



GenWatch3®
Core
Software Version 2.23.5

GenWatch₃

600-2.23.5-A.1
10/31/2023

Trademarks

The following are registered trademarks of Motorola: ATIA, control channel, SmartZone, ASTRO®.

Any other brand or product names are trademarks or registered trademarks of their respective holders.

The Genesis Group Trademark Information

GenWatch3® is a registered trademark of GenCore Candeo, LTD., a subsidiary of Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks.

Copyright

Copyright © 2006-2023; Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks. All rights are reserved. No part of this publication or the associated program may be reproduced, transmitted, transcribed, in whole or in part, in any form or by any means, whether it is mechanical, magnetic, optical, electronic, manual or otherwise, without the prior written consent of Burks GenCore Co., Inc. D.B.A:

The Genesis Group and Phil Burks

5800 Eagles Nest Blvd

Tyler, Texas 75703.

Includes technology licensed from Motorola.

Disclaimer

The GenWatch3 Users' Manual is printed in the U.S.A. Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks believe that the information included in this manual is correct; however, Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks reserves the right to alter, revise and make periodic changes to the manual and its contents. Burks GenCore Co., Inc. D.B.A. The Genesis Group does not assume responsibility to notify any person of such revisions or changes. While we have taken strides to carefully examine our software and documentation and believe that it is reliable, the Genesis Group and Phil Burks assume no responsibility for the use of the manual, or GenWatch3 software, nor for any patent infringements or other rights of third parties who may use the manual or the GenWatch3 software. Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks make no representations or warranties with respect to the contents or fitness for a particular purpose beyond the cost of the software paid by the end-user.

The software contains valuable trade secrets and proprietary information. Unauthorized use of the manual or software can result in civil damages and criminal prosecution. As an end user, you agree to abide by and heed these statements.

License

Title to the media on which the program is recorded and to the documentation in support of the product is transferred to you, but title to the program, and all subsequent copies of the program, despite the form or media in or on license is not a sale of the original or any subsequent copy. You assume responsibility for the selection of the program to achieve your intended results, and for the installation, use, and results obtained from the program.

Refer to the GenWatch3 Manual Overview for your full license. All license information contained on pages 4-7 (book 600-2.23.5-AA.1) are to be considered as contained herein.

Support

Customer satisfaction is our number one priority at Genesis. We are here to provide you with the best software possible, and we want to know when you have any questions, concerns, or problems with GenWatch3 so that we can make it a better product for everyone.

Refer to the *Troubleshooting & Support* section of the GenWatch3 Manual Shell (Book 600-2.23.5-AA.1) for complete support and contact information.

Document History

Revision	Description	Author
2.0.2	Initial Release	JAW
2.0.4	Updated to 2.0.4	JAW
2.0.4	Updated screenshots for new icons and updated login section to reflect new approach	JAW
2.0.4	Updated LaunchPad tools section	KIH
2.0.5	Proofreading/Editing	JWR
2.0.5	Release Revision	TDW
2.0.6	Updated screenshots	REB
2.0.6	Updated screenshots	CLB
2.0.6.6	Release Revision	KIH
2.1.0	Added IP Console Inhibit and Slot Disable Security privileges	REB
2.2	Document Reviewed	WRK
2.3	Revisions Before Release	CWF
2.4	Revisions Before Release	CWF
2.5	Revisions Before Release	CWF
2.5	Add Emergency Display section	KIH
2.5	Added Changing Global Settings section	REB
2.6	Added Security Warning Banner	REB
2.6	Added Change Service Account Password	KIH
2.6	Revisions Before Release	CWF
2.7	Revisions Before Release	CWF
2.8	Revisions Before Release	JAW
2.9	Revisions Before Release	JAW
2.9	Updated “Viewing Real-Time Module Status” section in Chapter 6.	REB
2.10	Revisions Before Release	JAW
2.11	Converted to Docx format	CWF
2.11	Added APM module	JAW
2.11	Added KPI module	BUD
2.12	Revisions Before Release	ATG
2.13	Revisions Before Release	ATG
2.14	Revisions Before Release	JAW
2.15	Revisions Before Release	REB
2.16	Revisions Before Release	JPS
2.16	Added two security privileges to Halcyon: GPS Location Requests and IMW Location Requests.	REB
2.17	Remove ChangeMe workflow from Halcyon	DW
2.17.7	Added Special Information to emergency window.	REB
2.17.12	Added CSV export of current users and activity Update hyperlinks	DW

2.17.17	Added ViewAllSites privilege in Alias.	REB
2.23.1	Added DynamicallyAddDefaultIpPlan config file setting.	REB

Table of Contents

<i>Trademarks</i>	3
<i>The Genesis Group Trademark Information</i>	3
<i>Copyright</i>	3
<i>Disclaimer</i>	3
<i>License</i>	3
<i>Support</i>	3
DOCUMENT HISTORY	4
TABLE OF CONTENTS	7
ABOUT THIS MANUAL	11
GOALS	11
WHO SHOULD READ THIS MANUAL?	11
HOW THIS MANUAL IS ORGANIZED	11
CHAPTER 1 INSTALLATION	13
INSTALLATION INFORMATION	13
CHAPTER 2 OVERVIEW	15
TERMS	15
WELCOME	15
WHAT IS GENWATCH3?	15
<i>Core Applications and Modules</i>	16
<i>Input and/or Output Modules</i>	16
<i>Process and/or Display Modules</i>	17
<i>Reporting Modules</i>	18
<i>Tools</i>	18
GENWATCH3 AND WINDOWS SECURITY	19
<i>Basic Input and Output</i>	19
<i>TCP/IP Communication</i>	19
CHAPTER 3 GENWATCH3 SERVICE	21
WINDOWS SERVICES	21
<i>Why is GenWatch3 a Service?</i>	21
<i>Administering Windows Services</i>	21
<i>Delayed Start option</i>	22
<i>Changing the GenWatch3 Service Account password</i>	23
GENWATCH3 SERVICE OVERVIEW	26
<i>GenWatch3 Service Diagnostics</i>	26
<i>Module Health</i>	27
GENWATCH3 CONFIG FILES.....	27
<i>Service Config Files</i>	27
<i>GUI Config Files</i>	29
<i>Updating a Config File</i>	30
DATABASE SIZE NOTIFICATIONS	32
STAGING FOR WINDOWS AUTHENTICATION	32
<i>Domains</i>	32
<i>Workgroups</i>	33
CHAPTER 4 GENWATCH3 MODULE GUIS OVERVIEW	35
WHAT ARE MODULE GUIs?	35
COMMON MODULE GUI BUTTONS	35

MODULE CONNECTION DISPLAYS AND FUNCTIONS.....	36
<i>Default Module Ports.....</i>	36
<i>Changing a Module's Default Port.....</i>	37
DATABASE INCOMPATIBILITY WARNINGS.....	37
MODULE HELP	37
CHAPTER 5 GW_ALERTS	39
WHAT IS GW_ALERTS?	39
LOGGING INTO GW_ALERTS.....	40
PASSWORD EXPIRATION	41
GW_ALERTS MENU.....	42
GW_ALERTS CONNECTION ICONS	42
GW_ALERTS NOTIFICATION WINDOWS	43
GW_ALERTS EMERGENCY DISPLAY	43
<i>Removing emergency messages</i>	44
CHAPTER 6 GW_LAUNCHPAD GUI	45
VIEWING REAL-TIME MODULE STATUS.....	46
<i>Modules List Menu.....</i>	46
CREATING MODULE NOTES	46
LOADING GUIS	47
LOAD THE GENWATCH3 LICENSE MANAGER.....	47
CREATING SHORTCUTS TO USEFUL TOOLS	47
SETTING UP A TEMPORARY FILTER FOR REAL-TIME ACTIVITY MODULES.....	48
CHANGING GLOBAL SETTINGS	49
CHAPTER 7 GENWATCH3 LICENSE MANAGER.....	51
DO I NEED TO ACTIVATE MY LICENSE?	51
WHAT IS THE GENWATCH3 LICENSE?.....	51
LOADING GENWATCH3 LICENSE VIEWER.....	52
LICENSE DETAILS	52
LICENSE MANAGER OPTIONS	53
<i>Activate Product(s)</i>	53
<i>Refresh License</i>	54
<i>Deactivate License</i>	54
CHAPTER 8 GW_SECURITY MODULE GUI	57
WHAT IS GW_SECURITY?	57
PRIVILEGES	58
<i>Privileges List</i>	58
SECURITY FOR WINDOWS AUTHENTICATION	64
ROLES	65
<i>Adding a New Role.....</i>	65
<i>Editing a Role</i>	66
<i>Deleting a Role</i>	66
USERS.....	66
<i>The Administrator Role and Admin User.....</i>	67
<i>Adding a New User</i>	67
<i>Editing a User.....</i>	68
<i>Changing a User's Password</i>	69
<i>Deleting a User.....</i>	70
<i>User Filters</i>	70
Adding Resources	70
Removing Resources.....	71
<i>Editing the Security Warning Banner</i>	71
ACTIVITY HISTORY	72

<i>Login History Snapshot</i>	74
CURRENT USERS	74
<i>Logging Out a User</i>	75
CHAPTER 9 GW_SYSLOG GUI	77
WHAT IS GW_SYSLOG?.....	77
SYSLOG PACKETS	78
<i>SysLog PRI Facility Values</i>	78
<i>SysLog PRI Severity Values</i>	79
SYSLOG CONNECTIONS	79
<i>Creating a SysLog Connection</i>	79
<i>Deleting a SysLog Connection</i>	80
<i>Disabling a SysLog Connection</i>	80
CHAPTER 10 GW_WEBSERVER MODULE	81
WHAT IS GW_WEBSERVER?.....	81
WEB SERVER CONFIGURATION	81
WEB SERVER REQUEST TYPES	82
CHAPTER 11 GENWATCH3 NOTIFICATIONS	83
WHAT IS A NOTIFICATION?.....	83
WHAT DO NOTIFICATIONS MEAN TO ME?	84
WORKING WITH NOTIFICATIONS	84
CHAPTER 12 AUTOMATIC PURGING	85
WHAT IS AUTOMATIC PURGING?.....	85
AUTOMATIC PURGE SETTINGS.....	85
VIEWING PURGING RESULTS	86

Goals

This document informs and instructs users on the operation of the core Graphical User Interfaces (GUIs) and modules for GenWatch3.

Who Should Read This Manual?

This manual was written for an audience of Motorola trunked radio system administrators with novice to mid-level computer experience.

How This Manual Is Organized

This manual is organized into the following chapters:

- **Installation:** Provides a list of reference documents for hardware and software installation.
- **Overview:** Gives an overview of the GenWatch3 solution.
- **GenWatch3 Service:** Describes the function and role of the GenWatch3 service in the GenWatch3 solution.
- **GenWatch3 Module GUIs Overview:** Describes the common functions of each GenWatch3 module GUI.
- **GW_Alerts:** Describes the function and role of the GW_Alerts System Tray application.
- **GW_LaunchPad GUI:** Describes the function and role of the GW_LaunchPad GUI.
- **GenWatch3 License Manager:** Describes the function and role of the GenWatch3 License Manager.
- **GW_Security GUI:** Describes the function and role of the GW_Security GUI.
- **GW_SysLog GUI:** Describes the function and role of the GW_SysLog GUI.
- **GW_WebServer:** Describes the function and role of the GW_WebServer module.
- **GenWatch3 Notifications:** Describes the GenWatch3 GUI Notification window shown by GW_Alert
- **Automatic Purging:** Describes the need and function of the automatic purging operation within GenWatch3.

This manual contains the following images, used to indicate that a segment of text requires special attention:



Additional Information: Additional information is used to indicate shortcuts or tips.



Warning: Warnings are used to indicate possible problem areas, such as a risk of data loss or incorrect/unexpected functionality.

This chapter contains the following sections:

- **Installation Information:** Describes where to find installation information.

Installation Information

For installation instructions and minimum hardware requirements, see the *GenWatch3 Installation and Quickstart Guide*.

For hardware installation instructions, refer to the *Hardware Installation Guide*.



The GenWatch3 machine must use an English-language version of Microsoft Windows using the English language set.

This chapter contains the following sections:

- **Terms:** An introduction of basic terms used in this manual.
- **Welcome:** Welcomes you to the Genesis GenWatch3 product.
- **What is GenWatch3?:** Defines the GenWatch3 product.
- **GenWatch3 and Windows Security:** Describes the Microsoft Windows security needs of GenWatch3.

Terms

- **Packet:** This is a message sent from a data source to GenWatch3 or a message sent from GenWatch3 to a data destination.
- **Module:** This is a part of the GenWatch3 solution. Each module performs a specific function within GenWatch3. For example, the GW_Group module organizes and shows real-time Push-to-Talk activity, while the GW_RSP25 module manages connections to P25 devices.
- **Windows Service:** A Windows service is an application that runs behind the scenes. Services automatically load when the computer boots up.
- **Port:** A data connection in a computer that allows local and/or remote access.

Welcome

Thank you for allowing Genesis to help you with your software needs. Genesis has combined our technology for decoding data streams (such as P25 control channels, ATIA [*Air Traffic Information Access*] feeds and other proprietary interfaces), the power of Microsoft .Net development, and our expertise in software design and implementation into a single, scalable application.

What is GenWatch3?

GenWatch3 is a dynamic data process solution. This means that GenWatch3 can accept and decode proprietary packet interfaces and encode, display, archive, relay, and respond to these packets. Because of its design, GenWatch3 modules can satisfy almost any data process need.

The GenWatch3 GUIs and modules are divided into the following categories:

- Core
- Input and/or output
- Process and/or display
- Reporting

The core modules are shown in Table 2.1 below. Each additional module is defined within its own respective GenWatch3 module book.

Core Applications and Modules

The following core GUIs and modules are those required for minimum GenWatch3 setup and functionality.

Module Name	Description	Document
GenWatch3 Service	Windows service that loads and runs all licensed GenWatch3 modules.	600-2.23.5-A.1 [this document]
GW_Alerts	Shows the status of GenWatch3 input connections. Shows notifications sent by GenWatch3, via Notification windows. Provides an entry point for GW_LaunchPad. This GUI is also where you log in to GenWatch3.	600-2.23.5-A.1 [this document]
GW_LaunchPad	Provides a single interface to load each module GUI and each tool provided by GenWatch3.	600-2.23.5-A.1 [this document]
GW_Security	Centralized security GUI/module for GenWatch3. The users, roles, and privileges defined in this module affect the display and function of each module's GUI within GenWatch3.	600-2.23.5-A.1 [this document]
GW_SysLog	Reports GenWatch3 service and module activity to one or more remote IP ports via SysLog packets. These packets can be received and parsed by third-party SysLog client software.	600-2.23.5-A.1 [this document]
GW_WebServer	Handles incoming GenWatch3 web requests and their responses.	600-2.23.5-A.1 [this document]

Table 2.1 – Core Applications and Modules

Input and/or Output Modules

The input and/or output modules accept input from and/or provide output to a specific data stream. The following input and/or output modules are currently available for this version of GenWatch3.

