GenWatch3®
Installation & Quickstart Guide
Software Version 2.23.5

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

Trademarks

The following are registered trademarks of Motorola: SmartZone, SmartNet, 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

Includes technology licensed from Motorola.

Disclaimer

The GenWatch3 Installation & Quickstart Guide 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
2.0.1	Initial Release	JAW
2.0.3	Revision before release	JAW
2.0.3	Updated installation screens	KIH
2.0.4	Release Revisions	KIH
2.0.4	Updated Remote DB instructions	KIH
2.0.5	Proofreading/Editing	JWR
2.0.6	Updated screenshots for F1 Help	REB
2.0.6	Added Firewall settings section	JAW
2.0.6.6	Revision before release	KIH
2.2	Addition to Firewall Settings section	CWF
2.2	Document Reviewed	WRK
2.3	Revisions before release	CWF
2.4	Revisions before release	WRK
2.5	Revisions before release	CWF
2.5	Added Remote Database Configuration	KIH
2.5	Updated Master Agent Service Settings screen	KIH
2.5	Added Service Account Change Warning	KIH
2.5	Changed Screenshot in SNMP Setup	KIH
2.5	Updated Master Agent Service Configuration	KIH
2.5	Add SQL/SNMP Integration Warning	KIH
2.6	Added Change Service Account Section	KIH
2.6	Revisions Before Release	CWF
2.7	Revisions Before Release	JAW
2.8	Revisions Before Release	WRK
2.8	Advanced Client Setup Section Added	CWF
2.9	Revisions Before Release	ATG
2.10	Revisions Before Release	ATG
2.11	Revisions Before Release	ATG
2.11	Removed "With Grant" option from permissions.	REB
2.12	Revisions Before Release	ATG
2.12	Added Client Upgrade Section	SC
2.13	Revisions Before Release	ATG
2.14	Revisions Before Release	JAW
2.15	Revisions Before Release	ATG
2.16	Revisions Before Release	JPS
2.17	Update hyperlinks	DW
2.17.17	Added GET SNMP option	ATG

Table of Contents

About this Manual

Goals

This document guides you through the GenWatch3 installation and initial setup process. After you complete the steps in this document, you will be ready to configure the input module(s) that GenWatch3 will use to communicate with your system(s).

Who Should Read This Manual?

This document is written for an audience with an understanding of computer and network administration. Specifically, anyone performing an initial installation of GenWatch3 should read this manual.

How This Manual Is Organized

This manual is organized as follows:

- **Installing GenWatch3:** Describes the process of installing GenWatch3.
- **Getting Started:** Instructions on logging into GW_Alert and beginning the GenWatch3 evaluation.
- **Configuring the GW_Security Module:** Instructions on changing the *Admin* login password.
- **Configuring the GW_Archiver Module:** Instructions on setting up data archiving for reporting and historical data.

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

ℹ **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.

Chapter 1 Installing GenWatch3

This chapter contains the following sections:

- **Warnings**: Provides some warnings about GenWatch3 configurations.
- **Minimum Hardware Specifications**: Describes where to find the hardware configuration required to support a GenWatch3 installation.
- **Hardware Enhancement Options**: Describes additional hardware options.
- **GenWatch3 Software Install**: Provides detailed instructions for installing and licensing the GenWatch3 software.
- **Firewall Configuration**: Describes the proper setup of the Windows firewall.
- **Advanced Client Setup**: Describes the proper setup of clients in a multi-domain environment.
- **Audit Logging**: Describes the audit logging in SQL Server.

Warnings

❌ If you wish to use SQL Server's SNMP integration functionality, you must install Windows SNMP components before SQL Server.

❌ You must install the full version of Microsoft SQL Server on the host machine in order to create a host/client install. SQL Server Express DOES NOT support remote user connectivity on its databases. The full version of Microsoft SQL Server DOES support remote user connectivity.

❌ SQL Server® Standard is recommended for users that wish to archive data and run daily reports. GenWatch3 is shipped with a freeware version of Microsoft SQL Server (SQL Server Express). SQL Server Express is limited by maximum size of 10 GB of archived data. When the maximum size is reached, the database will not be updated with new records and may stop functioning.

❌ The GenWatch3 machine must use an English-language version of Microsoft Windows.

❌ The GenWatch3 machine must not use a comma as a decimal symbol in the Number Format under Regional Settings.

❌ The GenWatch3 machine must not use hyphens in the Date Format under Regional Settings.

