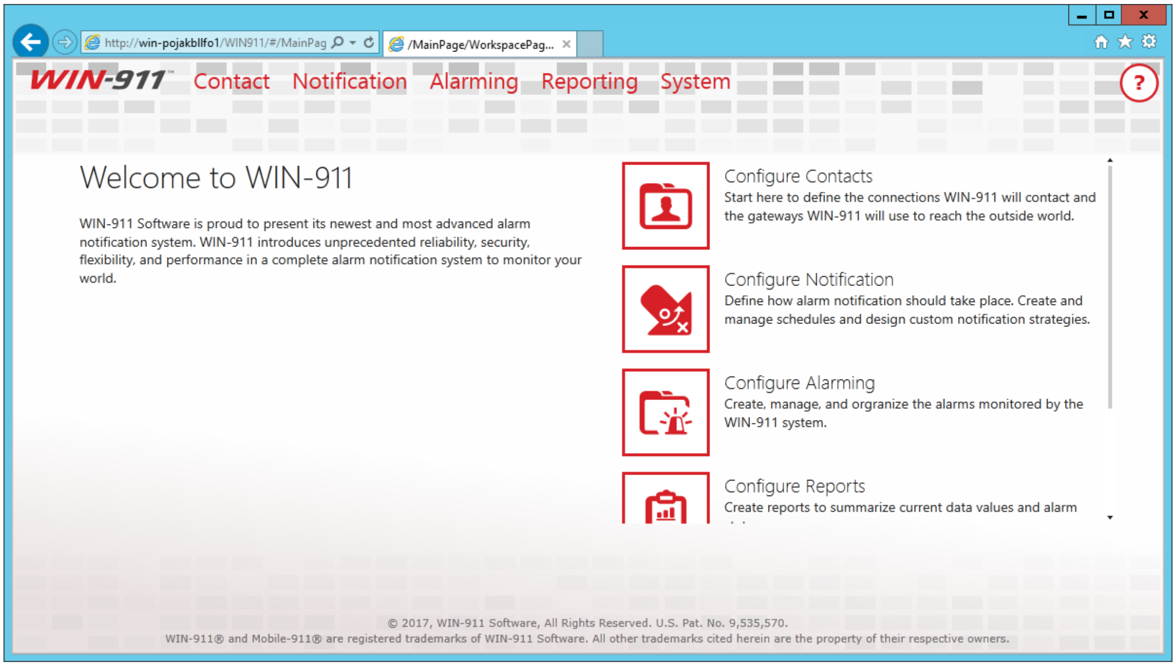
Table of Contents

Getting Started with WIN-911

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

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

Accessing the WIN-911 Configuration


http://win-pojakbllfo1/WIN911/#/MainPag
/MainPage/WorkspacePag...
WIN-911
Contact
Notification
Alarming
Reporting
System
?

Welcome to WIN-911

WIN-911 Software is proud to present its newest and most advanced alarm notification system. WIN-911 introduces unprecedented reliability, security, flexibility, and performance in a complete alarm notification system to monitor your world.

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

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

Configure Alarming
Create, manage, and orgranize the alarms monitored by the WIN-911 system.

Configure Reports
Create reports to summarize current data values and alarm

© 2017, WIN-911 Software, All Rights Reserved. U.S. Pat. No. 9,535,570.
WIN-911® and Mobile-911® are registered trademarks of WIN-911 Software. All other trademarks cited herein are the property of their respective owners.