Module Name	Description	Document
GW_ATIA	Receives data from a RFSS (Zone) Controller ATIA Port or a GenGET v7.0+ Data Reader / Data Processor attached to the ATIA port of a SmartZone or Dimetra system.	600-2.23.5-D.1
GW_RSP25	Receives data from a P25 radio that can deliver the Common Air Interface to a digital output. GW_RSP25 currently supports Millennium.	600-2.23.5-EE.1
GW_Location	Receives GPS, telemetry, event and sensor information from a GPS solution. GW_Location currently supports the ASTRO 25 outdoor locator protocol.	600-2.23.5-KK.1

Module Name	Description	Document
GW_Connect	Receives SNMP, APM, HPD, CADI, PMI, UCS, and IMW data from hardware and software on your network.	600-2.23.5-MM.1

Table 2.2 – Input and/or Output Modules

Process and/or Display Modules

Process and/or display modules perform specific functions on the packets generated by the input modules (GenWatch3 input). Some of these modules provide user interfaces, which result in commands sent out to a data stream connected to the input and/or output modules (GenWatch3 output). In addition to the core modules, the following process and/or display modules can be licensed for this version of GenWatch3:

Module Name	Description	Document
GW_Activity	Displays all activity received over the data stream in real time. This data includes system events such as Base Station Identifications, System Status, etc. This GUI also includes call activity such as dispatch/group and private calls. Each packet type can be excluded or included via the options at the top of the GUI.	600-2.23.5-E.1
GW_Affiliation	Shows real-time unit-to-group affiliations and unit-to-site registrations, where each group is represented by individual, customizable windows.	600-2.23.5-F.1
GW_Alias	Accepts input packets, dynamically adds new resources as they appear on the data stream, appends alias information to input packets and passes each appended packet onto the other modules.	600-2.23.5-G.1
GW_APM	Shows APM channel status information in site and subsite windows.	600-2.23.5.0.TT.1
GW_Archiver	Archives information received over the data stream into the database. Can optionally archive everything from system status to call activity. This archived data feeds the GenWatch3 reports.	600-2.23.5-H.1
GW_Channel	Shows real-time channel usage as well as busies, rejects, and diagnostics received over the data stream.	600-2.23.5-I.1
GW_GENsAC	Converts input packets into defined output packets. These packets are built, filtered, and sent to consoles.	600-2.23.5-Z.1
GW_GenSPOut	Converts input packets into defined output packets. These packets are built, filtered, and sent based on interfaces and connection definitions created within GW_GenSPOut.	600-2.23.5-K.1

Module Name	Description	Document
GW_Group	Shows real-time PTT/call activity in individual, customizable group windows.	600-2.23.5-L.1
GW_Halcyon	Manages radio commands and their corresponding ACKs. Accepts GW_RCM and CADI connections (Motorola SIMSII and RPC), processes requests from the connections, and passes qualified system events to these connections. Works with GW_SAM to allow it to issue radio commands.	600-2.23.5-T.1
GW_KPI	Displays real-time, interactive and statistical information on WACNs, systems, RFSSs and sites.	600-2.23.5-UU.1
GW_SAM	Monitors predefined ranges of groups and radio IDs for usage outside predefined patterns. Also watches for overlapping calls and impossible drive distance usage (multi-site or location supplemented only) that could be cloned radio activity.	600-2.23.5-J.1
GW_System Summary	Shows real-time graphical system usage for trunked radio systems.	600-2.23.5-N.1
GW_SysVista	Shows real-time graphical dash-board system usage statistics for trunked radio systems.	600-2.23.5-O.1
GW_Trigger	Monitors GenWatch3 packets for predefined patterns that result in external relay, email, SNMP, red/amber/green light or audio-visual alerts.	600-2.23.5-S.1
GW_Trio	Manages customer billing by compiling individual usage statistics into billing information.	600-2.23.5-NN.1

Table 2.3 – Process and/or Display Modules

Reporting Modules

Reporting modules display information recorded in the GenWatch3 database. The following reporting modules can be licensed for this version of GenWatch3:

Module Name	Description	Document
GW_Reports	Provides an interface to launch the canned reports offered in GenWatch3.	600-2.23.5-Y.1

Table 2.4 – Reporting Modules

Tools

The following applications are available in the Tools section of GW_LaunchPad. Tools provide supplemental setup or functionality within GenWatch3. See *Chapter 6 – GW_LaunchPad GUI* of this book for more information on

GW_LaunchPad tools. The following tools can be licensed for this version of GenWatch3:

Tool Name	Description	Document
GW_RCM	Loads the GW_RCM application. GW_RCM allows you to issue radio commands such as inhibit and call alert. This GW_RCM also provides a workflow for radio events such as emergency alarms, statuses, etc. (requires Motorola RPC CADI and GW_Connect RPC CADI capable license.)	600-2.23.5-V.1

Table 2.5 – Tools

GenWatch3 and Windows Security

Basic Input and Output

The GenWatch3 GUIs use the security context of the currently logged-in Windows user to access TCP/IP ports, read from files, write to files and many other functions. Some Windows installs may limit these functions.

For simple installs, the best way to ensure that your Windows user can perform these functions is to log into Windows using the Administrator user or a user with full administrative access to the machine. Simple installs include only machines that are not part of a domain.

For installs that include computers on a domain, you might need to set up some security options on the domain controller for your user and/or the GenWatch3 machine. When in doubt, check with your IT department, or contact GenWatch3 support.

The GenWatch3 Host installation includes a windows service named *GenWatchService*. The GenWatch3 service is designed to run under the built-in Windows account **LOCAL SYSTEM**. If you choose to run GenWatch3 under another user, you must ensure that this Windows user has the following privileges:

- Read/write access to databases in SQL Server.
- Read/write access on this machine to the *Application Data* directory. By default, this directory is *C:\ProgramData\Genesis\GenWatch3*.
- Authorization to open TCP/IP connections on this machine.
- If your install includes one or more client machines, authorization to create/receive TCP/IP connections to and from this machine.

TCP/IP Communication

When a GenWatch3 GUI connects to a module, the following occurs:

1. The GUI presents its Windows user as a security principle to the module. If the user is valid on the network, the process continues. (see the SuperListener_Authenticate event in the GenWatch3 event log).
2. The GUI and module PCs negotiate the type of encryption to be used based on the *Authentication Type* presented by the security principle in step 1. This is typically NTLM or Kerberos.
3. The GUI requests TCP/IP packet compression to be on or off based on the option selected during the GenWatch3 client install. If enabled, all packets over 1024 bytes will be compressed before they are sent over the network.

See the ***GenWatch3 Config Files*** section of this document for more information on viewing and changing the encryption and compression options.

This chapter contains the following sections:

- **Windows Services:** Defines Windows services and gives an overview of their function.
- **GenWatch3 Service Overview:** Defines the GenWatch3 service.
- **GenWatch3 Config Files:** Describes the options contained within the GenWatch3 configuration files.
- **Database Size Notifications:** Describes the messages sent by GenWatch3 to inform the user when the database is nearing its size limit.

Windows Services

A service is an application that runs in the background. If a service is set to 'Automatic', the service will start when the machine is booted and, in most cases, will load by the time Windows presents its login window. If it is not loaded in time, a simple error message will display.

Why is GenWatch3 a Service?

GenWatch3 must always be running so that it can archive and process activity on your system. Windows services do not require user interaction to load, so they will run even if the host PC is rebooted in the middle of the night.

Administering Windows Services

Services are administered via the Windows Computer Management application. To access this application:

1. Right-click on the **My Computer** icon on your desktop. This will result in a menu of options, including the **Manage...** option.
2. Click on the **Manage...** option in the menu. This will load the Computer Management application.
3. Expand the **Services and Applications** node in the tree on the left of the window.
4. Click on the **Services** node: This will show a list of all services registered on your PC in a list on the right of the window.
5. Find the GenWatch3 service in the list (it is named **GenWatchService**).

At this point you can right-click on the service to receive a list of service options. These options include:

- **Start** – Starts the service (Only available if the service is stopped)
- **Stop** – Stops the service (Only available if it is started)
- **Pause** - Pauses the service (Only available if it is started)
- **Resume** - Starts the service (Only available if it is paused)
- **Restart** – Stops the service, then starts the service (Only available if it is started)
- **Properties** – Displays the details about the selected service

Delayed Start option

Computers with minimal amounts of processing power may have difficulty starting all their services when they boot. This can affect the GenWatch3 service because it requires other services to be running when it starts. You may find messages in the Event Log stating, “The service did not respond to the start or control request in a timely fashion.” In this situation, setting the Startup type of the GenWatch3 service to Delayed Start can help.

This will delay the service’s startup when the computer reboots and allow other services to start first.

To change the setting, follow the instructions listed above in the **Administering Windows Services** section to access the service properties. Change the **Startup type** option on the **General** tab and click **OK**.

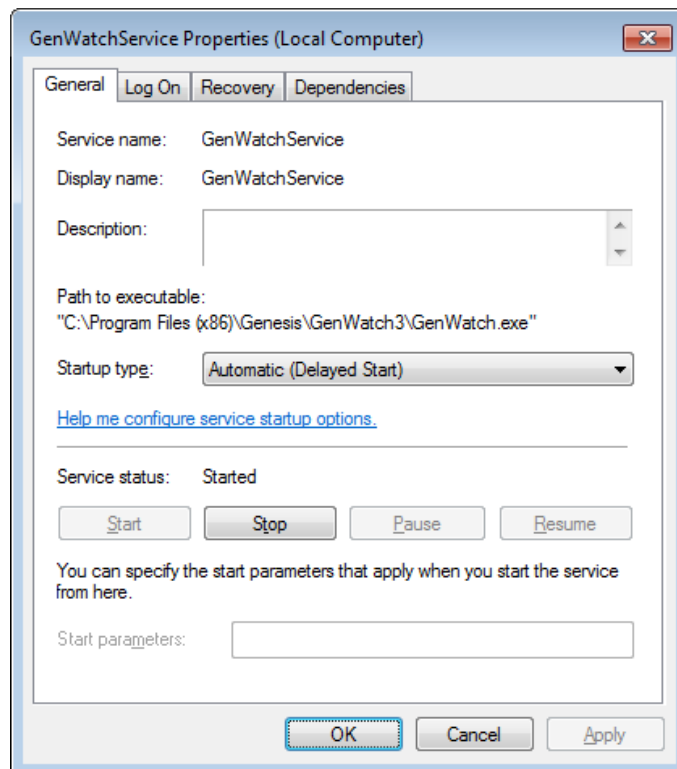


Figure 3.1 – GenWatch3 service configured for Delayed Start

Changing the GenWatch3 Service Account password

1. Close all GenWatch3 clients connected to the GenWatch3 host.
 - a. Each GenWatch3 client must close all modules and exit GW_Alert.
 - b. Verify from the GenWatch3 host that all clients have logged off using the **Current Users** list in the GW_Security GUI. Figure 3.2 shows that only the Admin account is logged in.
 - c. Close all modules on the host machine and exit GW_Alert.

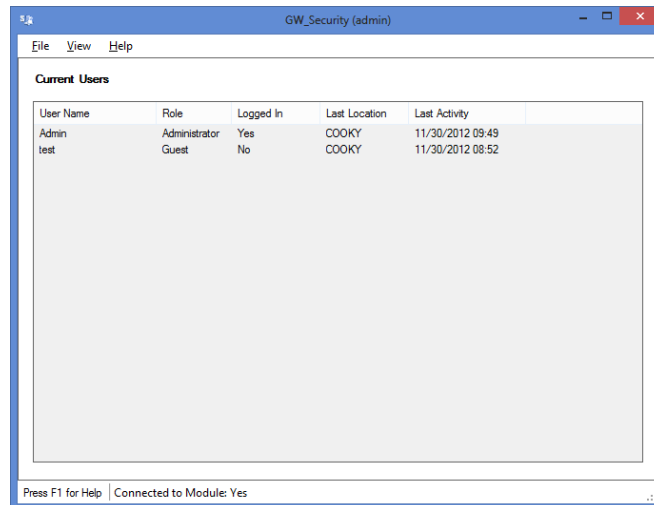


Figure 3.2 – Current Users List

2. Stop **GenWatchService**.
 - a. Right-click **My Computer** and select **Manage**.
 - b. Select **Services** then select the **GenWatchService**.
 - c. Click the **Stop** button. (Figure 3.3, Leave this window open)

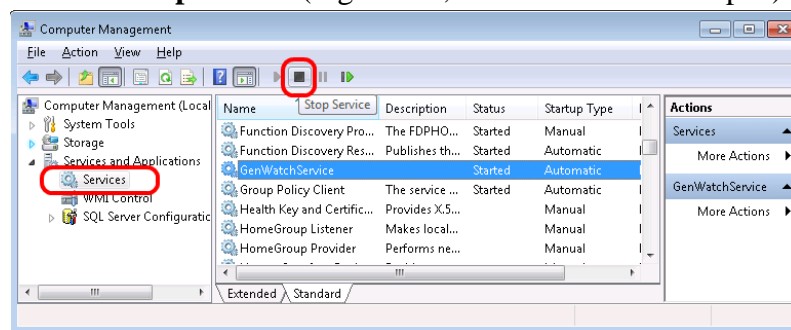


Figure 3.3 – Computer Management → Services

3. Change the password for the account.
 - a. Open the **Control Panel** and select **User Accounts**.
 - b. Click **User Accounts** and **Manage User Accounts**.
 - c. Go to the **Advanced** tab and click **Advanced** (Figure 3.4).

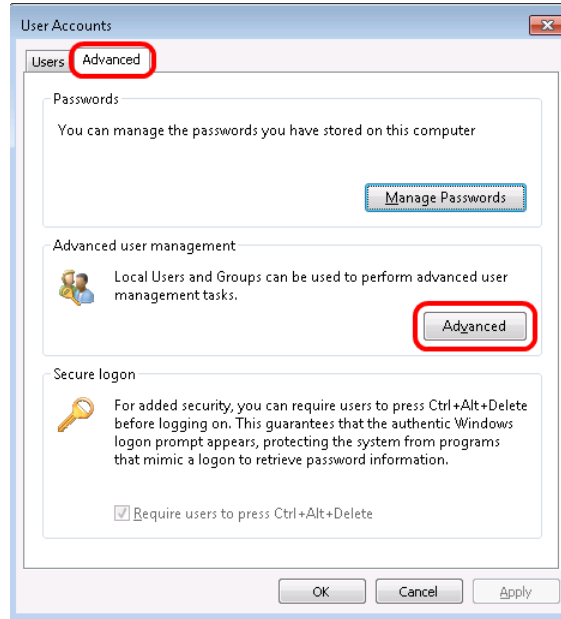


Figure 3.4 – User Accounts – Advanced tab

- d. Select **Users** and then right-click the account used by the GenWatchService and select **SetPassword...** (Figure 3.5).

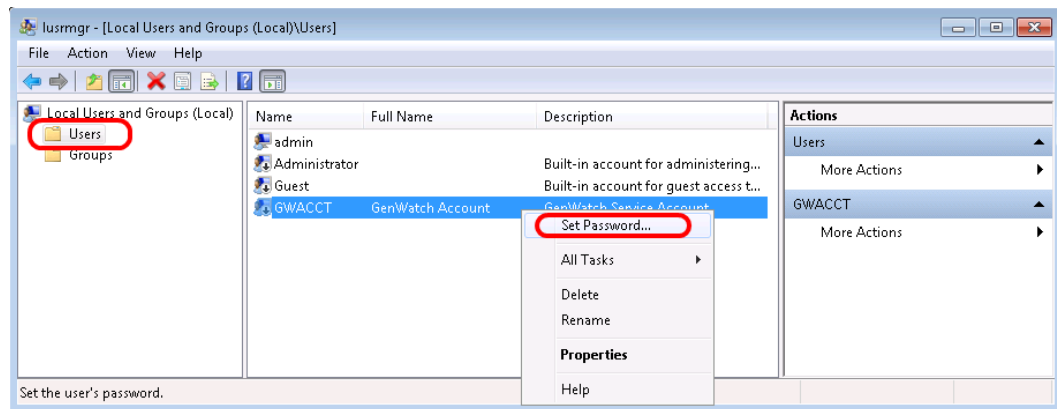


Figure 3.5 – Local Users and Groups

- e. Enter the new password in the **New password** and **Confirm password** fields. (Figure 3.6)



Figure 3.6 – Set Password

4. Update the logon credentials with the new password.
 - a. Within the Computer Management window, right-click **GenWatchService** and select **Properties** then go to the **Log On** tab.
 - b. Type the new password in the **Password** and **Confirm password** fields. (Figure 3.7)

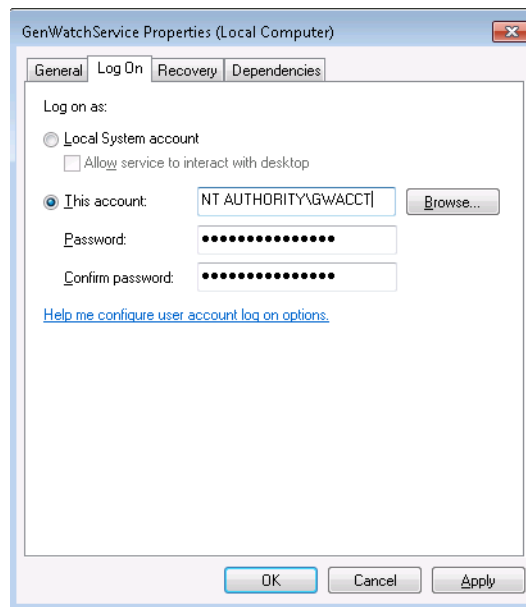


Figure 3.7 – Update the Account credentials

5. Start the **GenWatchService**.
 - a. Within Computer Management, select the **GenWatchService**.
 - b. Click the **Play Button**. (Figure 3.8)

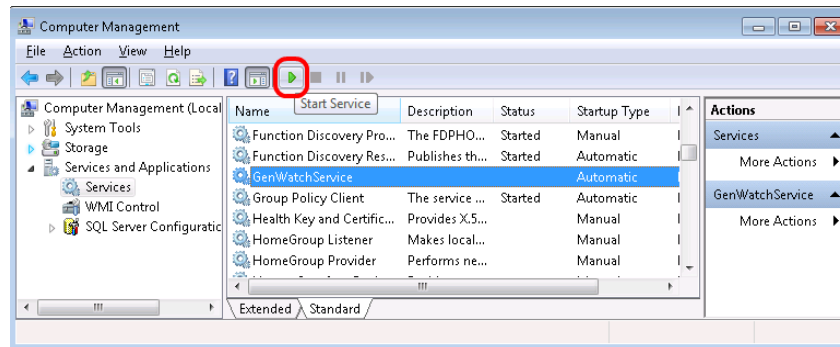


Figure 3.8 – Starting the GenWatchService

6. Login to the GenWatch3 host and ensure the service is running properly
7. Inform GenWatch3 clients that they may now launch GW_Alert and connect to the host machine.