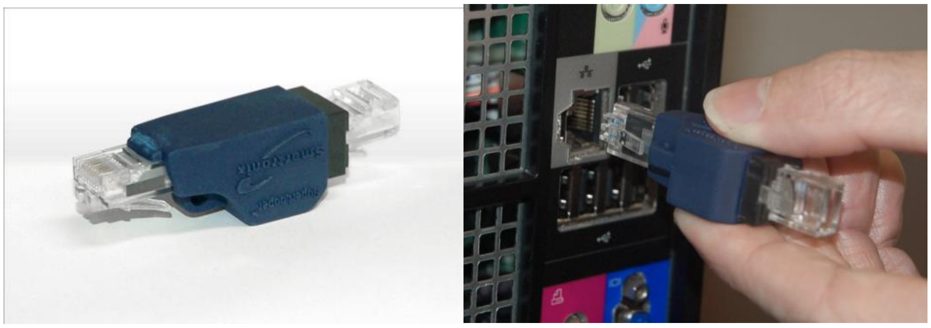
❌ The GenWatch3 machine (client or host) must be a member of a Microsoft Windows network. GenWatch3 relies on DNS resolution for the TCP/IP and SQL connections that it uses. If the machine running GenWatch3 is not a member of a network, the GenWatch3 software will not function properly unless you follow the instructions below.

❌ If you change the name of the GenWatch3 host computer, you must restart the GenWatch3 service.

❌ The GenWatch3 service must always be running. Please disable hibernation on the host machine.

Using GenWatch3 Without a Network

If you wish to use GenWatch3 on a machine that is not connected to a network, you must install a loopback adaptor. A hardware loopback adaptor has been included with your GenWatch3 host machine. Connect the adaptor to the machine's Ethernet port as shown below.



The Microsoft KM-TEST Loopback Adapter can be installed if a hardware adaptor is not available. To install this software loopback adapter, follow the steps below.

Windows 10

1. Click **Start**.
2. Search for *hdwwiz*.
3. Right click *hdwwiz* and select **Run as Administrator** (click **Yes** if a confirmation dialog appears).
4. This will launch the *Add Hardware Wizard*.
5. Click **Next**.
6. Select the **Install the hardware that I manually selected from a list (Advanced)** option.
7. Click **Next**.
8. Select **Network adapters** from the **Common hardware types** list.
9. Click **Next**.
10. Under the **Manufacturer** list, select **Microsoft**.
11. Under the **Network Adapter** list, select **Microsoft KM-TEST Loopback Adapter**.
12. Click **Next**.
13. On the next window, confirm that **Microsoft KM-TEST Loopback Adaper** is the hardware selected to be installed.
14. Click **Next** to start the installation.
15. Click **Finish** to complete the process and close the **Add Hardware Wizard**.

Minimum Hardware Specifications

See https://genesisworld.com/resources/

Hardware Enhancement Options

There is no such thing as *too much power*. The following hardware options will improve the performance of GenWatch3:

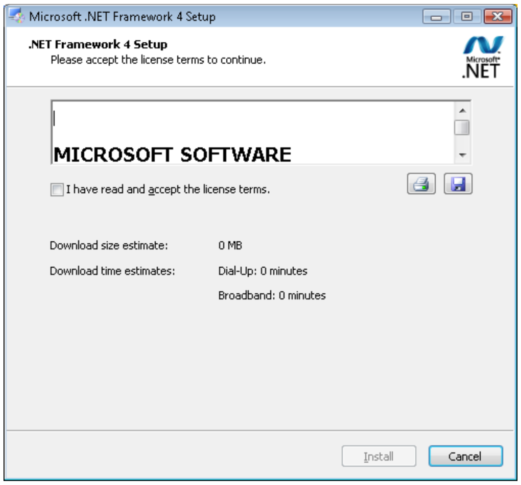
- **Increase the hard drive speed:** When archiving or reporting on a great deal of data, the hard drive will sometimes become the bottleneck of the system. This can lead to the processor waiting on the hard drive.
- **Increase the memory (RAM):** When GenWatch3 is processing data on a system with thousands of radio IDs and talkgroups, it uses a lot of memory. If your machine needs more memory than is available, it will begin using the swap file on the hard disk to store data that should be in memory. Because the hard drive operates at a speed that is up to 1000 times slower than memory, it is important to avoid hard drive swapping.
- **Increase the processor speed:** If your machine has a high-performance hard drive and plenty of memory, increasing the processor will increase the performance of the machine.

GenWatch3 Software Install

To begin the software installation process, insert (if on DVD or USB) or browse to the GenWatch3 installation media. If the GenWatch3 setup program does not launch automatically, browse to the installation media's root directory and double-click on *Start.hta*.

Required Software

In order to support GenWatch3, Microsoft's .NET Framework 4.8 or later must be installed on your computer. If it is not already installed, you will see a window similar to the one shown in Figure 1.1. Click **Install** to begin installing .NET Framework.



.NET Framework 4 Setup

Please accept the license terms to continue.

MICROSOFT SOFTWARE

□ I have read and accept the license terms.

Download size estimate: 0 MB

Download time estimates: Dial-Up: 0 minutes

Broadband: 0 minutes

Figure 1.1 – .NET Framework Installer.

GenWatch3 requires Microsoft SQL Server be installed on this computer or another computer on the network. Standard Edition or higher is required for remote database installations. For local database installations, if SQL Server is not already installed on this computer, SQL Server Express will be installed during the GenWatch3 installation process.