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

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

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

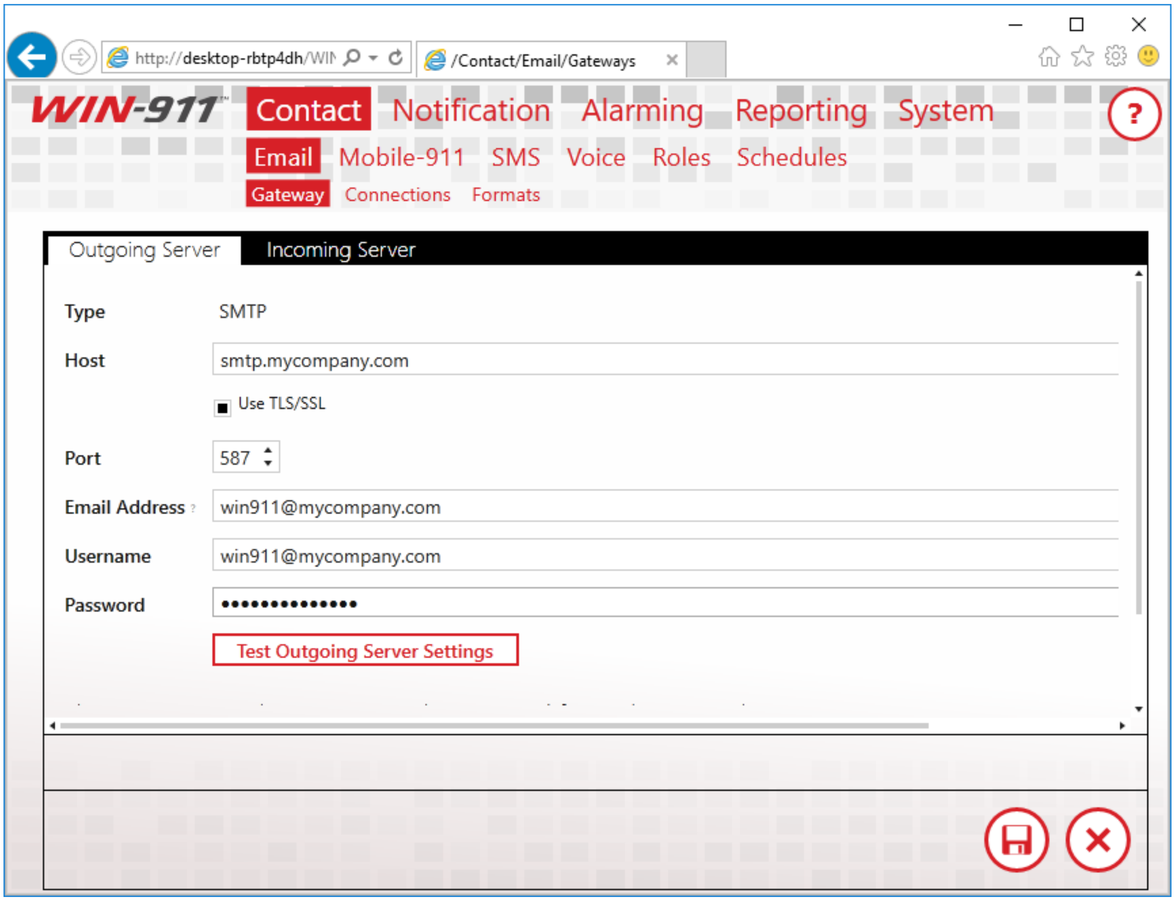
Configure a Notification Method

Gateways

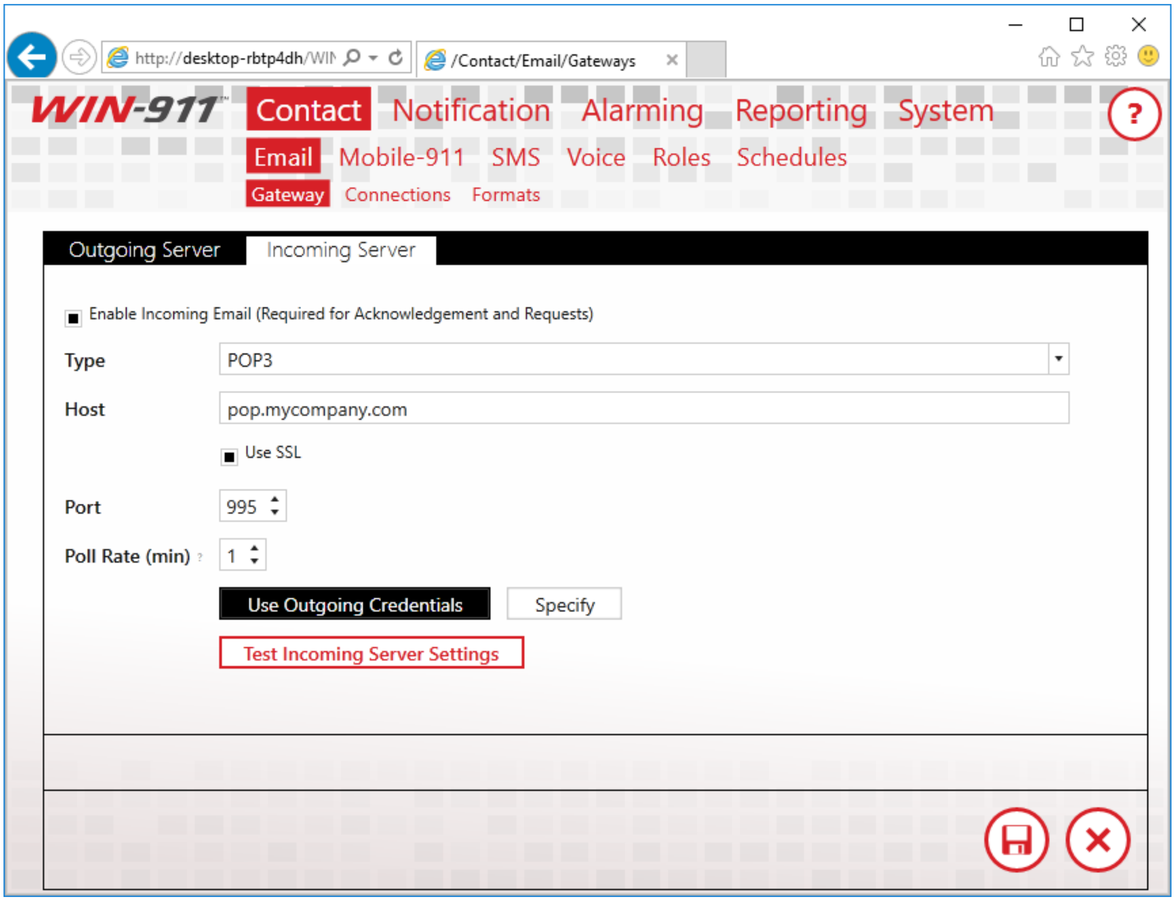
It is considered a best practice to configure any new installation by starting on the notification side of things, so we will begin by configuring our Email Gateway. Every Notifier has a Gateway. The Gateway defines the set of information required by WIN-911 to access the outside world. In the Mobile-911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