GenWatch3 Service Overview

When the GenWatch3 service is started, it loads all the GenWatch3 modules that are included in your GenWatch3 license. The service then starts all these loaded modules. Once started, these modules begin to perform their specific tasks. These tasks may include anything from receiving and parsing a data stream to archiving the parsed data stream to an SQL database.



If the GenWatch3 service is stopped, it will unload all modules. The modules will not process data until the service is restarted.

GenWatch3 Service Diagnostics

The GenWatch3 service reports activity to the Windows Event Log. You can access the Windows event log by taking the following steps:

1. Right-click on the **My Computer** icon.
2. Select **Manage...**
3. Expand the **Event Viewer** node under the **System Tools** node.
4. Expand the **Applications and Services Logs** node.
5. Click on the **GenWatch** node under the **Event Viewer** node.

The list that appears on the right contains events reported by the GenWatch3 service. All GenWatch3 events contain “GW_” in the Source column, except for GenWatchService, which can be found in the same area. Double-click on an entry to view that entry’s details.

Error	3/19/2020 11:41:53 AM	GenWatchServiceLog	0	None
Information	3/19/2020 10:57:00 AM	GW_Affiliation	0	None

Figure 3.9 – Error and Information Event Log Entries

Module Health

Every 5 minutes, the GenWatch3 service logs module health information for each module in the module health log. The log files are stored in the following directory:

<Application Data>\Logs\GenWatchService

By default, the **Application Data** directory is

C:\ProgramData\Genesis\GenWatch3. The module health folders contain a log file for each day, with a maximum of 14 days of log history.

GenWatch3 Config Files

The GenWatch3 service and GUIs use config files to store settings central to the service or logged in Windows user.

Service Config Files

This config file is named **GenWatch3.config** and is stored in the following location:

The Application data folder: *C:\ProgramData\Genesis\GenWatch3*.

Changes made to the service’s GenWatch3.config file will require a service restart to take effect.

The following table shows values that may appear in the service config file:

Config File Value	Description
AliasBatchAmount	Number of GW_Alias update SQL commands needed to execute a batch update. For large, multi-RFSS installations, this number should be raised to 500 or 1,000 to decrease SQL service usage. Each time GenWatch3 is upgraded, it will update this setting to be a minimum of 200.
AliasBatchMaxSeconds	Maximum number of seconds GW_Alias will wait before executing any batched SQL commands.

Config File Value	Description
ArchiverBatchAmount	Number of GW_Archiver SQL commands needed to execute a batch command. For large, multi-RFSS installations, this number should be raised to 500 or 1,000 to decrease SQL service usage. Each time GenWatch3 is upgraded, it will update this setting to be a minimum of 200.
ArchiverBatchMaxSeconds	Maximum number of seconds GW_Archiver will wait before executing any batched SQL commands.
DatabaseName	Name of the GenWatch3 database.
DynamicAdd	Determines if resources (such as IDs and Groups) should be dynamically added to the Alias database if mentioned in data.
DynamicallyAddDefaultIpPlan	Determines if resources (such as RFSSs, sites and subsites) should be dynamically assigned default SNMP IP Address Ranges based on the most common configuration.
ExpireIds	Remove IDs from Alias if the maximum number is exceeded.
GenGETInstance	Name of the GenGET database instance.
GenGETServerName	Name of the machine hosting the GenGET database.
GW3ServerName	Name of the machine hosting the service.
Impersonate	Determines if this installation should use Windows user impersonation in relation to SQL interaction.
InstallFilePath	Location of GenWatch3 application.
InstallType	Not used.
IPVersion	IP version used on this machine. Options include IPv4 and IPv6 .
KPIDatabaseName	Name of the KPI database.
MaxDatabaseSize	Maximum database size expected in MB. This results in warning when the database approaches this size. i.e. 9 GB would be 9000.
RadioAliasUpdateThreshold	The number of consecutive identical alias updates that must be seen before GW_Alias will change a radio's alias.
RawDataFilePath	Root path where raw data files generated by input modules are stored.
RestApiClientTcpPort	The port configured during the configuration of the host to be used by the GW_WebServer module. Changing this may cause the module to be unable to handle requests due to other

Config File Value	Description
	firewall and URI reservation requirements configured during installation/configuration of the host.
RestApiRequestLogging	Enables logging of all GW_WebServer requests.
RestApiVerboseLogging	Used with the RestApiRequestLogging setting to include the body of requests and responses in the log.
RestartService	Not used.
SerialNumber	Serial number of this installation.
ServerName	Name of the machine hosting the SQL Server database.
SkyViewPath	The install path of SkyView.
TalkgroupAliasUpdateThreshold	The number of consecutive identical alias updates that must be seen before GW_Alias will change a group's alias.
ThrottleRate	The maximum number of packets allowed per second from the ATIA data source.
Trio	Determines if Trio is installed.
TrioDBServerName	Name of the machine hosting the Trio SQL database.
UseTcpCompression	Toggles the option for TCP/IP compression between a module and its GUI.
UseTcpEncryption	Toggles the option for TCP/IP encryption and Windows credential authentication between a module and its GUI. If enabled, the module PC must trust the domain of the GUI PC. If a workgroup is involved, the Windows user logged into the GUI must exist with the same password under the Windows security of the module.

GUI Config Files

This config file is also named ***GenWatch3.config*** and is stored in the following location:

The Windows login user documents folder: *C:\Users\<Windows User>\Documents\Genesis\GenWatch3.*

Changes made to a GUI's GenWatch3.config file may require you to reload the GUI to take effect.

The following table shows values that may appear in the GUI config file:

Config File Value	Description
AgencySelector	State information regarding the Agency selector

Config File Value	Description
	form.
AliasImportPath	The last path specified during an alias import.
DatabaseName	Name of the GenWatch3 database.
DebugUnlock	Encrypted debug unlock code provided by support during a support session.
DynamicAdd	Not used.
GW3HostMachine	Name of the machine hosting the service.
GW3HostMachineList	List of machine names used as hosts.
GW3ServerName	Not used.
IDSelector	State information regarding the ID selector form.
InstallFilePath	Not used.
InstallType	Not used.
IPVersion	Not used.
KPIDatabaseName	Name of the KPI database.
LastLoginInfo	Obsolete.
LastLoginName	Last user that logged into GW_Alert on this machine.
RawDataFilePath	Not used.
SerialNumber	Not used.
ServerName	Name of the machine hosting the SQL Server database.
SiteSelector	State information regarding the Site selector form.
TGSelector	State information regarding the Talkgroup selector form.
Trio	Not used.
TrioDBServerName	Not used.
UnitHistoryFromDT	Last from date/time used by this Windows user of this machine.
UnitHistoryToDT	Last to date/time used by this Windows user of this machine.
UseTcpCompression	Toggle the compression option for TCP/IP data transferred between a module and its GUI. If enabled, each packet over 1K is compressed.
ZoneSelector	State information regarding the Zone/RFSS selector form.

Updating a Config File

To update config file settings, take the following steps:

1. Browse to the config file path. For service config file options, refer to the **Service Config Files** section above. For GUI config file options, refer to the **GUI Config Files** section above.
2. Double-click on the **GenWatch3.config** file. This may result in a dialog asking you to choose an application to use to open this file. In this case, choose Microsoft Notepad.

3. Update the config file value(s) you wish to change.
4. Click **File** and **Save** to save your changes.



Depending on your PC's User Access Control (UAC) settings, you may need to run your text editor as Administrator in order to save the service's GenWatch3.config file.

Database Size Notifications

The GenWatch3 service issues a notification to all connected Alerts users when the database is reaching the maximum expected database size specified by the *MaxDatabaseSize* value in the service config file.

The default maximum expected database size is 9,000 megabytes (about 9 gigabytes). To update this value, follow the steps in the *Updating a Config File* section above.



Microsoft SQL Express has a size limitation of about 10 gigabytes. If you change the *MaxDatabaseSize* on a Microsoft SQL Express install of GenWatch3 to more than 10 GB, you will encounter severe issues.



Changing this setting may void your warranty. If you find it necessary to change this value, please contact GenWatch3 support.

Staging for Windows Authentication

You can use two methods of authentication for GenWatch3, Genesis and Windows. This section covers Windows Authentication for domains and workgroups.

Domains

Windows Authentication on domains requires a bit of planning and staging with your Windows Domain and SQL administrators. For each role you wish each user to assume in GenWatch3, you will need a Windows security group. These Windows security groups must exist as SQL instance logins within the SQL instance that houses the GenWatch3 database. Additionally, these SQL instance logins must be mapped to the GW and KPI databases using the *db_gw3user* role.

For example, given that an administrator role called *gw3admin* in the *cty* domain that will serve an administrator role in GenWatch3. And Windows user *cty\dave* will be one of the users that assumes this role. Set up the following:

1. In the GenWatch3 *GW_Security* module, create the *cty\gw3admin* role and assign the desired privileges.
2. Add the *cty\gw3admin* security group to the domain's security groups.
3. Assign the *cty\gw3admin* role to Windows user *cty\dave*.
4. In the SQL instance, add *cty\gw3admin* as a login.
5. Map *cty\gw3admin* to databases GW and KPI using role *db_gw3user*.

The first time cty\dave logs into GenWatch3, cty\dave will be auto created in the SEC_Users table with a role of gw3admin.



Be careful not to assign multiple security groups used in GenWatch3 to your Windows users. Windows users logging into GenWatch3 must have exactly one domain security group that exists as a role in the SEC_Roles table. These are matched on <domain>\<name> (i.e. cty\gw3admin is used for the gw3admin security group on domain cty). If there is not exactly one match, the user will be rejected.

Workgroups

Genesis Authentication is recommended for workgroups because they do not have a central authentication system. Each machine in a workgroup must be configured independently. If you would like to use Windows Authentication, please see the following information.

For each role you wish a user to assume in GenWatch3, you will need a Windows security group on each computer that will be used to log into the application. These Windows security groups must exist as SQL instance logins within the SQL instance that houses the GenWatch3 database with the same computer name as the machine that hosts the GenWatch3 service. Additionally, these SQL instance logins must be mapped to the GW and KPI databases using the db_gw3user role. A user must have the same Windows password on all machines in the workgroup.

As an example, consider a network with two computers. SystemHost is the host computer that runs GenWatch3 and the GenWatch3 database. SystemClient runs a GenWatch3 client. We want to create a role named gw3admin that will serve an administrator role in GenWatch3. User Dave will be a member of this group. Dave wants to be able to log into GenWatch3 from either computer.

These are the steps required to set up this system:

1. In the GenWatch3 GW_Security module, create the SystemHost\gw3admin and SystemClient\gw3admin roles and assign the desired privileges. **Note that these are two independent roles and their privileges must be maintained separately.**
2. Create the gw3admin security group in Windows on both SystemHost and SystemClient.
3. Assign the gw3admin role to Windows user Dave on both SystemHost and SystemClient.
4. In the SQL instance, add SystemHost\gw3admin as a login.
5. Map SystemHost\gw3admin to databases GW and KPI using role db_gw3user.

The first time Dave logs into GenWatch3 from a computer, <computer_name>\Dave will be auto created in the SEC_Users table with a role of <computer_name>\gw3admin. If Dave logs in from another computer, the role will be updated to the new computer name.



A user's permissions could vary based on which machine they use to log into GenWatch3 if the roles are not maintained consistently for each machine.



Be careful not to assign multiple security groups used in GenWatch3 to your Windows users: Windows users logging into GenWatch3 must have exactly one security group that exists as a role in the SEC_Roles table. These are matched on <computer_name>\<name> (i.e. SystemHost\gw3admin is used for the gw3admin security group on computer SystemHost). If there is not exactly one match, the user will be rejected.



If the GenWatch3 databases are owned by a local machine account, that account will not be able to log into GenWatch3 because its role cannot be changed.

This chapter contains the following sections:

- **What are Module GUIs?:** Describes the function of the GenWatch3 module GUIs.
- **Common Module GUI Buttons:** Defines each common module GUI button.
- **Module Connection Buttons, Display and Functions:** Defines each button display and function associated with the data stream between the module GUI and the module.
- **Database Incompatibility Warnings:** Describes the database incompatibility warnings issued by GenWatch3.
- **Module Help:** Describes the integrated help/manual GUIs that can be accessed from any GenWatch3 module GUI.










What are Module GUIs?




GenWatch3 provides a GUI for each of its modules. Each module GUI differs in its purpose and its interaction with its module. Some module GUIs simply provide a setup interface for the module, such as the GW_Archiver GUI. Some module GUIs show input packet traffic such as GW_Activity or statistics such as GW_SysVista.

Although each GUI looks and behaves differently, all GUIs share some common functionality. This chapter describes these common functions.

Common Module GUI Buttons

Many of the buttons in GenWatch3 use icons common to all its GUIs. These buttons perform the following actions:

- : The **Add** button allows you to add items such as connections in various GenWatch modules.
- : The **Delete** button allows you to remove items such as connections in various GenWatch modules.
- : The **Save** button will save the item currently being edited.
- : The **Options** button will allow the user to configure additional options for a module or targeted item.
- : The **Edit** button allows a user to edit an item.
- : The **Previous** button is used to navigate to the previous item or page.
- : The **Next** button is used to navigate to the next item or page.
- : The **Refresh** button is used to retrieve a fresh copy of an item or items from a data source.
- : The **Browse** button allows users to choose an item such as a color, radio or talkgroup from a list.

- : The **Clear** button will reset the values on a form.
- : The **History** button will display a list of historical events for the targeted item.
- : The **Cancel** button cancels the edit in progress.

Module Connection Displays and Functions

Each module GUI must maintain a constant connection with its respective module. This connection is used to:

- Allow the module to pass data to the module GUI, such as:
 - Licensing information.
 - Real-time data.
 - Global GenWatch3 notifications, such as GW_Alias or GW_Security updates or GW_Trigger events.
- Notify the module when settings or options are changed in the module GUI.

Each module GUI contains:

- Module Status box: Displays the current connection status.

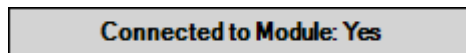


Figure 4.1 – Module Status box

Default Module Ports

Each GenWatch3 module has a distinct port number that it uses to communicate with its GUI. The table below shows each module's default port number:

Module	Default Port
GW_LaunchPad	10300
GW_Alerts	10301
GW_Activity	10320
GW_Archiver	10321
GW_SysLog	10323
GW_Alias	10324
GW_Group	10325
GW_Channel	10326
GW_SystemSummary	10327
GW_Affiliation	10328
GW_SAM	10329
GW_GenSPOut	10330
GW_Location	10331
GW_Security	10332
GW_SysVista	10333
GW_Trigger	10338
GW_Halcyon	10339
GW_ATIA	10340
GW_Reports	10342
GW_RSP25	10343

Module	Default Port
GW_GENsAC	10344
GW_TRBO	10348
GW_Connect	10349
GW_Trio	10350
GW_GenIIB	10351
GW_APM	10353
GW_KPI	10354

Table 4.1 – GenWatch3 Module Default TCP/IP Ports

Changing a Module's Default Port

The default port for each module is shown in the table above. You can change these ports if they conflict with another application attempting to use the same ports. To change the module port, contact GenWatch3 support.