Preparing to Install

After the .NET Framework is installed, the **GenWatch3 Installer** will launch. The *Welcome* screen in Figure 1.2 allows you to begin the installation process or launch any of the installation guides included in the GenWatch3 installation media.

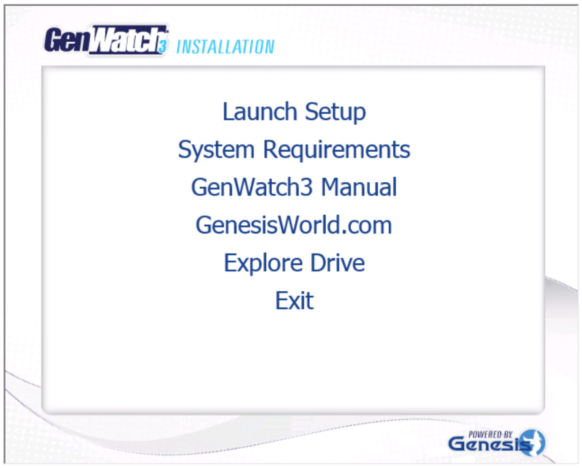


Figure 1.2 – GenWatch3 *Welcome* screen

When you click **Launch Setup**, the GenWatch3 setup process will begin.

The installation of any prerequisite components may require you to restart your computer. After a restart, the installer should resume the setup process automatically. If it does not, browse to the GenWatch3 installation media's root directory and double-click on *Start.hta*.

Install Screens

Installation screen

On the *Installation* screen, select to install software or database only.

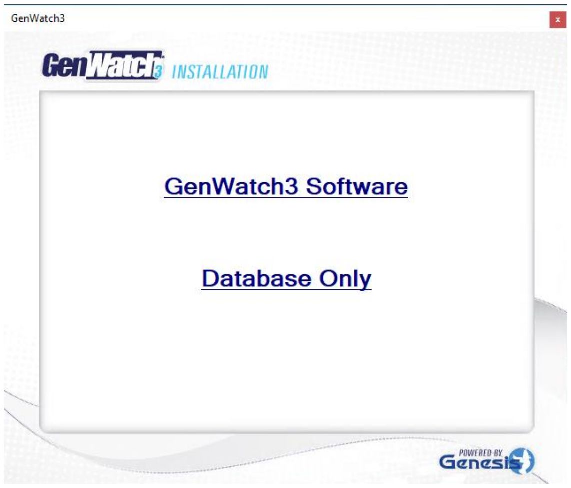
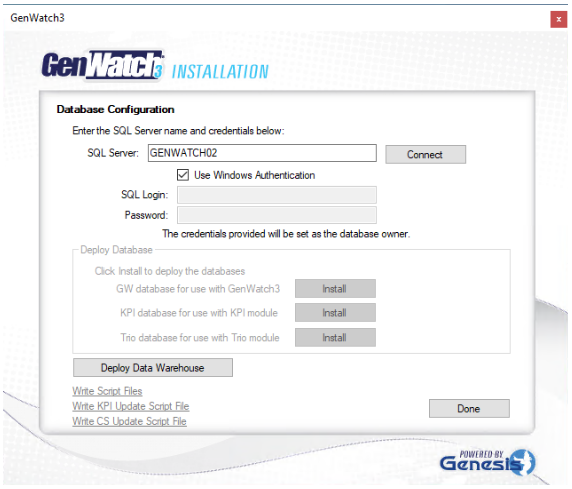


Figure 1.3 – *Installation* Screen

Database Only Screen

If you select **Database Only** on the *Installation* screen, you will see the *Database Only* screen (Figure 1.4). This screen allows you to deploy GenWatch3 related databases only. It will not install the application itself.



Database Configuration

Enter the SQL Server name and credentials below:

SQL Server: GENWATCH02

☑ Use Windows Authentication

SQL Login:

Password:

The credentials provided will be set as the database owner.

Deploy Database

Click Install to deploy the databases

GW database for use with GenWatch3

KPI database for use with KPI module

Trio database for use with Trio module

Figure 1.4 – *Database Only* Screen

- **SQL Server:** The SQL Server instance where the database(s) should be installed.
- **Use Windows Authentication:** Use the current Windows user to connect to the SQL Server instance.
- **SQL Login/Password:** The SQL user credentials to connect to the SQL Server instance if **Use Windows Authentication** will not be used.

1. Click **Connect** to connect to the specified SQL Server.
    a. Once the connection is validated and successful, you will be able to deploy the database(s).
2. Click **Install** next to the desired database to deploy it.
3. Repeat for each desired database.