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

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



Type	SMTP
Host	smtp.mycompany.com
	■ Use TLS/SSL
Port	587
Email Address	win911@mycompany.com
Username	win911@mycompany.com
Password	••••••••••••••



■ Enable Incoming Email (Required for Acknowledgement and Requests)

Type: POP3

Host: pop.mycompany.com

■ Use SSL

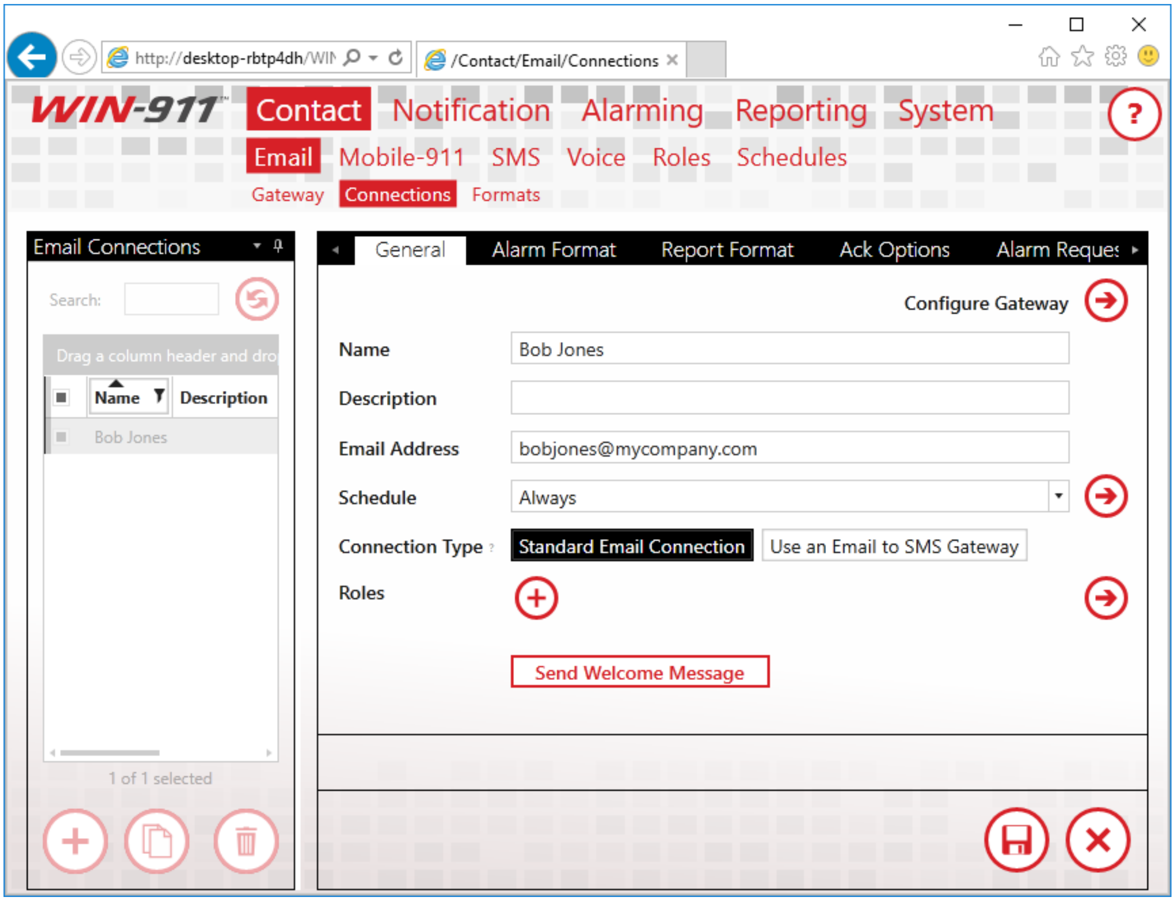
Port: 995

Poll Rate (min): 1

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

Connections

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



Name: Bob Jones

Description:

Email Address: bobjones@mycompany.com

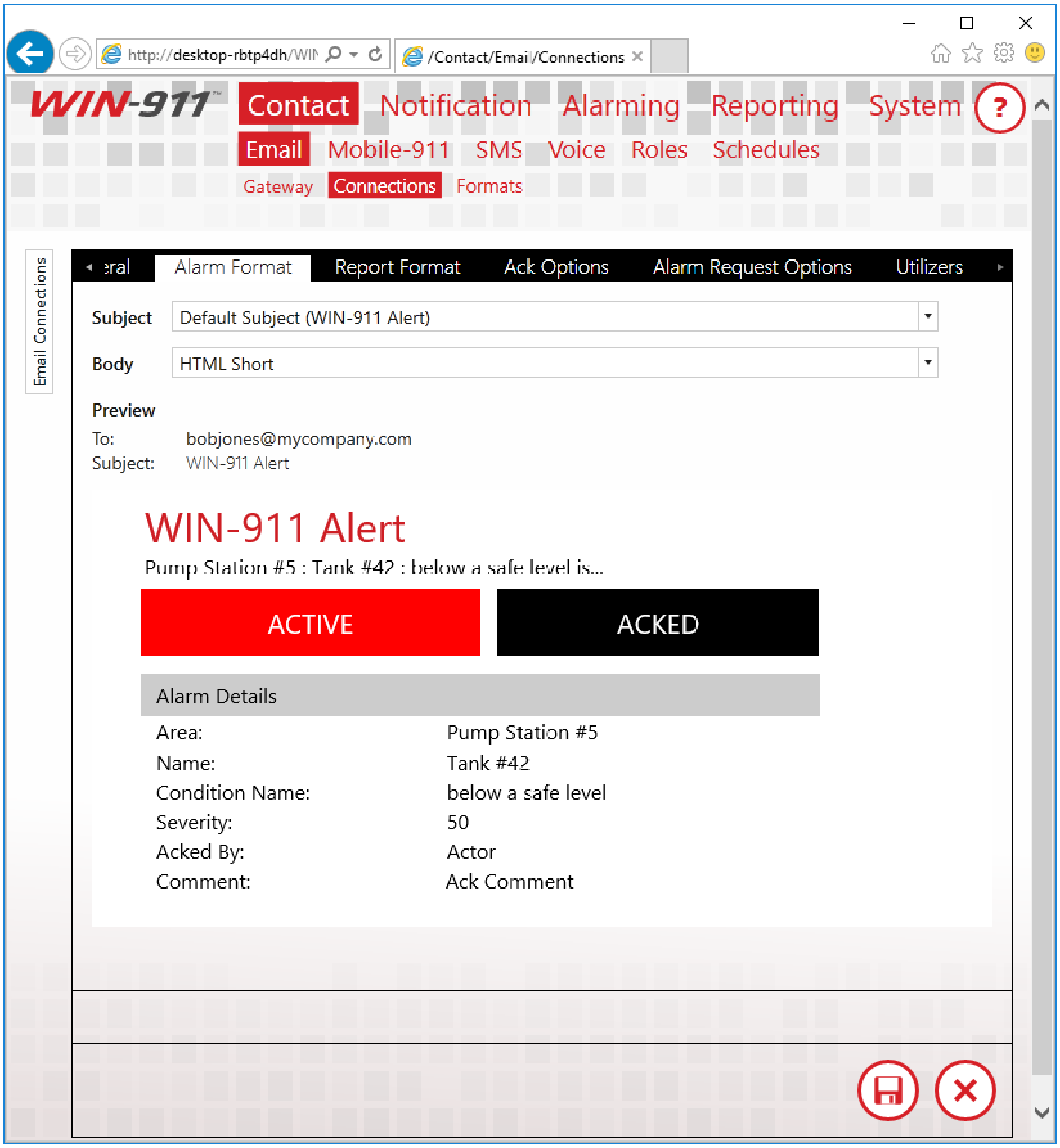
Schedule: Always

Connection Type: [✓ Standard Email Connection] Use an Email to SMS Gateway

Roles:

Enter a unique name for the connection and an email address. Pick a Schedule from the list of default Schedules available to you, or if none of these meet your needs, click the arrow next to the list of Schedules to be taken to a workspace where you may define a new one. Schedules are configured using a calendar control much like any scheduling application. Use the GUI to configure when a connection is on or off duty. When you’re done, use your browser’s back button to finish configuring your connection. You may also attach a Role to a

Connection. Roles are used to organize connections. We'll talk about Roles more when we discuss alarm escalation. There are a few predefined Roles already configured. Use the arrow button to create a new one, if you would like to. An arrow next to any field will take you to a workspace where you may configure that setting. You'll find this pattern repeated throughout the WIN-911 user interface.



Subject: Default Subject (WIN-911 Alert)