Changing a port may void your warranty. If you feel you need to change a module port, please contact GenWatch3 support.

Database Incompatibility Warnings

When a GUI loads, it checks its version against the version of the GenWatch3 database used by the GenWatch3 host. If there is a difference between versions or either version could not be determined, the GUI shows a warning like the one below.

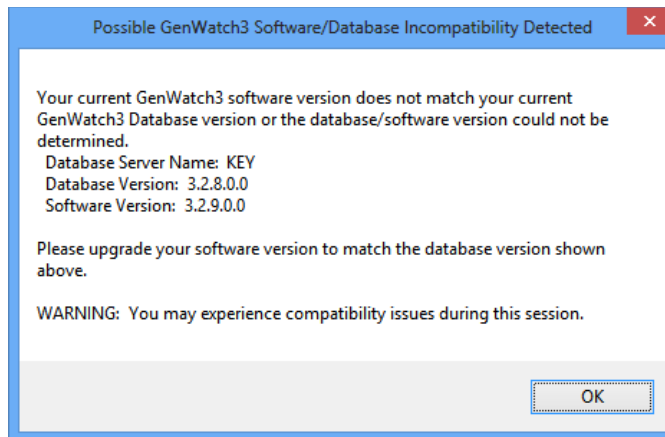


Figure 4.2 – Database Incompatibility Warning

This warning commonly results from a GenWatch3 client installation using a different version than the GenWatch3 host installation. If you see this warning, please contact your system administrator or Genesis support.

Module Help

GenWatch3 has an integrated help system if you need help for any part of GenWatch3. Each module has its own help manual that can be easily accessed from within the module's GUI. To show the help manual for a specific module,

load that GUI and press the **F1** key. This will display the help manual in the *GenWatch3 Help Viewer* as shown below.

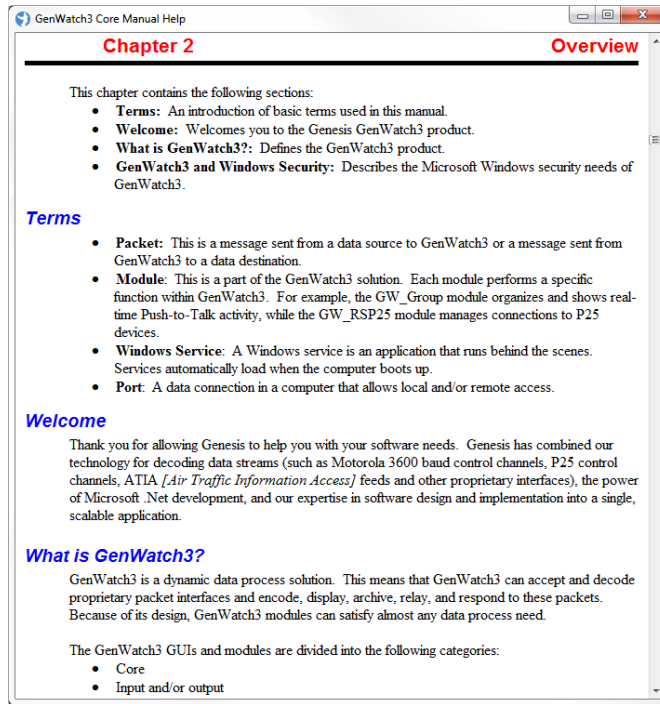


Figure 4.3 – GenWatch3 Help Viewer

In the *GenWatch3 Help Viewer*, you can navigate throughout the manual. A Table of Contents appears near the start of the manual, allowing quick navigation through the manual.



In many cases, GenWatch3 will automatically navigate within the manual to display the section which pertains to the part of the GUI directly under the mouse cursor. For example, in the GW_Activity module GUI, if you press **F1** while the mouse hovers over the Packet Types list in that GUI, the GenWatch3 Help Viewer will load the GW_Activity manual and automatically navigate to the Packet Types section of the manual.

This chapter contains the following sections:


- **What is GW_Alerts?:** Describes the GW_Alerts application and its role in the GenWatch3 solution.
- **Logging into GW_Alerts:** Describes the GenWatch3 login window as provided by GW_Alerts.
- **GW_Alerts Menu:** Describes the use of the GW_Alerts menu.
- **GW_Alerts Connection Icons:** Describes the types of icons shown by GW_Alerts and how to interpret and/or interact with them.
- **GW_Alerts Notification Windows:** Describes the Notification Window feature provided by GW_Alerts.

What is GW_Alerts?

GW_Alerts is a System Tray application. This means that this application does not display a GUI. Instead, it shows an icon in the Windows System Tray (the bottom-right area of your desktop next to the clock). GW_Alerts will show one of the following icons:

- : This icon indicates that the GW_Alerts application is running and is currently connected to the GenWatch3 service.
- : This icon indicates that the GW_Alerts application is running but is not currently connected to the GenWatch3 service.

If you do not see either of these icons, you may need to start GW_Alerts. To start GW_Alerts, take the following steps:

1. Click on the Windows Start button.
2. Click on All Programs (or Programs in some versions of Windows).
3. Click on Startup.
4. Click the GenWatch3 icon  GenWatch3. This will load GW_Alerts and show the login window.

Logging into GW_Alerts

The GenWatch3 Installer places a shortcut to GW_Alerts in the Startup folder of your Windows Start menu. This means that when Windows starts up (after reboot, power off, etc.), it loads GW_Alerts automatically. After GW_Alerts loads, the **Login** window will appear:

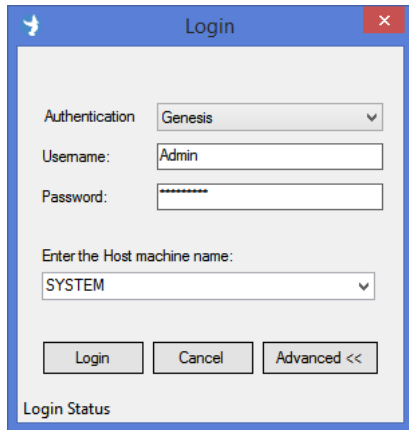


Figure 5.1 – GenWatch3 Login Window

The *Login* window contains the following options:

- **Authentication:** Type of authentication used to log into GenWatch3. Options include Genesis and Windows.
- **Username:** GenWatch3 username you wish to log in with. This box will contain the username that last logged in on this machine. If this is your first time logging in, use **Admin**
- **Password:** Password of the GenWatch3 user entered in **Username**.
- **Enter the Host machine name:** Name of the machine that is running the GenWatch3 service. This drop-down list will contain the names of all previous host machines used on this machine.
- **Cancel:** Click this button to cancel login and close GW_Alerts.
- **Login:** Click this button once you have entered or verified the **Authentication**, **Username**, **Password**, and **Host machine name**.
- **Advanced:** Shows / Hides the **Enter the Host machine name** option.

GenWatch3 uses your login information provided in this login window for GW_LaunchPad and all other GenWatch3 GUIs. In GW_LaunchPad, click the **Switch User** item under the **File** menu to log in as a different user or to log into a different GenWatch3 host.



GenWatch3 users are limited to a single Alerts session. If you attempt to use a GenWatch3 user to log into GW_Alerts from multiple machines, GenWatch3 will reject each attempt beyond the first.



Accounts are stored in SQL Server and may be locked out if a user tries to log in with an incorrect password too many times. SQL Server uses domain settings to determine the number of failed logins allowed before the account is locked out and the duration of the lockout. SQL Server does not report the reason a login attempt was rejected to the client for security reasons. A SQL Server administrator can determine if an account is locked out and unlock it. See SQL Server documentation for this procedure.

If an administrator requires users to agree to a policy statement before logging in, the statement will open in a new window after the user clicks the **Login** button. The user must click the **I Agree** button to proceed with the login.

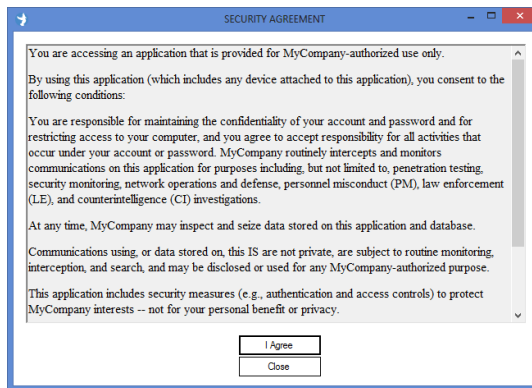


Figure 5.2 – GenWatch3 Security Warning Banner

Password Expiration

Passwords for GenWatch3 logins are stored in the Microsoft SQL Server instance that hosts the GenWatch3 database. Password expiration is based on your local security policy or domain security policy if the GenWatch3 host is a member of a domain.

If passwords are set to expire, Alerts will show how many days remain until the logged-in user's password expires.

If the user's password has expired and requires a change, Alerts will present a Change Password window upon login. Use this window to change the password of the user that is attempting to log in.

GW_Alerts Menu

The GW_Alerts menu appears when you right-click on the GW_Alerts icon. This menu contains the following options:

- **LaunchPad:** Loads the GW_LaunchPad application.
- **Modules:** Displays a list of shortcuts to licensed modules. Click to open a module directly.
- **Tools:** Displays list of shortcuts to Tools configured in GW_LaunchPad.
- **Emergencies:** Provides access to the Emergency Display window.
 - **Show:** Displays the Emergency window.
 - **Show on Emergency:** “Arms” the emergency window so that it is displayed when an emergency event occurs.
- **Close All Modules:** Closes all open GenWatch3 windows except for GW_LaunchPad.
- **Exit:** Closes GW_Alerts.










If GW_Alerts is closed, you will not receive GenWatch3 Notifications. Also, the connection icons will not show. Genesis recommends that you never close GW_Alerts.

GW_Alerts Connection Icons

The above section described the GW_Alerts icons that show the running and connected state of GW_Alerts. Additionally, GW_Alerts will show an icon in the System Tray for each active (enabled) connection in each GenWatch3 input module. For example, if your GW_RSP25 module has two active connections, GW_Alerts will show two connection icons.

Some GenWatch3 input module connections offer TCP/IP packet forwarding. For example, you can set up a GW_RSP25 connection to connect to a P25 data source via COM port 1 and forward the P25 packets to TCP/IP port 10599. A client TCP/IP application can connect to port 10599, and therefore become a client to the GW_RSP25 connection.

Connection icons show one of the following states:

-  : Connection is encountering an error.
-  : Connection with a connected client is encountering an error.
-  : Connection has received packets within the past several seconds. The amount of time varies by connection type.
-  : Connection with a connected client has received packets within the past several seconds. The amount of time varies by connection type.
-  : Connection has not received packets within the past several seconds. The amount of time varies by connection type. (Blinks between red and white background.)
-  : Connection with a connected client has not received packets within the past several seconds. The amount of time varies by connection type. (Blinks between red and white background.)
-  : Connection that manages multiple data sources is receiving data from at least one source, but at least one other source is either not receiving data or has a connectivity issue.



Hover (move the mouse) over a connection icon to see its connection type, name and status.

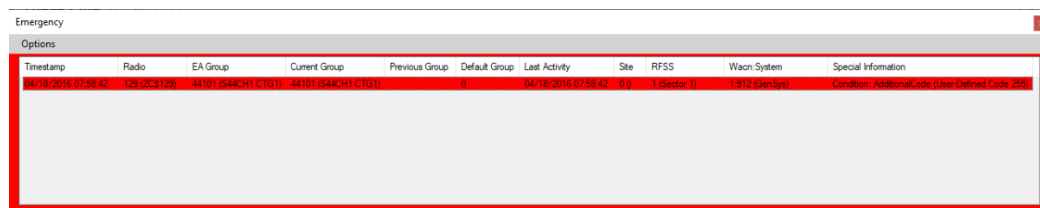
GW_Alerts Notification Windows

Notifications come in many forms. They can range from a Link Down notification from an input module (indicating that the data stream is down) to an Unacknowledged Emergency Alarm (sent by GW_Halcyon indicating that an emergency alarm was not delivered to a dispatcher). No matter what the flavor, these notifications are displayed in the GenWatch3 Notification window via GW_Alerts.

See *Chapter 11 - GenWatch3 Notifications* for more information on the GenWatch3 Notification window.

GW_Alerts Emergency Display

The Emergency Display window provides direct information about emergency events on the system. The list font can be changed through the options menu.



Timestamp	Radio	EA Group	Current Group	Previous Group	Default Group	Last Activity	Site	RFSS	Wacon System	Special Information
04/18/2016 07:58:42	129 (2C3129)	44101 (S4ACH1 CTG1)	44101 (S4ACH1 CTG1)			0	04/18/2016 07:58:42	0.0	1 (Sector 1)	1.912 (GenSys)
Condition: AdditionalCode (User-Defined Code 255)										

Figure 5.3 – Emergency Display

The emergency window contains the following columns. **Bold** items are updated with new activity from the emergency unit.

- **Timestamp**: Displays the time of the initial emergency alarm.

- Radio: Displays the ID and alias of the unit in an emergency state.
- EA Group: Displays the group received in the emergency alarm packet.
- **Current Group: Displays the group to which the radio is currently affiliated.**
- Previous Group: Displays the group the radio was affiliated to prior to the emergency alarm.
- Default Group: Displays the default group selected in alias.
- **Last Activity: Displays the time of the last received activity.**
- **Site: Displays the site on which the radio is currently affiliated.**
- **RFSS: Displays the RFSS involved.**
- **WACN:System: Displays the WACN:System involved.**
- Special Information: Displays additional information about the emergency status of the radio (when available).

Access the Emergency Display by right-clicking the GW_Alert icon and select one of the following options under the **Emergencies** submenu:

- **Show** to display the emergency window
- **Show on Emergency** to display the emergency window when an emergency event occurs.

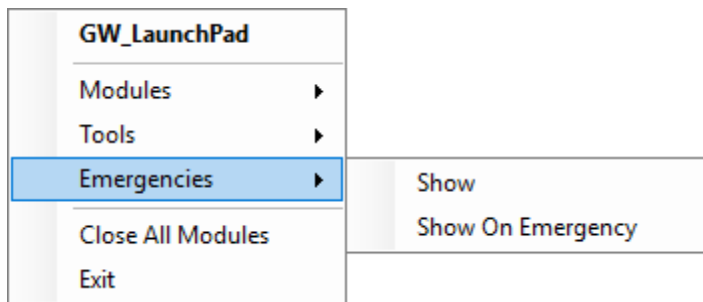


Figure 5.4 – Emergencies submenu

Removing emergency messages

Emergency messages can be cleared by right-clicking on an emergency and choosing an option from the Emergency Context Menu.

- **Delete** removes the currently selected emergency.
- **Clear All** to remove all emergencies.

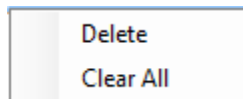


Figure 5.5 – Emergency Context Menu



Emergencies will be displayed for users that have the GW_Security *Administrator* privilege or have the emergency's Group or Agency and Location in GW_Security's User Filter.

This chapter contains the following sections:

- **Viewing Real-time Module Status:** Describes how to view and understand the *Modules* list and the *Info* section.
- **Creating Module Notes:** Describes how to create and view module notes.
- **Loading Module GUIs:** Describes how to load the module GUI for a module.
- **Loading the GenWatch3 License Manager:** Describes how to load the GenWatch3 License Manager window.
- **Creating Shortcuts to Useful Tools:** Describes how to create shortcuts within GW_LaunchPad to the applications that you use the most.
- **Setting Up a Temporary Filter for Real-Time Activity Modules:** Describes how to create a filter that will affect multiple GUIs for a limited time.
- **Changing Global Settings:** Describes how to further customize GenWatch3.