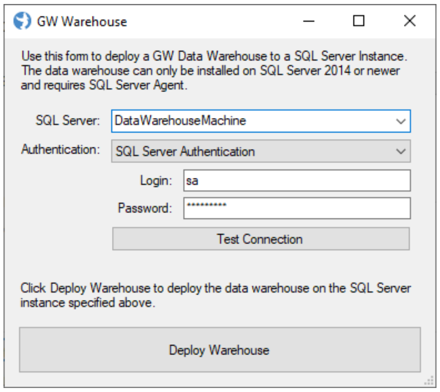
If you wish to manually create or update the GenWatch3 databases, you may access the database script files directly via the **Write Script Files** link. To manually update an existing KPI database, use the **Write KPI Update Script File** link. To manually add Configuration Services to an existing GW database, use the **Write CS Update Script File** link.

GW Warehouse Screen

Clicking **Deploy Data Warehouse** on the *Database Only* screen will show the *GW Warehouse* screen (Figure 1.5).

The GW Warehouse is a database used for long term storage and reporting on deployments in which the call volume prohibits reporting directly from the primary GW database.

1. Select a SQL Server for the warehouse – This should be a SQL Server running on a separate machine from the primary GW database.
2. Provide Administrative level credentials to the selected SQL Server.
3. Click **Test Connection** – The connection is tested and validated. If the SQL Server is not valid for warehouse installation the reason is displayed.
4. Click **Deploy Warehouse** – The warehouse is deployed to the SQL Server.



Use this form to deploy a GW Data Warehouse to a SQL Server Instance. The data warehouse can only be installed on SQL Server 2014 or newer and requires SQL Server Agent.

SQL Server: DataWarehouseMachine

Authentication: SQL Server Authentication

Login: sa

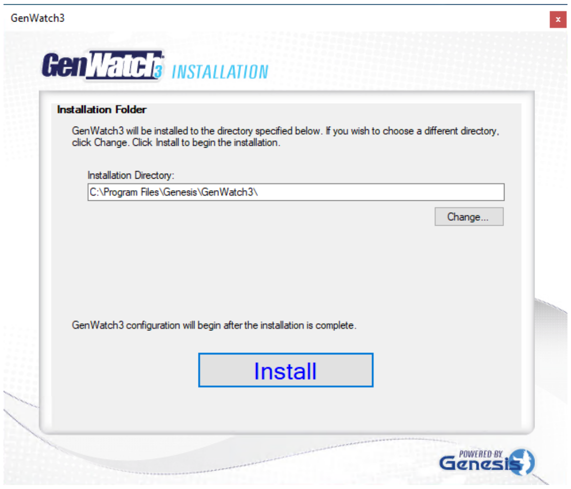
Password: *********

Click Deploy Warehouse to deploy the data warehouse on the SQL Server instance specified above.

Figure 1.5 – *GW Warehouse* screen

Installation Folder Screen

If you select **GenWatch3 Software** on the *Installation* screen, you will see the *Installation Folder* screen (Figure 1.6). On this screen, you can choose the directory where the GenWatch3 application files will be installed.



GenWatch3 will be installed to the directory specified below. If you wish to choose a different directory, click Change. Click Install to begin the installation.

Installation Directory:
C:\Program Files\Genesis\GenWatch3\

GenWatch3 configuration will begin after the installation is complete.

Figure 1.6 – *Installation Folder* Screen

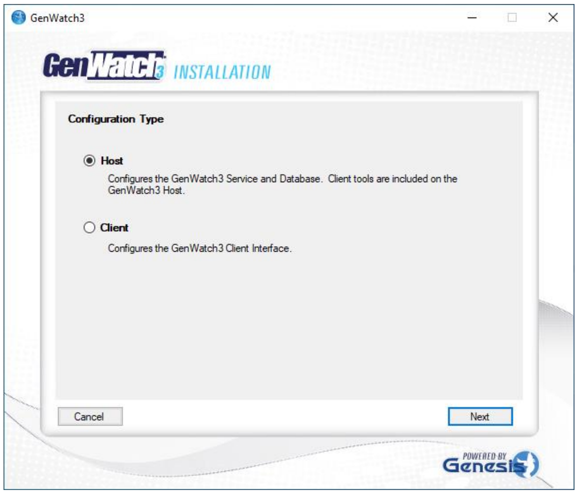
Click **Install** to install the GenWatch application files to the chosen directory. You will see a progress bar as GenWatch3 is installed. Once complete, you will be able to configure the installation and the *Setup Type* screen will be shown.

Configuration Screens

Setup Type Screen

At the *Setup Type* screen (Figure 1.7) choose the type of GenWatch3 configuration you wish to perform: **Host** or **Client**.

Click **Next** to continue.



Configuration Type

● Host

Configures the GenWatch3 Service and Database. Client tools are included on the GenWatch3 Host.

○ Client

Configures the GenWatch3 Client Interface.

Figure 1.7 – *Setup Type* screen

- **Host:** Select **Host** to install the GenWatch3 service and the GenWatch3 interfaces. If GenWatch3 will be installed on one machine, select **Host**.
- **Client:** Select **Client** to install only the GenWatch3 interfaces. These are used to display information processed and stored by a GenWatch3 host.