Body: HTML Short

Preview

To: bobjones@mycompany.com
Subject: WIN-911 Alert

WIN-911 Alert

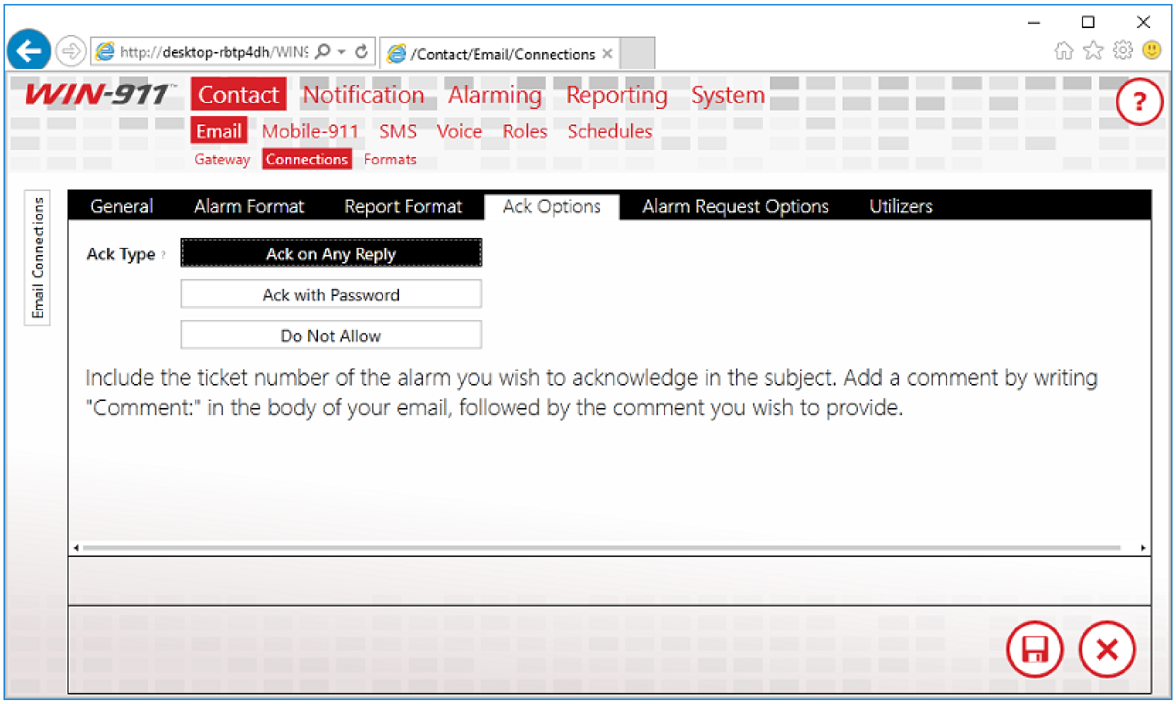
Pump Station #5 : Tank #42 : below a safe level is...

ACTIVE ACKED

Alarm Details

Area:	Pump Station #5
Name:	Tank #42
Condition Name:	below a safe level
Severity:	50
Acked By:	Actor
Comment:	Ack Comment

Select an Alarm Format that best suits your needs. You may format the subject and body in any way you wish. WIN-911's message formats are stored as XSLTs. XSL is a powerful programming language used for transforming XML documents. WIN-911 uses XSLTs to transform alarms into email messages, voice calls, text messages, etc. Editing XSL is quite a complex task and is well outside the scope of this document. For more information on creating XSLTs, consult with W3Schools or contact WIN-911's support department. We'll be glad to help you design a Format that best suits your needs.



Ack Type: Ack on Any Reply

Include the ticket number of the alarm you wish to acknowledge in the subject. Add a comment by writing "Comment:" in the body of your email, followed by the comment you wish to provide.

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

There are a few more settings available for you to configure, but they are not necessary. For the full documentation regarding Email

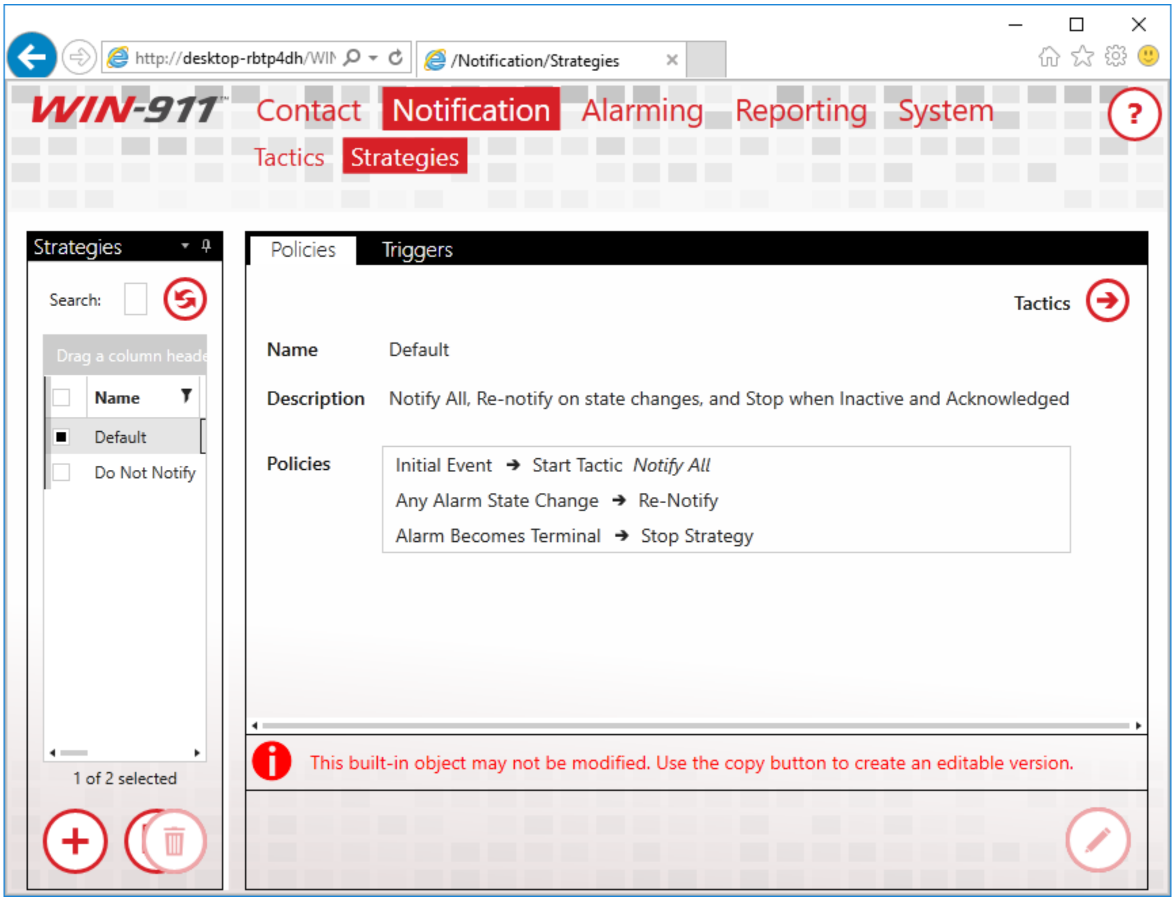
Connections, see the WIN-911 Email manual. Save the Connection and we'll move on to configuring your escalation rules.