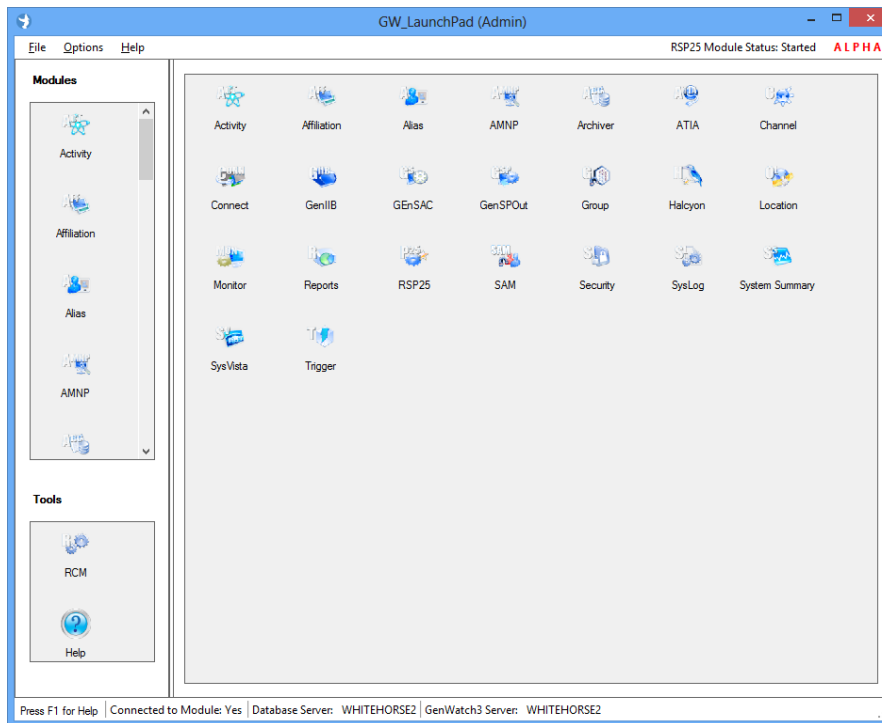


Figure 6.1 – GW_LaunchPad GUI

Viewing Real-time Module Status

GW_LaunchPad allows you to view module activities and statuses for the selected module icon. This status is shown on the right side of the menu bar. It shows:

1. **Module Name:** Shows the selected module's name.
2. **Status:** Shows the selected module's overall status at the time it was selected. Module statuses include:
 - **File Not Found or Not a DLL:** GenWatch3 module file is missing or corrupt.
 - **Invalid DLL:** GenWatch3 module file does not satisfy the installed version of the module interface.
 - **Not Licensed:** GenWatch3 license does not include this module.
 - **Expired:** Evaluation/lease period has expired.
 - **Starting:** The GenWatch3 service is starting the module.
 - **Started:** The module is started (currently processing).
 - **Stopping:** The GenWatch3 service is stopping the module.
 - **Stopped:** The module is currently stopped (not processing).

Modules List Menu

To view the Modules menu, right-click on the Modules list. The Modules menu includes the following options:

- **Open Interface:** Opens the selected module's GUI.
- **Show Quick Launch:** Shows all module icons in the Product Sheet section of GW_LaunchPad.
- **Show Module Product Sheets:** Shows the product sheet of the selected module in the Product Sheet section of GW_LaunchPad.
- **Refresh Modules:** Refreshes the Modules list and the status of all modules.
- **Temporary Filter:** Opens a window to set up a temporary filter for real-time activity modules.
- **Global Settings:** Opens a window to change GenWatch3 options for the current user, such as the unit of measure displayed.

Creating Module Notes

GW_LaunchPad allows you to make PC-specific notes for each GenWatch3 module. PC-specific means that each user that uses GW_LaunchPad on this machine will see these notes. These notes allow you to:

- Leave a module-related note for the next user.
- Provide yourself with additional information about the module.

To create module notes, take the following steps:

1. Hover the mouse over the slider to the right of the modules list. This will show a slider adjustment icon.
2. Click and hold and move the slider to the right, exposing the *Notes* section.

3. Select the module for which you wish to make notes.
4. Type the notes in the *Notes* section.

Loading GUIs

GW_LaunchPad provides a portal (central location) for launching the GUIs. To launch a GUI, take the following steps:

1. Find the icon of the module that you wish to launch in the Modules list.
2. Double-click on the module icon. This will load the GUI for the module that you double-clicked.

Load the GenWatch3 License Manager

GW_LaunchPad provides an entry point into the GenWatch3 License Manager if you are running GW_LaunchPad from the GenWatch3 server machine. To load License Manager, click in the **View License** option in the **Help** menu. This will load *GenWatch3 License Manager*.

You can read more in *Chapter 7 - GenWatch3 License Manager*.

Creating Shortcuts to Useful Tools

GW_LaunchPad provides a handy feature that allows you to easily link to other files or programs on your machine. For instance, if you commonly run Notepad or Excel, you can add them to GW_LaunchPad as “Tools” and then start them from within the GW_LaunchPad *Tools* window. The *Tools* window is found below the Modules list and will already contain a link to GenWatch3 help. It will also contain the link to RCM if you purchased the Commander series of GenWatch3.



Clicking the help link will launch the help page with the program assigned to open .htm files in Windows.

To add a tool to GW_LaunchPad, perform the following steps:

1. Click the **Add Tool** option under the **Options** menu. This will open the *Add Tool* window shown below.
2. Enter or browse to the location of the file to be added to the tools.
3. A tool name will be populated based off the name if a file is selected. Edit the name of the tool if desired or enter a name if the location was entered manually.

A screenshot of the 'Add Tool' dialog box. It has a blue title bar with the text 'Add Tool' and a red close button. Inside, there are two text input fields. The first is labeled 'Tool name:' and is empty. The second is labeled 'Tool file location:' and is also empty. To the right of the 'Tool file location:' field is a 'Browse' button. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Figure 6.2 – Add Tool

Below is a sample of what your *Tools* window might look like if you are licensed for the RCM tool:

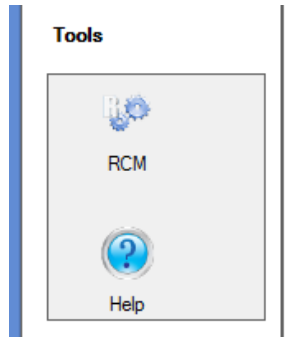


Figure 6.3 – Tools

Setting Up a Temporary Filter for Real-Time Activity Modules

GW_LaunchPad allows you to create a filter that will affect the GW_Activity, GW_Channel and GW_Group modules for a specified amount of time. This allows you to quickly narrow your focus down to a specific set of radio IDs or talkgroups without having to manually disable the filter later.

To create a temporary filter, perform the following steps:

1. Open the Modules menu by right-clicking in the modules box. Select **Temporary Filter**; this will open the *Temporary Filter* window.
2. Check the **Enable Temporary Filter** box. This will allow you to edit the filter settings.
3. From the **Filter Type** drop-down box, choose the type of resource you'd like to filter on.
4. Specify a duration for the filter on the **Duration** control. Setting a duration of zero will cause the filter to last until manually disabled using this window.
5. Click the **+** button to add resources to your filter list.
6. From the selector window, you can search your GW_Alias database for resources based on a variety of properties or leave the fields blank to return all resources of that type. Click **Search** to see the list of resources that meet your criteria.
7. Select the resources you would like to be able to see on the real-time activity modules, then click **OK**. Activity from resources that are not selected will not be visible on GW_Activity, GW_Channel or GW_Group, but that activity will still be archived to your database.
8. To remove a single resource, highlight the resource and click the **-** button.
9. To remove all resources from the filter, click the **⊖** button.

10. Click the **OK** button on the *Temporary Filter* window. This will activate the filter and start its timer. A timer showing the remaining time will be displayed on LaunchPad.

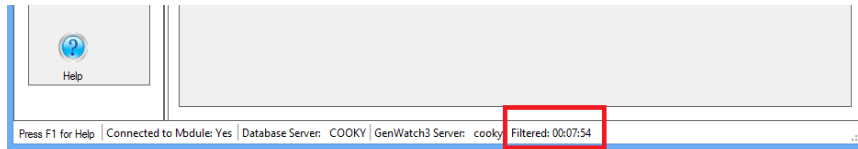


Figure 6.4 – Temporary Filter and Filter time remaining

To manually disable a temporary filter, perform the following steps:

1. Click the **Temporary Filter** option in the Modules menu. This will open the *Temporary Filter* window. You can also open this window by double-clicking the filter timer on the bottom-right corner of the Launch GUI.
2. Uncheck the **Enable Temporary Filter** box.
3. Click **OK**. The filter will be disabled.



If no resources are added to a filter the filter will be disabled when the user attempts to apply the filter.

Changing Global Settings

GW_LaunchPad allows each GenWatch3 user to specify preferences that will be applied to every applicable module GUI. Changing a global setting on one user will not affect the global settings used by any other user. Module GUIs must be closed and reopened to reflect updated global settings.

To change the global settings, right-click in the Modules list to bring up the Modules menu. Select **Global Settings** to open the *Global Settings* window.

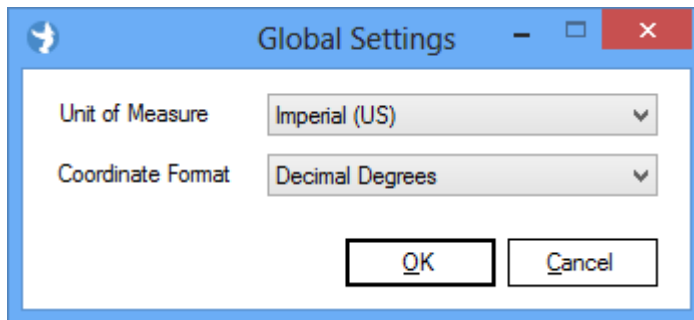


Figure 6.5 – Global Settings Window

The following options can be changed:

- **Unit of Measure:** This specifies whether measurements displayed in GenWatch3 should use imperial or metric units. This is used in several module GUIs to display distances in either miles or kilometers.
- **Coordinate Format:** This specifies the format to be used when displaying geographic coordinates, such as those provided by GPS systems. The options are:
 - **Decimal Degrees:** Formats coordinates like *32.305108*
 - **Degree Minutes Seconds:** Formats coordinates like *32° 18' 18.389"*

This chapter contains the following sections:

- **Do I Need to Activate My License?:** Describes scenarios that would not require you to activate your GenWatch3 license.
- **What is the GenWatch3 License?:** Describes the function and role of the GenWatch3 license.
- **Loading GenWatch3 License Viewer:** Describes how to load the *GenWatch3 License Viewer*.
- **License Details:** Describes the information shown in the *GenWatch3 License Viewer*.
- **License Manager Options:** Describes the function of each option above the License Details.

Do I Need to Activate My License?

Some installs of GenWatch3 come pre-installed on a GenWatch3 machine (PC). These installs have an activated license. The activation steps defined in this chapter are not necessary for these installs.

If your GenWatch3 computer was not shipped to you from The Genesis Group or staged by a third party, you will need to go through the activate license process described below.

In short, if the *Activate Product(s)* window greets you when you load GW_Alerts, you need to activate your license.

What is the GenWatch3 License?

The GenWatch3 license allows you to customize your GenWatch3 installation by selecting from various GenWatch3 product packages. The GenWatch3 license also protects your software from piracy and illegal distribution. GenWatch3 licensing exists within the GenWatch3 Service, each module, and in some module GUIs. The *GenWatch3 License Viewer* shows all licensing information for GenWatch3, including each licensed module.

Loading GenWatch3 License Viewer

To load *GenWatch3 License Viewer*, take the following steps:

1. Load GenWatch3 GW_LaunchPad
2. Click on the **View License** option under the **Help** menu. This will load the *GenWatch3 License Viewer*.

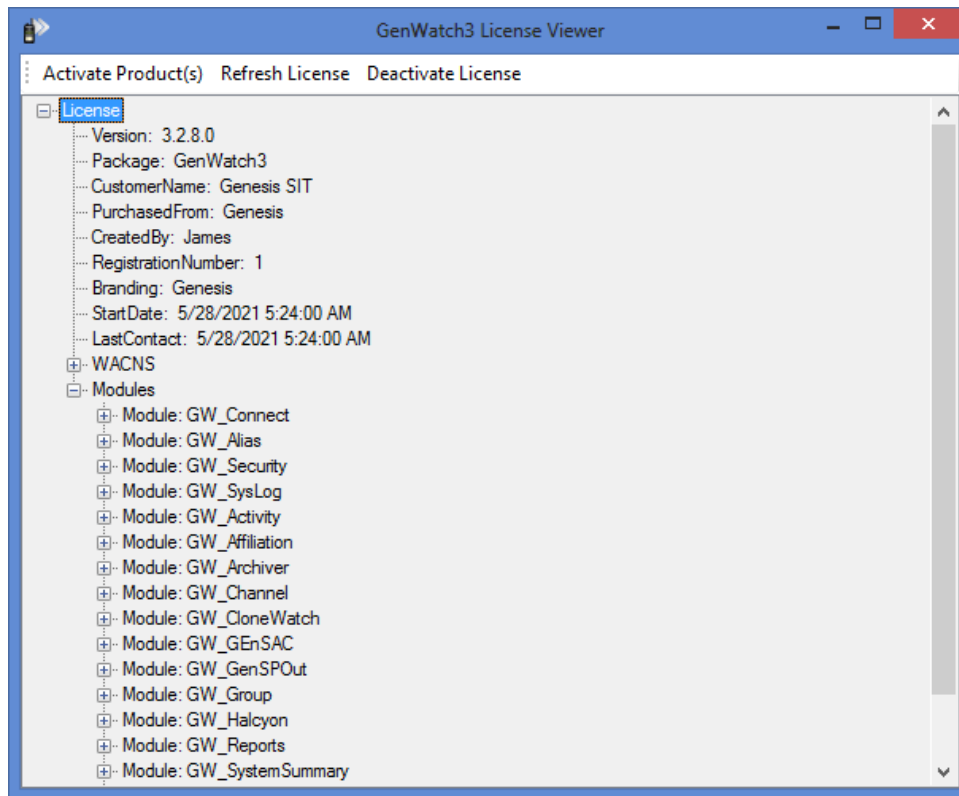


Figure 7.1 – GenWatch3 License Viewer

The GenWatch3 service (the behind-the-scenes application that runs the GenWatch3 modules) is licensed for a specific machine. If a GenWatch3 machine changes drastically, your license will become invalid and you must contact GenWatch3 support to obtain a new GenWatch3 license. Changes such as replacing a hard drive or upgrading the operating system will invalidate the license.

License Details

The License Details tree shows detailed information regarding your activated GenWatch3 license. The major sections include:

- **Version:** Licensed GenWatch3 version.
- **Package:** GenWatch3 package purchased.
- **CustomerName:** Customer this license is registered to.
- **PurchasedFrom:** Company you purchased this license through.
- **RegistrationNumber:** Generally, the purchase order for this license.

- **Branding:** Branding option. This is usually Genesis.
- **StartDate:** The date/time this license was issued.
- **LastContact:** Last modification made to this license.
- **WACNS:** The topmost tier of the licensed infrastructure. This infrastructure will contain at least one licensed system.
- **Modules:** Contains an entry for each licensed module. Each module contains a **Restrictions** section, with an entry for each of its specific license features.

License Manager Options

Activate Product(s)

This option opens the *Activate Product(s)* window. This window is used to evaluate the GenWatch3 product or to activate GenWatch3 after you have purchased a license.

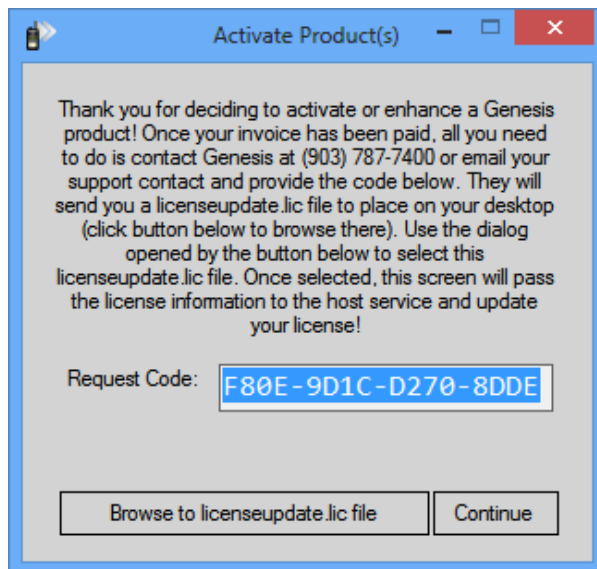


Figure 7.2 – Activate Product(s) Window

The *Activate Product(s)* window contains the following options:

- **Browse to licenseupdate.lic file:** Click this button to show the *Open File* dialog box. This dialog box allows you to browse your local and network machine for the GenWatch3 license file.
- **Continue:** Click this button to close the *Activate Product(s)* window. This button is only available if your GenWatch3 installation is licensed.
- **X:** Click this button to close the *Activate Product(s)* window. If your GenWatch3 is not licensed, this will also close GW_Alerts.