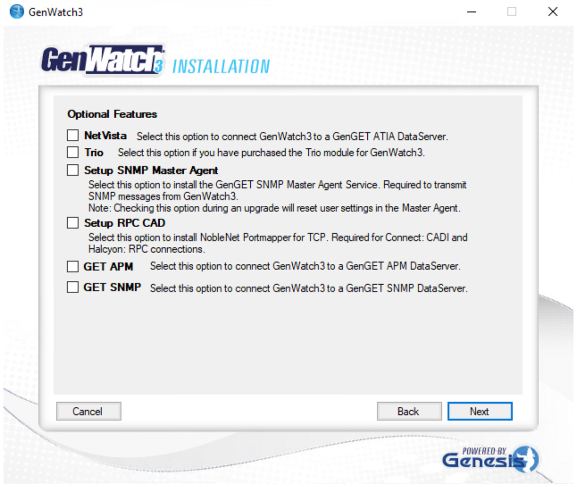
Optional Features

At the *Optional Features* screen (Figure 1.8) review the available features and select those you wish to enable.

Additional features:

- **NetVista:** This option should be selected only if GenGET ATIA is also installed. Selecting this option will enable the *GenGET Database Options* screen.
- **Trio:** This option should be selected if the Trio module has been purchased to use on this GenWatch3 installation.
- **Setup SNMP Master Agent:** This option should be selected if this GenWatch3 installation needs to be able to send SNMP messages. Selecting this option will enable the *GET SNMP Master Agent Options* screen.
- **Setup RPC CAD:** This option is required for GW_Connect: CADI and GW_Halcyon: RPC connections to function correctly.
- **GET APM:** This option should be selected only if GenGET APM is also installed. Selecting this option will enable the *GenGET Database Options* screen.
- **GET SNMP:** This option should be selected only if GenGET SNMP is also installed. Selecting this option will enable the *GenGET Database Options* screen.

Click **Next** to continue.



Optional Features

☐ **NetVista** Select this option to connect GenWatch3 to a GenGET ATIA DataServer.

☐ **Trio** Select this option if you have purchased the Trio module for GenWatch3.

☐ **Setup SNMP Master Agent**
Select this option to install the GenGET SNMP Master Agent Service. Required to transmit SNMP messages from GenWatch3.
Note: Checking this option during an upgrade will reset user settings in the Master Agent.

☐ **Setup RPC CAD**
Select this option to install NobleNet Portmapper for TCP. Required for Connect: CADI and Halcyon: RPC connections.

☐ **GET APM** Select this option to connect GenWatch3 to a GenGET APM DataServer.

☐ **GET SNMP** Select this option to connect GenWatch3 to a GenGET SNMP DataServer.

Figure 1.8 – Optional Features screen

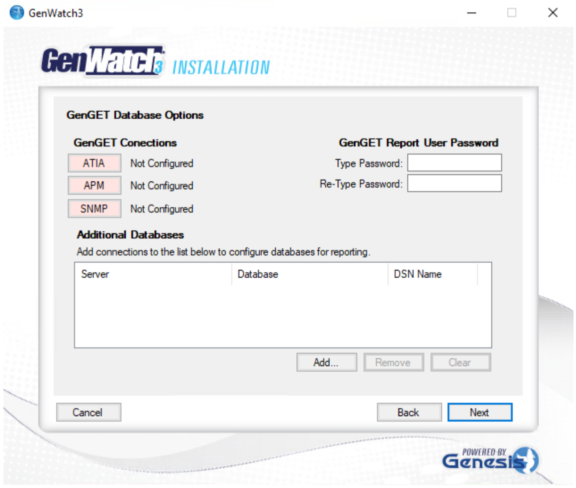
GenGET Database Options Screen

The *GenGET Database Options* screen (Figure 1.9) allows the configuration of options related to GET products. This screen only displays if the **NetVista**, **GET APM**, or **GET SNMP** options were selected on the Optional Features screen.

The GenGET Connection buttons will be colored red initially. They will change to green once the connection is successfully configured.

- **GenGET Connections**
  - **ATIA:** Click this button to provide the information required to connect to the GenGET ATIA database. Only visible if NetVista was selected on the *Optional Features* screen.
  - **APM:** Click this button to provide the information required to connect to the GenGET APM database. Only visible if GET APM was selected on the *Optional Features* screen.
  - **SNMP:** Click this button to provide the information required to connect to the GenGET SNMP database. Only visible if GET SNMP was selected on the *Optional Features* screen.
- **GenGET Report User Password:** The password that will be used to run GenGET reports in GW_Reports. The GenGET Report User is named ReportsGW.
- **Additional Databases:** Click this button to provide the information required to connect to optional GET databases. This can be used to create the reporting user in the GET databases.

Click **Next** to continue.



GenWatch3

GenWatch3 INSTALLATION

GenGET Database Options

GenGET Conections

ATIA Not Configured

APM Not Configured

SNMP Not Configured

GenGET Report User Password

Type Password:

Re-Type Password:

Additional Databases

Add connections to the list below to configure databases for reporting.