Configuring Escalation

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

Strategies

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



Name	Default
Description	Notify All, Re-notify on state changes, and Stop when Inactive and Acknowledged
Policies	Initial Event ➔ Start Tactic *Notify All* Any Alarm State Change ➔ Re-Notify Alarm Becomes Terminal ➔ Stop Strategy

This built-in object may not be modified. Use the copy button to create an editable version.

The Default Strategy will send every alarm to every connection configured in your WIN-911 system and send every update about every alarm to every user who previously received a message about the alarm. It will stop sending messages after the alarm is Terminal. An alarm is considered Terminal when it is inactive and acknowledged. The Strategy only has three rules, formally called Policies, which define this behavior.

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

The first rule means that when the initial alarm is received, WIN-911 should start a Tactic called “Notify All.” The Tactic determines who should actually be notified for an event. The “Notify All” Tactic tells

WIN-911 to notify every connection configured in the system about the alarm. When it does so, it takes into account the Schedule defined for the connection. If the connection is on-duty, the alarm will be sent, if it is off-duty, the connection will be passed over. We'll talk more about Tactics later.

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

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

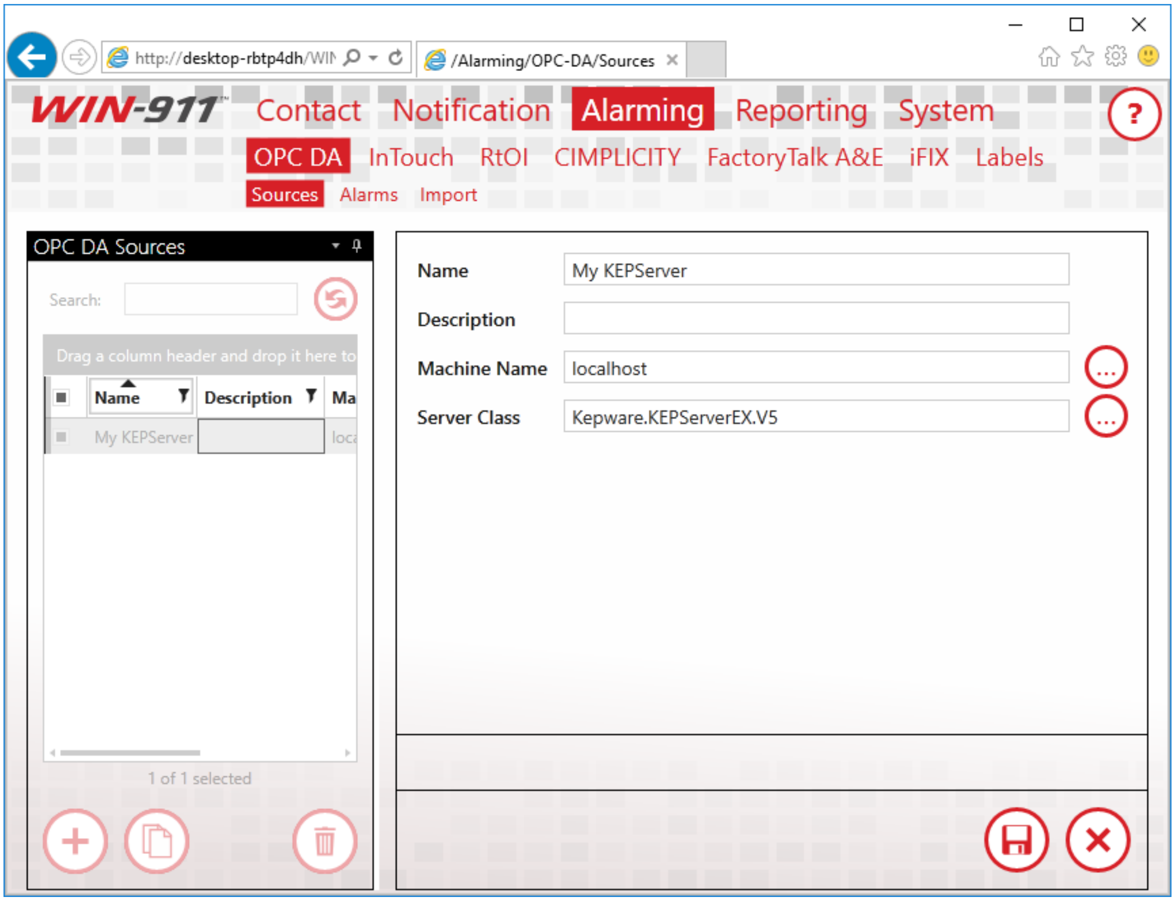
There are two types of Tactics, Basic and Advanced. Basic Tactics are simply a list of connections. When a Basic Tactic is started, everyone on the list is notified. Basic Tactics are easy to configure, and correspondingly, offer less flexibility regarding notification. That said, they meet the majority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