If your GenWatch3 installation was not licensed by your vendor, GenWatch3 shows the *Activate Product(s)* window when you run GW_Alerts. This is our way of telling you that your GenWatch3 installation is not licensed.

To activate your purchased GenWatch3 license, take the following steps:

1. Select the ENTIRE code in the Request Code box.
2. Right-click on the selected code. This will show an edit pop-up menu with options including **Copy**.
3. Choose **Copy** from the edit pop-up menu.
4. Open your email application and create a new email to support@genesishworld.com
5. Right-click in the body of the email. This will show an edit pop-up menu with options including **Paste**.
6. Choose **Paste** from the edit pop-up menu. This will paste your Request Code into the email exactly as it was on the *Activate Product(s)* window.
7. Also include in the email your company name and your contact information.
8. Send the email.
9. Contact GenWatch3 support (see the Support section of this manual). The support person will assist you with the rest of the activation process.

The result of this license request is a license file, usually named `licenseupdate.lic`. Use the **Browse to licenseupdate.lic file** button (described above) to select the license file and click **OK**. This will send the file to the GenWatch3 service and update the GenWatch3 license.

Updating the GenWatch3 license results in a GenWatch3 Notification window (described in *Chapter 11 – GenWatch3 Notifications*), warning you and all other administrator-level GenWatch3 clients that a GenWatch3 user has updated the license. If you are activating the initial license for GenWatch3, this will also enable the **Continue** button.

Refresh License

This option queries the GenWatch3 service for the current license. The *GenWatch3 License Viewer* shows the results of the query.



If no email is available at the installation site, the person performing the install will need to run GW_LaunchPad, get the activation code, physically go to a location that does have access to email, request the activation file from Genesis, copy the activation file provided by Genesis to some form of removable media (CD, Disk, Flash drive, etc.), bring the file back to the installation site, and place it in the GenWatch3 installation directory.

Deactivate License

If you need to move your GenWatch3 host to a different machine, you will need to deactivate the license on the current host. The **Deactivate License** button results in a *GenWatch3 Unlock Code* window. You must contact GenWatch3 support in order to receive an unlock code.

Once you enter the unlock code, you will receive a dialog box showing the deactivation confirmation code. This code is provided to GenWatch3 support to confirm that the license has been deactivated.



The Deactivate License option is only available to users with the *GW_Security Administrator* privilege.

This chapter contains the following sections:

- **What is GW_Security?:** Describes the role of security within GenWatch3.
- **Privileges:** Describes the function of privileges.
- **Security for Windows Authentication:** Notes for using Windows Authentication.
- **Roles:** Describes the function of roles and how to maintain them.
- **Users:** Describes the function of users and how to maintain them.
- **Activity History:** Describes how to view the user activity history view.
- **Current Users:** Describes how to view the list of current users.

What is GW_Security?

In GenWatch3, security refers to the different functions and data filters that you can allow or disallow on a per-module-per-user basis. GenWatch3 applies these security options to each user when they log into GW_LaunchPad. They are carried over to each GUI or tool that this user launches within GW_LaunchPad. The security properties within GW_Security are made up of three entities:

- **Privileges:** Predefined allowances for actions and view rights within the GenWatch3 module GUIs. Privileges exist on a per-module basis.
- **Roles:** Used to describe and house a group of privileges.
- **Users:** Used to define the people that use the GenWatch3 module GUIs. Users are assigned a role and a list of groups which they can view (Unconditional access to all groups is a role privilege granted on a module-by-module basis).

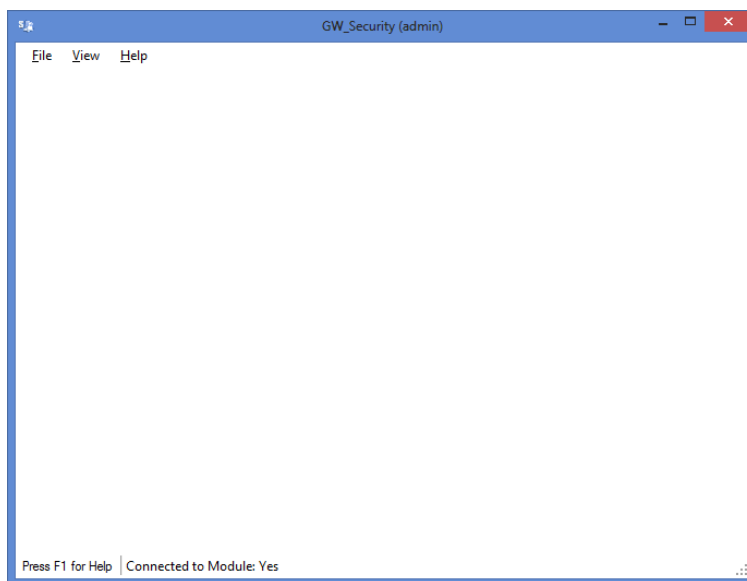


Figure 8.1 – GW_Security GUI

Privileges

Privileges are pre-defined module-level allowances for actions and view rights within a GenWatch3 GUI. Each module contains a set of pre-defined privileges. Privileges are assigned to roles; therefore, a user who is assigned a role inherits that role's privileges.

Privileges List

The table below shows each module and its pre-defined privileges:

Module	Privilege	Description
GW_Activity	Access	Allows the user to access this module's GUI.
	DisableThrottle	Allows the user to remove the packet throttle (some data stream packets are throttled to 1 distinct packet per second).
	ViewAllAgencies	Ignores user-level agency filters.
	ViewAllGroups	Ignores user-level group filters.
	ViewAllSites	Ignores user-level site filters.

Module	Privilege	Description
GW_Affiliation	Access	Allows the user to access this module's GUI.
	ViewAllAgencies	Ignores user-level agency filters.
	ViewAllGroups	Ignores user-level group filters.
	ViewAllSites	Ignores user-level site filters.

Module	Privilege	Description
GW_Alias	Access	Allows the user to access this module's GUI.
	Delete	Allows the user to delete existing resources.
	Edit	Allows the user to update existing resources.
	Import	Allows the user to import and add resources.
	Resynchronize	Allows the user to request the module to resynchronize its alias list with the alias database.
	ViewAllGroups	Ignores user-level group filters when selecting groups for triggers in GW_Trigger.
	ViewAllSites	Ignores user-level site filters when selecting sites for triggers in GW_Trigger.

Table 8.1 – Module Privileges

Module	Privilege	Description
GW_APM	Access	Allows the user to access this module's GUI.
	ViewAllSites	Ignores user-level site filters.

Module	Privilege	Description
GW_Archiver	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to update archiving options.

Module	Privilege	Description
GW_ATIA	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to add, update, and delete connections.
	SetupFilters	Allows the user to edit the filter settings for each connection.

Module	Privilege	Description
GW_Channel	Access	Allows the user to access this module's GUI.
	ViewAllAgencies	Ignores user-level agency filters.
	ViewAllGroups	Ignores user-level group filters.
	ViewAllSites	Ignores user-level site filters.

Module	Privilege	Description
GW_Connect	Access	Allows the user to access this module's GUI
	Edit	Allows the user to add, update, and delete connections.

Module	Privilege	Description
GW_GenIIB	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to add, update, and delete controllers.

Table 8.1 – Module Privileges (cont.)

Module	Privilege	Description
GW_GEnSAC	Access	Allows the user to access this module's GUI.

Module	Privilege	Description
GW_GenSPOut	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to add, update, and delete settings.

Module	Privilege	Description
GW_Group	Access	Allows the user to access this module's GUI.
	ViewAllAgencies	Ignores user-level agency filters.
	ViewAllGroups	Ignores user-level group filters.
	ViewAllSites	Ignores user-level site filters.

Table 8.1 – Module Privileges (cont.)

Module	Privilege	Description
GW_Halcyon	Access	Allows the user to access this module's GUI.
	Call Alert	Allows user to issue Call Alerts.
	Database Snapshot	Allows the user to issue Database Snapshots.
	Dynamic Regrouping	Allows the user to issue Dynamic Regroupings (Regroup, Failsoft Assignment and selector lock).
	Emergency Alarm	Allows the user to monitor Emergency Alarm events.
	Failsoft Assignment	Allows the user to issue commands that include Failsoft Assignment.
	GPS Location Requests	Allows the user to issue location requests to the GW_Location module.
	IMW Location Requests	Allows the user to issue location requests to an IMW connection.
	Radio Check	Allows the user to issue Radio Checks (Request Radio Affiliations).
	Selective Inhibit	Allows the user to issue Selective Inhibits.
	Selector Lock or Unlock	Allows the user to issue commands that include Selector Locks.
	Status Message	Allows the user to monitor Status and Message events.
	Unattended Emergency Alarm	Allows the user to receive Emergency Alarm events that fail to be delivered to a connected RCM or CADI user.
	ViewAllAgencies	Ignores user-level agency filters.
	ViewAllGroups	Ignores user-level group filters.
	ViewAllSites	Ignores user-level site filters.

Module	Privilege	Description
GW_KPI	Access	Allows the user to access this module's GUI.

Table 8.1 – Module Privileges (cont.)

Module	Privilege	Description
GW_Location	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to add, update, and delete connections.

Module	Privilege	Description
GW_Reports	Access	Allows the user to access this module's GUI.
	ViewAllAgencies	Ignores user-level agency filters.
	ViewAllGroups	Ignores user-level group filters.
	ViewAllSites	Ignores user-level site filters.

Module	Privilege	Description
GW_RSP25	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to add, update, and delete connections.
	SetupFilters	Allows the user to edit the filter settings for each connection.

Module	Privilege	Description
GW_SAM	Access	Allows the user to access this module's GUI.

Table 8.1 – Module Privileges (cont.)

Module	Privilege	Description
GW_Security	Access	Allows the user to access this module's GUI.
	Administrator	Allows the user Administrator access to GenWatch3.
	ChangePassword	Allows the user to change passwords. If combined with ManageUsers, then the user can change the password of any user. Otherwise, the logged-in user can only change his/her password.
	ManageRoles	Allows the user to add, update, and delete roles. If not given, then the user has view-only access to the role assigned to him/her.
	ManageUsers	Allows the user to add, update, and delete users. If not given, then the user has view-only access to their own user properties.*
	ViewCurrentUsers	Allows the user to view the list of currently logged-on users.*
	ViewUserActivity	Allows the user to see other users' activity. If not given, the user can only see their own activity.*

*Only users with the Administrator role will be able to see other users with the Administrator role.

Module	Privilege	Description
GW_SysLog	Access	Allows the user to access this module's GUI.
	Edit	Allows the user to add, update, and delete connections.

Module	Privilege	Description
GW_SystemSummary	Access	Allows the user to access this module's GUI.

Module	Privilege	Description
GW_SysVista	Access	Allows the user to access this module's GUI.

Table 8.1 – Module Privileges (cont.)

Module	Privilege	Description
GW_Trigger	Access	Allows the user to access this module's GUI.

Module	Privilege	Description
GW_Trio	Access	Allows the user to access this module's GUI.
	Add	Allows the user to add new records via the various GW_Trio data entry windows.
	Edit	Allows the user to edit records via the various GW_Trio data entry windows.
	Delete	Allows the user to delete records via the various GW_Trio data entry windows.
	Post	Allows the user to perform other operations that affect billing such as posting documents, running invoices, etc.

Table 8.1 – Module Privileges (cont.)

*You will see Role Privilege options for these features even if you are not licensed for these features.



The Edit privilege is required to commit changes within the module. A user without this privilege may be able to change values within a module; however, they will not be able to save them. If a module does not have an Edit privilege, the Access privilege will allow updates.

Security for Windows Authentication

If you are using Windows Authentication for your GenWatch3 logins, make sure to read the *Staging for Windows Authentication* section of this document before setting up roles and users in GW_Security.

Roles

Roles are used to describe and house a set of privileges. A role is assigned to a user. This assigns the role's privileges to the user. Typical roles include:

- **Dispatcher:** User has access to all real-time activity GUIs, but no configuration GUIs.
- **Reporter:** User only has access to the GW_Reports module.

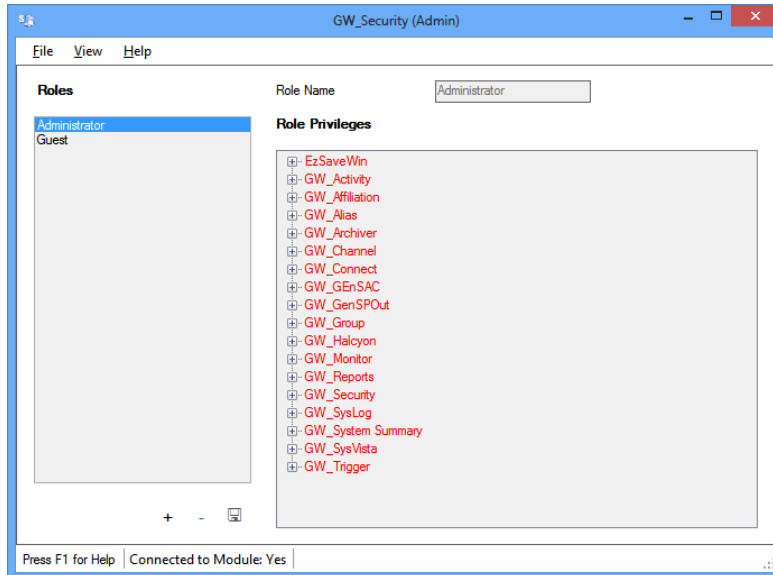


Figure 8.2 – GW_Security User Management GUI



The modules that appear in the *Role Privileges* list are determined by the license used to activate the software and may differ from screenshots provided in this document.

Adding a New Role

To add a new role, you must be logged into GenWatch3 with a user that includes the *ManageRoles* privilege in its role. To add a new role, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Roles** on the **View** menu. This will show the role management section of the GW_Security GUI.
3. Click the **Add New** button. This will clear the **Role Name** box.
4. Enter a role name that is not already in use.
5. Under each module, check each **Role Privilege** you want to include in this role and uncheck any **Role Privilege** that you do not want included. Clicking the checkbox next to the module name will select and unselect all role privileges under the module.
6. Click the **Update** button.

Editing a Role

To edit an existing role, you must be logged into GenWatch3 with a user that includes the *ManageRoles* privilege in its role. To edit an existing role, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Roles** on the **View** menu. This will show the role management section of the GW_Security GUI.
3. Click on the role in the **Roles** list that you wish to edit.
4. Change the **Privileges** assigned to this role.
5. Click the **Update** button.

Deleting a Role

To delete an existing role, you must be logged into GenWatch3 with a user that includes the *ManageRoles* privilege in its role. Roles can only be deleted if they are not assigned to a user. To delete an existing role, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Roles** on the **View** menu. This will show the role management section of the GW_Security GUI.
3. Click on the role in the *Roles* list that you wish to delete.
4. Click the **Remove** Button or right-click on the role in the *Roles* list that you wish to delete to show a menu of role options, including **Remove**. This will result in a confirmation dialog.
5. Click **Yes** to remove the role.



If a user does not have the GW_Security *ManageRoles* privilege, the user can view the privileges of his/her own role but not the privileges of any other roles.



Role names cannot begin or end with a space and each character must be in the range of ASCII 0-255, excluding the following characters:
/ \ [] ; | = + * ? < > " , @ { } () . ' ` & % \$!

Users

Users define the people that use the GenWatch3 software. Users are assigned a role and a list of groups, agencies and sites which they can view (unconditional access to all groups, agencies and sites are privileges). You provide a username when you log into GenWatch3 GW_LaunchPad. This username is passed to each of the GenWatch3 GUIs as it is loaded. Each GUI examines the privileges assigned to the user's role to determine the view and edit rights for the given user. Based on these privileges, the GenWatch3 GUI will limit the data and functions for the user.

Changes to user privileges are recognized by the GenWatch3 GUIs in real time. If you are logged into a GUI with edit privileges and across town the system administrator removes your edit privileges for your current GUI, you will notice some buttons disappear from your GUI. When a user has a GUI open and the

“Access” privilege is removed the module will not be closed; removing the access privilege prevents the user from opening the module in the future. Also, if Launchpad is open and the Access privilege is removed from one or more modules the icons will remain until Launchpad is closed and reopened or the user refreshes the modules list. The user will not be able to open the modules during this time without the Access privilege.