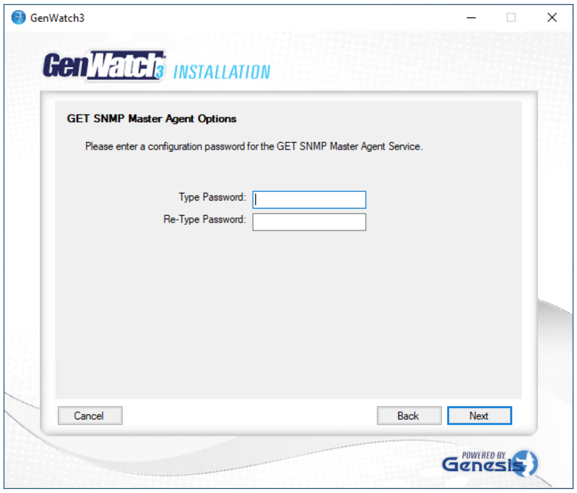
Server	Database	DSN Name

Figure 1.9 – *GenGET Database Options* screen

GET SNMP Master Agent Options Screen

The *GET SNMP Master Agent Options* screen (Figure 1.10) prompts you to set the configuration password for the GET SNMP Master Agent. This screen only displays if the **Setup SNMP Master Agent** option was selected on the *Optional Features* screen.

Click **Next** to continue.



GET SNMP Master Agent Options

Please enter a configuration password for the GET SNMP Master Agent Service.

Type Password:

Re-Type Password:

Figure 1.10 – *GET SNMP Master Agent Options* screen

Database Options Screen

The *Database Options* screen (Figure 1.11) allows you to choose an SQL Server Instance to host the GW database. The selection will default to the local, default instance of SQL Server if it exists. If there is not a default instance installed, the *<Install SQL Express>* option will be available. Click *<Browse for more>* to search the network for existing SQL Server instances. The server and instance name may also be entered manually.

The *<Browse for more>* option may not find all SQL Servers on the network.

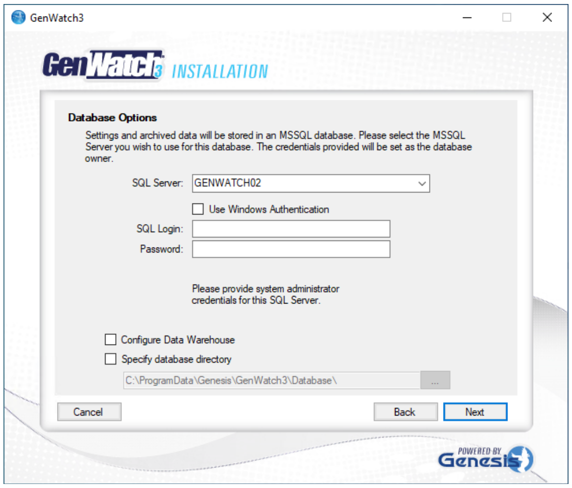
Authentication provides the following options:

- *Windows Authentication* – Setup will log into the database using the current Windows user account.
- *SQL Server Authentication* – Setup will log into the database using the specified SQL user credentials. The credentials entered must have system administrator privileges on the SQL Server instance.

Check **Configure Data Warehouse** to deploy the GenWatch3 data warehouse. Refer to the *GW Warehouse Screen* section section earlier in this chapter for details.

Check **Specify database directory** to choose the directory for the database.

Click **Next** to continue.



Database Options

Settings and archived data will be stored in an MSSQL database. Please select the MSSQL Server you wish to use for this database. The credentials provided will be set as the database owner.

SQL Server: GENWATCH02

□ Use Windows Authentication

SQL Login:

Password:

Please provide system administrator credentials for this SQL Server.

□ Configure Data Warehouse

□ Specify database directory

C:\ProgramData\Genesis\GenWatch3\Database\

Figure 1.11 – *Database Options* screen

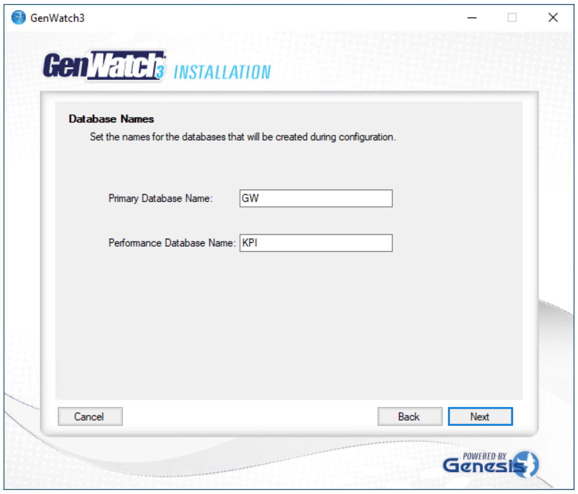
Remote Database Considerations

- **Domain Users** – This account may need to be added to the Domain Users group
- **Workgroup Users** – This account must exist on the database machine and all client machines

Database Names Screen

The *Database Names* screen (Figure 1.12) prompts you enter names for the databases used by GenWatch3. Renaming the databases is optional and you can continue the setup without changing them.