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

Configure Data Sources

Sources

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



Name: My KEPServer

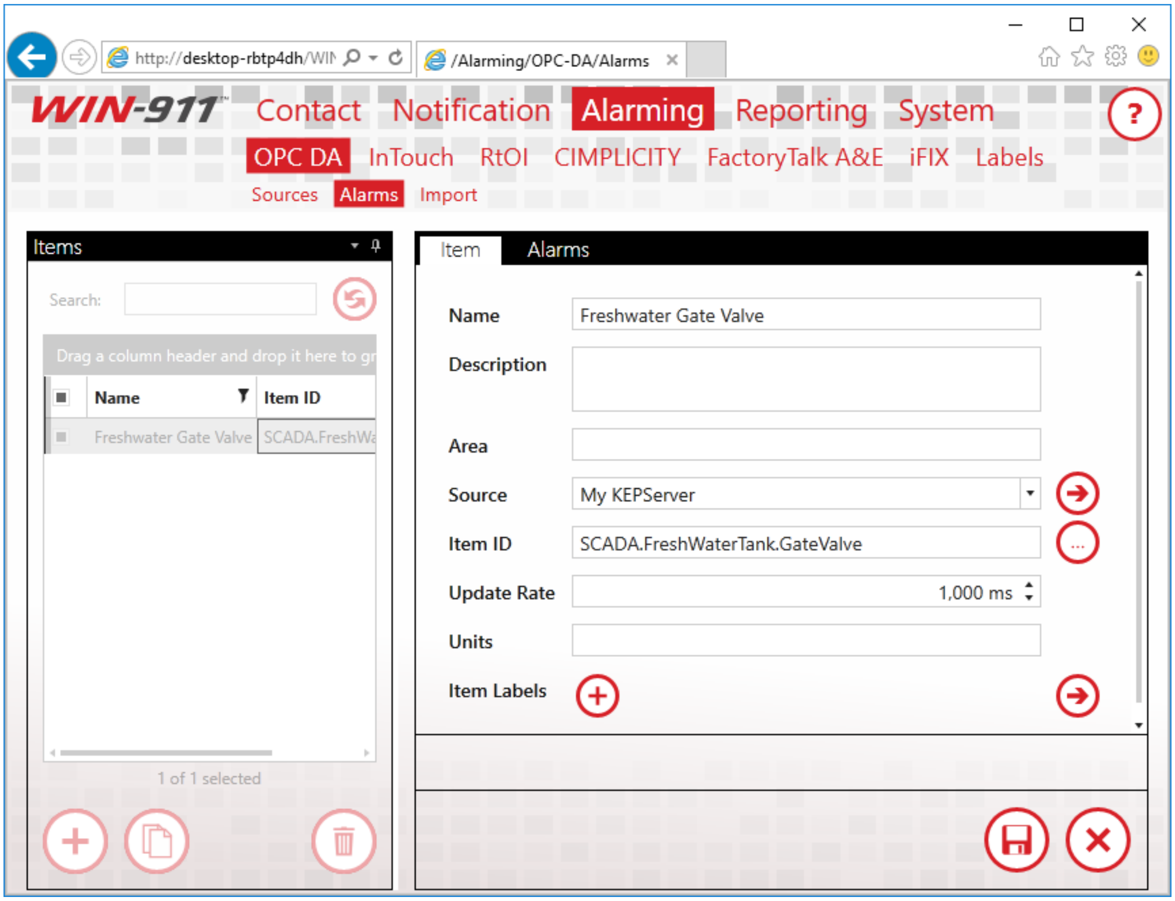
Description:

Machine Name: localhost

Server Class: Kepware.KEPServerEX.V5

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

Alarms



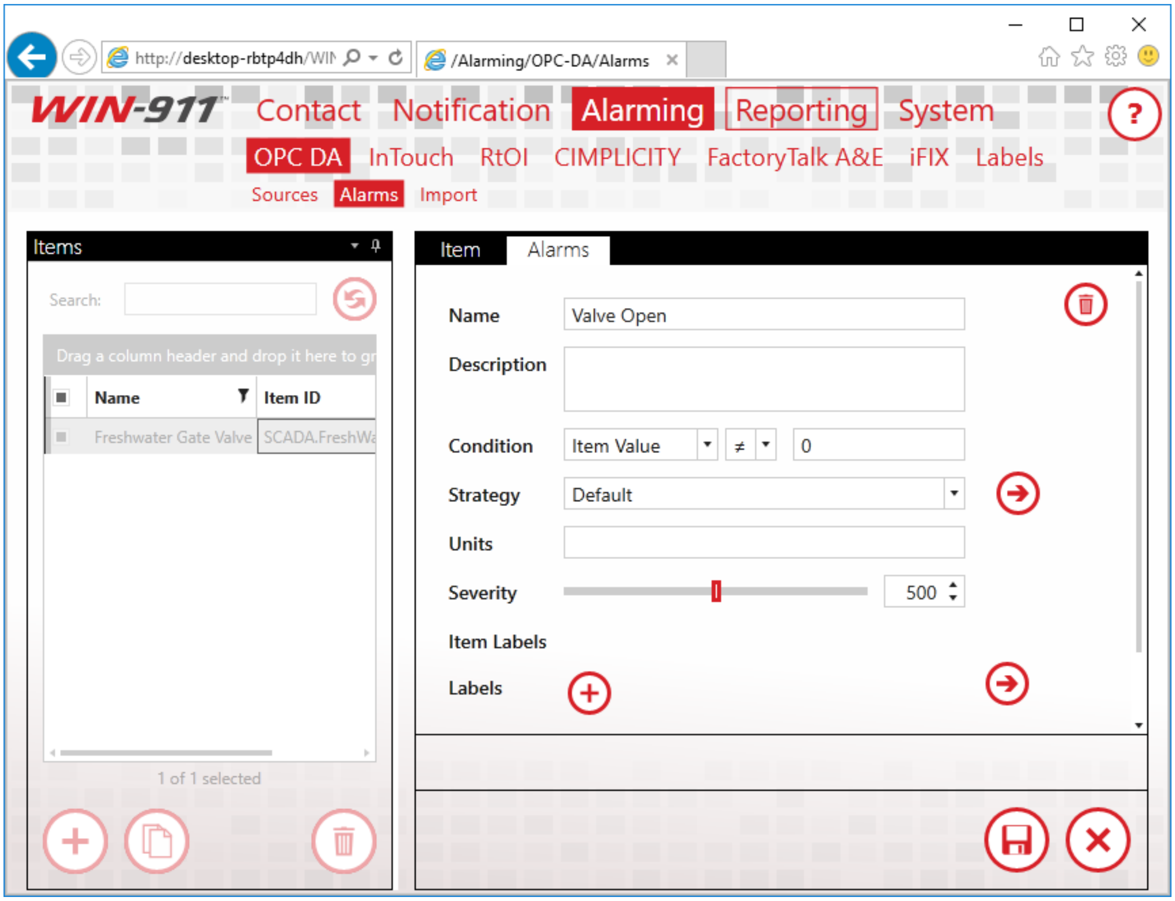
Name	Item ID
Freshwater Gate Valve	SCADA.FreshWa

Name	Freshwater Gate Valve
Description	
Area	
Source	My KEPServer
Item ID	SCADA.FreshWaterTank.GateValve
Update Rate	1,000 ms
Units	
Item Labels	

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

Labels

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



Name	Item ID
Freshwater Gate Valve	SCADA.FreshWa

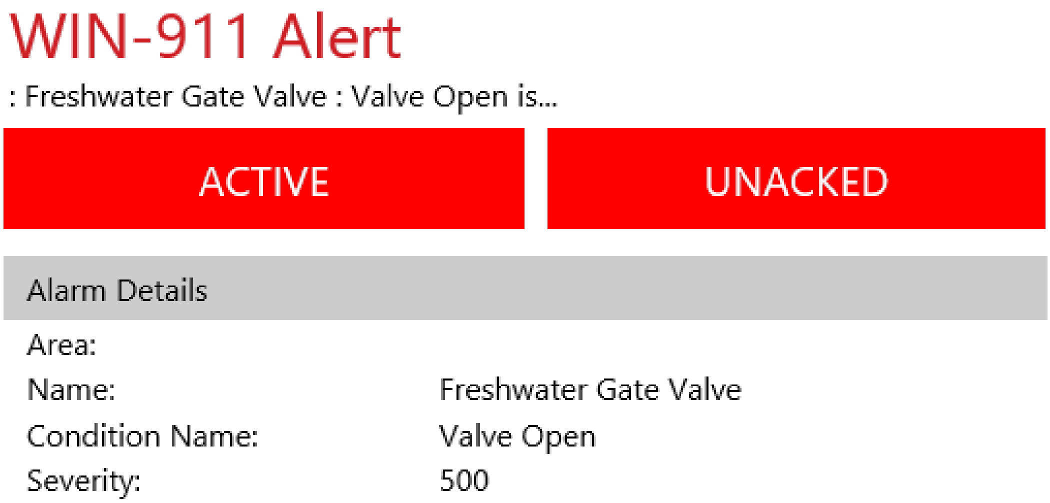
Name: Valve Open
Description:
Condition: Item Value ≠ 0
Strategy: Default
Units:
Severity: 500
Item Labels
Labels

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

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

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

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



WIN-911 Alert

: Freshwater Gate Valve : Valve Open is...

ACTIVE

UNACKED

Alarm Details

Area:	
Name:	Freshwater Gate Valve
Condition Name:	Valve Open
Severity:	500

Congratulations on configuring you first WIN-911 System.

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

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

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

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