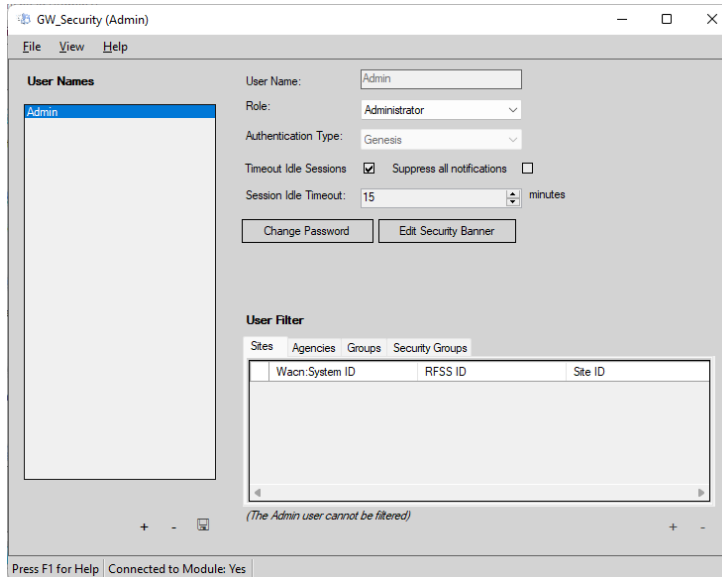


Figure 8.3 – GW_Security User Properties Window

The Administrator Role and Admin User

The GenWatch3 install includes the **Administrator** role and the **Admin** user. This role and user cannot be updated. This user and role represent the administrator user with the administrator role. This role has all privileges available in GenWatch3. The only attribute of this user and role that can be changed is the password.



Only **Administrator** role users can assign the **Administrator** role to other users. For non-**Administrator** role users, the **Administrator** role is not included in the Role list.

Adding a New User

To add a new user, you must be logged into GenWatch3 with a user that includes the *ManageUsers* privilege in its role. To add a new user, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Users** on the **View** menu. This will show the user management section of the GW_Security GUI.
3. Click the **Add New** button. This will clear and enable the **User Name** box and show the **Password** and **Confirm** boxes.
4. Enter a username that is not already in use.
5. Choose an **Authentication Type** to determine how the user logs into GenWatch3. To login with Windows authentication (i.e. current Windows

user authentication), choose Windows. To login with Genesis authentication (i.e. username and password authentication), choose Genesis.

6. Select a role from the **Role** list.
7. Choose a **Timeout Idle Sessions** option. If checked, this user is logged out after **Session Idle Timeout** minutes of inactivity within the GenWatch3 GUIs. Activity includes keyboard input or mouse movement/clicks.
8. If you checked the **Timeout Idle Sessions** option, enter a value for **Session Idle Timeout**. The minimum value is 5 minutes. The maximum value is 1,440 minutes (24 hours).
9. Choose a **Suppress all notifications** option. If checked, this user will not receive any notifications. See *Chapter 11 - GenWatch3 Notifications* for more information on the GenWatch3 Notification window.
10. Enter a password for this user in the **Password** box and the **Confirm** box.
11. If you would like for the user to only be able to see certain agencies, sites, groups or message types, modify this in the **User Filter** panel. (see the *User Filters* section below)
12. Click the **Update** button.



There is a limit on password length of 128 characters. Anything beyond this limit will be truncated automatically if pasted into the password field.



There are username and password length limitations for users intended to be used by RPC CADI client devices. Users created in GW_Security for RPC CADI devices that connect to a GW_Halcyon RPC CADI connection should follow these restrictions in order to connect to the RPC CADI connection:

1. For RPC CAD Version 1 connections, the username can be no longer than 9 characters.
2. For RPC CAD Version 2 and 3 connections, the username can be no longer than 49 characters.
3. For all three versions, the user's password can be no longer than 31 characters.

Editing a User

To edit an existing user, you must be logged into GenWatch3 with a user that includes the *ManageUsers* privilege in its role. To edit an existing user, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Users** on the **View** menu. This will show the user management section of the GW_Security GUI.
3. Click on the user in the *User Names* list that you wish to edit.
4. If you would like for the user to only be able to see certain groups or message types, modify this in the *User Filter* panel. (see the *User Filters* section below)
5. Click the **Update** button.



The *Authentication Type* option is not editable.

Changing a User's Password

This option is only available to users with an **Authentication Type** of Genesis.

To change a user's password, take the following steps:

1. Click on the user in the **User Names** list whose password you wish to change.
2. Click the **Change Password** button. This will show the *Change Password* window.
3. Enter the password for the current GenWatch3 user in the **Current Password for <username>** box.

4. Enter the user's new password in the **New Password for <username>** box and the **Confirm new password for <username>** box.
5. Press the **OK** button.



The GW_Security *ChangePassword* privilege is required to change another user's password. The logged-in user can change his/her own password without this privilege.



There is a limit on password length of 128 characters. Anything beyond this limit will be truncated automatically if pasted into the password field.

Deleting a User

To delete an existing user, you must be logged into GenWatch3 with a user that includes the *ManageUsers* privilege in its role. To delete an existing user, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Users** on the View menu. This will show the user management section of the GW_Security GUI.
3. Click on the user in the **User Name** list that you wish to delete.
4. Click the **Remove** Button or right-click on the role in the **User Names** list that you wish to delete to show a menu of role options, including **Remove**. This will result in a confirmation dialog.
5. Click **Yes** to remove the user.



Attempting to remove a user that has active processes in SQL Server may not be successful. In this instance the user will be disabled and will be grayed out in the Users → User Names list, the User Properties for the user will have a **Remove User** button and all other controls will be disabled.

User Filters

For users within roles that do not have the *ViewAllSites*, *ViewAllAgencies* and/or the *ViewAllGroups* privilege for each module, the resources that they can view are selected in the **User Filter** panel in the bottom right.



When licensed for a PMI Connection in the GW_Connect module, users can have the PMI resources they view limited with the Security Groups filter. This filter is only available when so licensed. Once GenWatch3 is connected to the PMI server, security groups can be assigned to a user. This filter only restricts resources within the AstroPMI windows within the GW_Trio module. A user's role can also have the GW_Trio PMI *ViewAllSecurityGroups* privilege to bypass filtering.

Adding Resources

To add resources to the **User Filter**:

- Click the **Add Filter Resources...** button. This will load the resource selector window.
- Enter search criteria and click the **Search...** button. This will populate the resource list.
- Select one or more resources by clicking the checkbox in the leftmost column. To select all resources in the list, click the **Select All** button. To unselect all resources in the list, click the **Unselect All** button.

- Click the **OK** button. This will close the resource selector window and populate the **User Filter** with the selected resources.
- Click the **User Update** button on the *User Properties* panel. This will save the **User Filter** changes.

Removing Resources

To remove resources from the **User Filter**:

- Select the resources in the **User Filter**. Use Shift + Click to select a range. Use Ctrl + Click to select additional resources.
 - This is standard windows functionality
- Clicking the **Remove Filter Resources...** button. This results in a confirmation dialog.
- Click **Yes** on the confirmation dialog. This will remove the selected resources.
- Click the **User Update** button on the *User Properties* panel. This will save the **User Filter** changes.

If you scroll to the right in the **Groups** tab of the **User Filter** panel, you will see a list of checkboxes for different kinds of radio events. A user can also be filtered from seeing certain kinds of messages by unchecking these boxes. **PTT Display, Affiliation, Emergency Alarm, Call Alert, Change Me, Message, Radio Ack, Status, Snapshot Response, Aff Download Status, and Config Info** can all be toggled. In this version of GenWatch3, these options only affect event delivery in the RPC connection in GW_Halcyon.

Editing the Security Warning Banner

The GW_Security GUI allows an administrator to create or edit a security warning banner to be displayed every time a GenWatch3 user logs in. When the security warning banner is enabled, all users must click a button indicating they agree to the terms defined in the customized banner before they can log in. When disabled, the banner will not be displayed during login attempts.

To edit, enable or disable the security warning banner, take the following steps:

1. Load the GW_Security GUI while logged into GenWatch3 as a user with the GW_Security *Administrator* privilege.
2. Click the **Users** option in the **View** menu. This will show the **User Properties** section of the GW_Security GUI.
3. Click the **Edit Security Banner** button. This will show the *Edit Security Warning Banner* window.
4. Enter text into the **Header** field. This will be used as the title of the window that displays the security warning banner.
5. Enter the text of your banner into the **Security Warning Banner Text** field. Several basic text formatting tools are provided to change the font, font size, alignment, etc. The field will also preserve formatting if the text is copied and pasted in from a word processor or other rich text editing application.

-
- The screenshot shows a Windows-style dialog box titled "Edit Security Warning Banner". It has a blue title bar with standard window controls. The main area contains three text input fields: "Header:" with the value "SECURITY AGREEMENT", "Security Warning Banner Text:" containing several paragraphs of placeholder security text, and "Footer:" which is currently empty. Below the text areas are two checkboxes: "Enable Security Warning Banner" (which is checked) and "Show Security Warning Banner On Logon" (which is unchecked). At the bottom are three buttons: "Preview", "OK", and "Cancel".
- Edit Security Warning Banner
- Header: SECURITY AGREEMENT
- Security Warning Banner Text:
- You are accessing an application that is provided for MyCompany-authorized use only.
- By using this application (which includes any device attached to this application), you consent to the following conditions:
- You are responsible for maintaining the confidentiality of your account and password and for restricting access to your computer, and you agree to accept responsibility for all activities that occur under your account or password. MyCompany routinely intercepts and monitors communications on this application for purposes including, but not limited to, penetration testing, security monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, MyCompany may inspect and seize data stored on this application and database.
- ☒ Enable Security Warning Banner
- ☐ Show Security Warning Banner On Logon
- Preview OK Cancel

Activity History

- **Timestamp:** The date and time the activity occurred.
- **Description:** Full description of the activity.
- **Module:** The GenWatch3 GUI in which the activity occurred.
- **Computer Name:** The computer name on which the activity occurred.

To view user activity for other users, you must be logged into GenWatch3 with a user that includes the *ViewUserActivity* privilege in its role. Only users with the Administrator role will be able to see the activity of other users with the Administrator role. Follow the steps below to view user activity:

1. Load the GW_Security GUI.
2. Select **History** on the **View** menu. This will show the user activity section of the GW_Security GUI.
3. Select the user for which you want to view activity. This will show the activity for this user for the past 30 days in the *User Activity* list to the right of the *User Names* list.

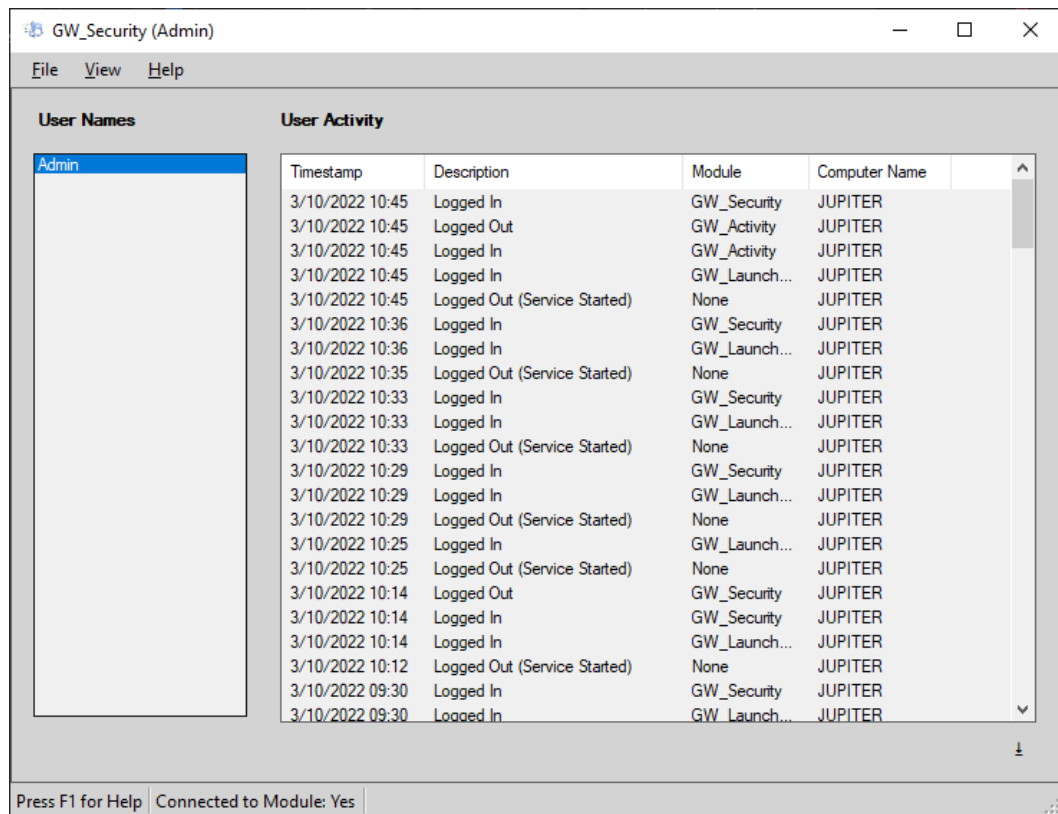


Figure 8.5 – GW_Security Activity History Window

A user's activity history can be exported by clicking the **Export** button.

Login History Snapshot

Each time you log into GenWatch3, GW_Alert will show the last time your user logged in and any failed login attempts between now and your last successful login attempt. This information is also available in the GW_Security Activity History window.

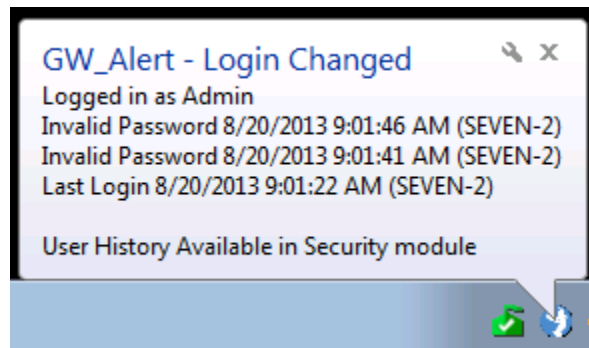


Figure 8.6 – Login History Snapshot



Notifications must be enabled in Windows for this information to appear.

Current Users

GenWatch3 monitors user information for each user. This information allows you to view the current user information for each user. This information includes the following per user:

- **User Name:** The name of the user.
- **Role:** The role of the user.
- **Logged In:** Shows if the user is currently logged into GW_Alerts.
- **Last Location:** The computer on which this user logged in most recently.
- **Last Activity:** The date and time this user performed one of the following actions:
 - Logging into a GenWatch3 module GUI.
 - Logged out from a GenWatch3 module GUI.
 - Perform an administrative function such as adding an input module connection.
 - When a user is denied access to a GenWatch3 module GUI due to security denial.

Please refer to the **Activity History** for this user to view the details of the last activity entry.

This window does not refresh automatically. To retrieve up-to-date information, click the **Refresh** button.

To export the list of users, click the **Export** button.

To view current login states for other users, you must be logged into GenWatch3 with a user that includes the *ViewCurrentUsers* privilege in its role. Only users with the Administrator role will be able to see other users with the Administrator role. Follow the steps below to view current login states:

1. Load the GW_Security GUI.
2. Select **Current Users** on the **View** menu. This will show the *Current Users* section of the GW_Security GUI.