Click **Next** to continue.



Database Names

Set the names for the databases that will be created during configuration.

Primary Database Name: GW

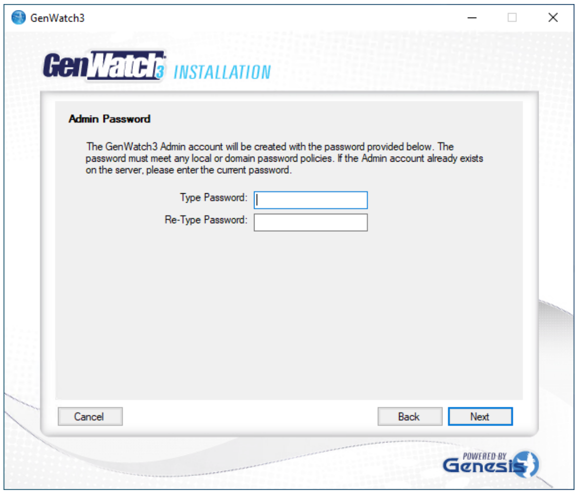
Performance Database Name: KPI

Figure 1.12 – *Database Names* screen

Admin Password Screen

The *Admin Password* screen (Figure 1.13) prompts you to set the *Admin* password. The *Admin* account is created during the configuration and is used to login to GenWatch3 when the configuration is complete.

Click **Next** to continue.



Admin Password

The GenWatch3 Admin account will be created with the password provided below. The password must meet any local or domain password policies. If the Admin account already exists on the server, please enter the current password.

Type Password:

Re-Type Password:

Figure 1.13 – *Admin Password* screen

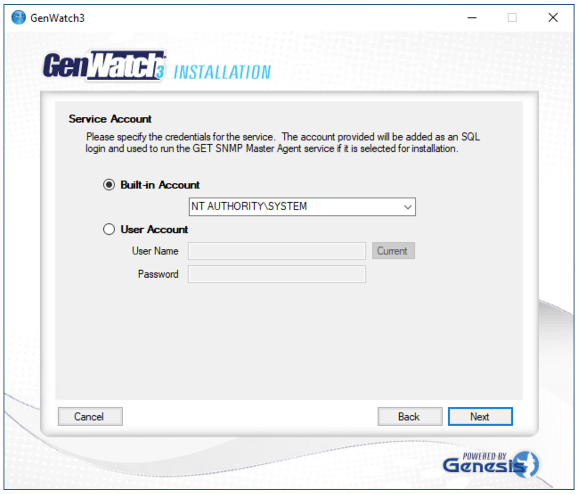
The password provided must meet the password policy in SQL Server. Some policies require a combination of upper-case, lower-case, and numeric values.

GenWatch3 creates the *Admin* login on the SQL Server instance and associates it with the *Admin* user it also creates in the Primary, Performance (and Trio if selected) GenWatch3 databases. This is not a Windows login user.

Service Account Screen

The *Service Account* screen (Figure 1.14) prompts you to set the account used to run the GenWatch3 service. The same credentials are used for the GET SNMP Master Agent service if it is installed. An SQL Login is automatically added for the credentials specified.

Click **Next** to continue.



Service Account

Please specify the credentials for the service. The account provided will be added as an SQL login and used to run the GET SNMP Master Agent service if it is selected for installation.

● **Built-in Account**

NT AUTHORITY\SYSTEM

○ **User Account**

User Name

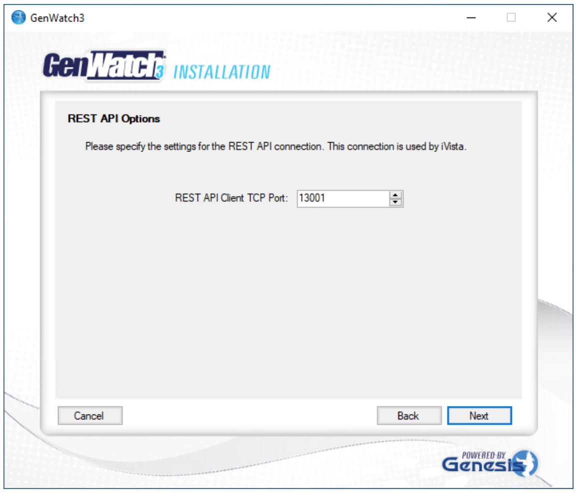
Password

Figure 1.14 – *Service Account* screen

REST API Options Screen

The *REST API Options* screen (Figure 1.15) prompts you to set the port for the GenWatch3 REST API. This API is used for communication between GenWatch3 and the Genesis iVista and GenGET products.

Click **Next** to continue.



REST API Options

Please specify the settings for the REST API connection. This connection is used by iVista.