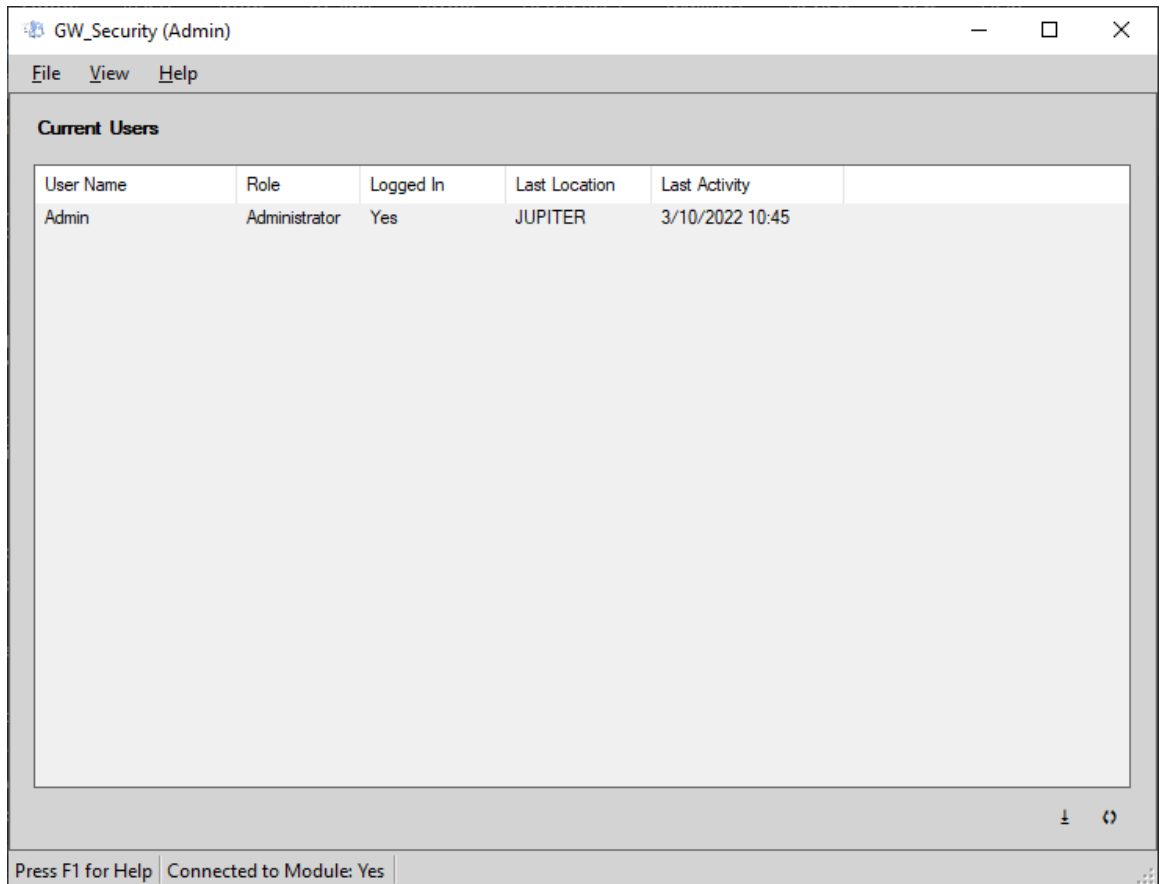


Figure 8.7 – GW_Security Current Users Window



If the GenWatch3 software closes unexpectedly, the currently logged-in user will appear to be logged in until the next time they successfully log out.

Logging Out a User

To log out a logged-in GenWatch3 user, you must be logged into GenWatch3 with a user that includes the *ManageUsers* privilege in its role. To log out a logged-in user, follow the steps below:

1. Load the GW_Security GUI.
2. Select **Current Users** on the **View** menu. This will show the current user information section of the GW_Security GUI.
3. Click on the user in the *Current Users* list that you wish to log out. Only users that are logged in can be logged out.

4. Right-click on the user in the *User Name* List.
5. Click the **Log Out this User** option. This will result in a confirmation dialog.
6. Click **Yes** to log out the user.



The Admin user cannot be logged out.

This chapter contains the following sections:

- **What is GW_SysLog?:** Describes the role of GW_SysLog within GenWatch3.
- **SysLog Packets:** Defines the structure of a SysLog packet.
- **SysLog Connections:** Describes the role of SysLog connections.

What is GW_SysLog?

GW_SysLog manages SysLog connections. The GW_SysLog module routes events and notifications created by the GenWatch3 service and modules to each of these SysLog connections.

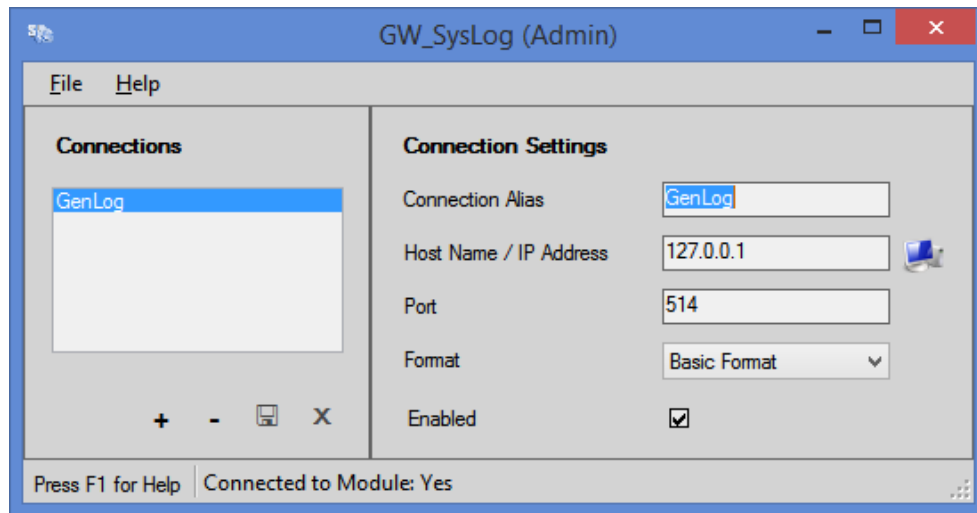


Figure 9.1 – SysLog GUI



SysLog: A de facto standard for forwarding log messages in an IP network. There are several 3rd party applications (sold by vendors other than The Genesis Group) that can receive, process, store, and issue alarms based on SysLog packets.

SysLog Packets

SysLog is an event format that has been the standard in the UNIX world for many years. SysLog packets are basically ASCII text (letters and numbers), limited to 1024 characters, in which the information in the text follows the SysLog format. Some information in SysLog packets is optional, such as date and time. The SysLog packets sent by the GenWatch3 GW_SysLog module can have one of the following formats:

Format	Description
Basic	<PRI> Message
RFC 3164	<PRI>[Mmm dd hh:mm:ss] [HOSTNAME] [Message]
RFC 5424	<PRI>[YYYY-MM-DD"T"hh:mm:ss.###-hh:mm] [HOSTNAME] [APPNAME] [PROCID] [MSGID (just a dash)] [Message]

The PRI is a numeric value that stores both the message facility (Local7 is always used within GenWatch3) and the severity. To determine the value for facility and severity, divide the PRI value by 8. The quotient is the facility, and the remainder is the severity.

SysLog PRI Facility Values

Value	Description
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages (note 1)
5	messages generated internally by SysLog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon (note 2)
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7) ← Value used by GenWatch3 GW_SysLog module

SysLog PRI Severity Values

Value	Description
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages



SysLog Connections

The **Connections** list on the left side of the SysLog GUI shows all current SysLog connections. GW_SysLog broadcasts each SysLog packet that it receives to each SysLog connection. These connections use unencrypted UDP (*universal datagram packet*) protocol, so the message is sent to the destination (Host Name / IP Address and port) even if the destination is not listening. There are many SysLog client applications on the market that allow you to:

- Monitor SysLog activity on a destination.
- Log the packets to file, database, etc.
- Send out e-mail messages, page a person, or trigger another event when a certain severity level is received.
- Route the packets to another location.
- Many more options.


Creating a SysLog Connection

To create a SysLog connection, take the following steps:

1. Click the  button. This will result in a new item being added to the **Connections** List. The new item will have an alias like “New Connection 1”.
2. Click on the new entry in the **Connections** list. This will show the settings for this connection in the **Connection Settings** section.
3. Enter a value for **Connection Alias**.
4. Enter a value for **Host Name / IP Address**. This value can be any value that can be successfully resolved via DNS (Directory Name Service). Both computer names and IP addresses work. Notice that the default value is 127.0.0.1. This value is the IP address of the local machine.
5. Enter a value for **Port**. Port 514 is the standard SysLog port.
6. Check the **Enabled** checkbox.
7. Click the  button.


Deleting a SysLog Connection

To delete a SysLog connection, take the following steps:

1. Select the connection that you wish to delete in the **Connections** list.
2. Click on the  button. This will result in a confirmation message.
3. Click **Yes**.

Disabling a SysLog Connection

If you wish to keep a SysLog connection in place without sending packets to the connection, you can disable the connection. To disable a connection, take the following steps:

1. Select the connection that you wish to disable in the **Connections** list.
2. Uncheck the **Enabled** checkbox.
3. Click the  button.

This chapter contains the following sections:

- **What is GW_WebServer?:** Describes the role of GW_WebServer within GenWatch3.
- **Web Server Configuration:** Defines how the GW_WebServer module is configured.
- **Web Server Request Types:** Describes the types of requests the GW_WebServer handles.

What is GW_WebServer?

GW_WebServer manages incoming web requests to GenWatch3. The GW_WebServer module routes these requests to the appropriate module in GenWatch3 and sends the responses back to the client making the request.

The GW_WebServer module does not have a GUI.

Web Server Configuration

The GW_WebServer module has three settings that can be configured. Due to their nature they cannot be changed via a GUI and require the GenWatch3 service to be restarted at a minimum. These settings are:

- **Port:** The web server port is configured during the installation/configuration of the GenWatch3 host via the REST API port portion of the configuration. Due to its nature of configuring the host's firewall along with endpoint reservations, changing the port can only be done during this configuration of the host.
- **Request Logging:** Enabling Request Logging allows all requests made of the web server to be logged. Doing so can result in very large log files over the course of a day and as such is disabled by default. Genesis Support may instruct this to be enabled temporarily to troubleshoot web server issues. This setting is changed by setting the *RestApiRequestLogging* setting in the service's *GenWatch3.config* file on the host. It requires the GenWatch3 service to be restarted to take a change into effect.
- **Verbose Logging:** In conjunction with the above logging setting, this will additionally log the body of each request and response. This results in even larger log files and should be enabled temporarily only when instructed by Genesis Support. This setting is changed by setting the *RestApiVerboseLogging* setting in the service's *GenWatch3.config* file on the host. It requires the GenWatch3 service to be restarted to take a change into effect.

Web Server Request Types

The GW_WebServer module handles three main types of requests. These are:

- **Statistics:** Specific statistics are available via the appropriate request mainly to drive various features used by GenWatch3 iVista.
- **Alias Management:** To integrate with GenWatch3 iVista, various Alias related requests are made to get, update, and retrieve alias information for resources managed by the GW_Alias module.
- **Client Updates:** GenWatch3 clients at version 2.15 or greater can be automatically updated after the host is upgraded. The web server handles these requests and allows the clients to download the client installer from the host itself. An update can be initiated by logging into the host from a client. The client will detect a new version is available and guide the user through the update process.
- **Client Installs:** Along with updates above, new clients can easily be installed with minimal effort. Using a web browser on any computer needing a GenWatch3 client installed, navigate to a URL such as the following:

<https://{host}:{port}/GenWatch3/ClientInstaller/>

Just replace {host} with the hostname or IP of the GenWatch3 host machine. Also replace {port} with the REST API Client TCP port configured during the installation/configuration of the GenWatch3 host. This will display a page describing the requirements and process for installing a client.

This chapter contains the following sections:

- **What is a Notification?:** Describes the role of notifications within GenWatch3.
- **What Do Notifications Mean to Me?:** Explains why notifications are important to the GenWatch3 user.
- **Working with Notifications:** Describes the process of dealing with notifications.

What is a Notification?

A notification is sent to GenWatch3 users when certain events happen on the system. Some events only target users with the *GW_Security Administrator* privilege while some target all users. These events are like those available in the *GW_Trigger* module. They use the same core GenWatch3 notification process, minus the archiving of notifications, external relays, and responsibility logic.

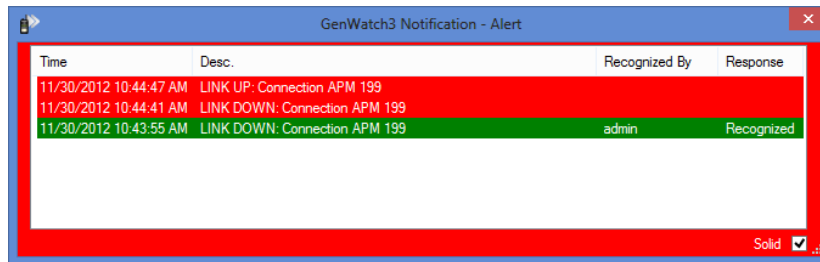


Figure 11.1 – GenWatch3 Notification Window

Above is an example of the *GenWatch3 Notification* window. We have received several notifications concerning our input connection to a data stream. The newest notification is at the top. The topmost notification is “Link Up.” This tells us that we lost the data stream a couple of times within a few seconds. In the end, the data stream was back up.



If the message description is longer than what will fit in the Desc. column, you can move and rest your mouse over the Desc. column.



Notifications will not display to a user if the **Suppress all notifications** option is checked for that user in *GW_Security*.

GenWatch3 sends the following notifications:

Type	Source	Targets
Existing talkgroup reported by data stream as a multigroup	GW_Alias	Administrator
New Suspect Notification	GW_SAM	Administrator
Link Down Notification	Data stream input modules	All Connected Users
Link Up Notification	Data stream input modules	All Connected Users

What Do Notifications Mean to Me?

Notifications are provided for two reasons:

1. To inform users of the status of the data stream, as it goes up and down. This notification will prompt administrators to attempt to restore the connection and will let other users know why they are not receiving real-time data. As a user or administrator, these notifications are useful.
2. To inform administrators of a data entry issue regarding groups. This allows the administrators to be proactive in correcting these issues. As an administrator, these notifications are useful.
3. GW_Trigger trigger rule violations. Some trigger events (set up in the GW_Trigger module) include showing a GenWatch3 Notification window (for additional warning that the trigger event occurred). Sometimes a sound will play, or a relay will remain open until a user clicks on the trigger event in the GenWatch3 Notification window, therefore incorporating the GenWatch3 Notification window into the trigger event's workflow.

Working with Notifications

When a module issues a notification, a *GenWatch3 Notification* window will appear. When you select the event in the list, it will respond to the event. This means that all GenWatch3 users (including you) will see your username in the **Recognized By** column and the **Response** column will read Recognized.

When the *GenWatch3 Notification* window opens, it normally appears in the same position it was in when the current user closed it. However, because the *GenWatch3 Notification* window contains important information, it will always attempt to appear in a location where the entire window is visible to the user and, if possible, where the window fits on one monitor.

This chapter contains the following sections:

- **What is Automatic Purging?:** Describes the need and function of the automatic purging operation within GenWatch3.
- **Automatic Purge Settings:** Describes the settings used for automatic purging by GenWatch3.
- **Viewing Purging Results:** Describes how you can view the results of the automatic purging operation.

What is Automatic Purging?

GenWatch3 continually logs activity. If left unchecked, these activities would eventually take up a large amount of database space and decrease GenWatch3's performance. To avoid this issue, GenWatch3 performs an automatic purging operation every night at 12:00 AM. The type of purging is defined in the automatic purge settings.

Automatic Purge Settings

The automatic purge settings are defined in the **Purge** table in the **GW** database. The **Purge** table contains the following settings for each automatic purging operation:

- **ID:** Unique identifier for this automatic purging operation.
- **GWModuleID:** ID of the module responsible for performing this automatic purging operation. This value references a row in the **GW_Modules** table.
- **TableName:** Name of the table to purge.
- **DateAgeDays:** Number of days before an activity is purged.
- **MaxRows:** Maximum number of rows allowed in the table.
- **ByAge:** 0 if this table is not purged by age. 1 if this table is purged by age. Each **DateTime** column in this table is checked for a date older than **DateAgeDays** days. If one or more **DateTime** values are older than **DateAgeDays**, then the activity is purged.
- **ByRows:** 0 if this table is not purged by maximum number of rows. 1 if this table is purged by maximum number of rows. Each activity in excess of **MaxRows** is purged.

The **ByAge** and **ByRows** options are not mutually exclusive. A table can be purged with both the **ByAge** and **ByRows** options. In this case, the **ByAge**-based purging occurs first, followed by the **ByRows**-based purging.

Viewing Purging Results

The automatic purging results are reported in the Windows Event log if the purging operation removes one or more activities. See the *GenWatch3 Service Diagnostics* section of *Chapter 3 - GenWatch3 Service* for instructions on viewing the Windows Event log.