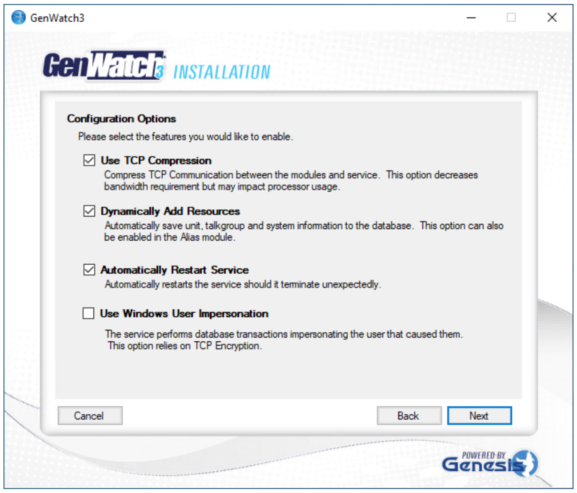
REST API Client TCP Port: 13001

Figure 1.15 – *REST API Options* screen

Configuration Options Screen

The *Configuration Options* screen (Figure 1.16) allows you to select what options you would like to enable or install.

Click **Next** to continue.



Configuration Options

Please select the features you would like to enable.

☑ **Use TCP Compression**
Compress TCP Communication between the modules and service. This option decreases bandwidth requirement but may impact processor usage.

☑ **Dynamically Add Resources**
Automatically save unit, talkgroup and system information to the database. This option can also be enabled in the Alias module.

☑ **Automatically Restart Service**
Automatically restarts the service should it terminate unexpectedly.

□ **Use Windows User Impersonation**
The service performs database transactions impersonating the user that caused them. This option relies on TCP Encryption.

Figure 1.16 – *Configuration Options* screen

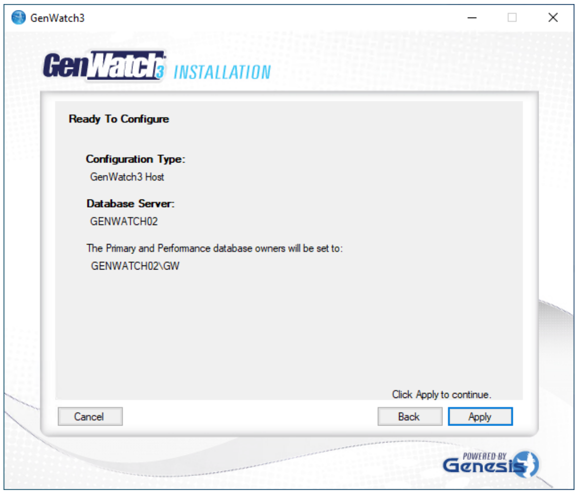
❌ The **Use Windows User Impersonation** option requires that any Windows user that logs into GenWatch3 must have the same SQL server and database permissions as that of the account under which the GenWatch3 service runs. These permissions are listed below:

- For each of the databases created by GenWatch3 (GW, KPI, and Trio) the user must be assigned to the built-in *db_securityadmin* role as well as the *db_gw3service* role created in each database during the installation of GenWatch3.
- The user must be assigned the **GRANT** option on the **ALTER ANY CONNECTION** server level permission.
- Additionally, the Windows user cannot have higher permission levels on the SQL server and databases than the GenWatch3 service account as SQL Server will prevent the service from impersonating a user with more permissions than itself.

Ready To Configure Screen

When all configuration information has been collected, both host and client setup types will show the *Ready to Configure* screen shown in Figure 1.17.

Click **Apply** to begin configuring GenWatch3.



Ready To Configure

Configuration Type:
GenWatch3 Host

Database Server:
GENWATCH02

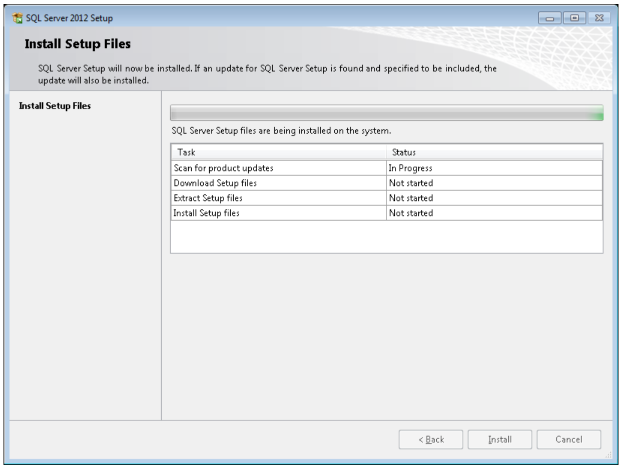
The Primary and Perfomance database owners will be set to:
GENWATCH02\GW

Click Apply to continue.

Figure 1.17 – *Ready to Configure* screen

SQL Server Express Installation Screens

If you choose to install SQL Server Express you will see screens similar to the ones in Figure 1.18 and 1.19 as SQL installs on the local machine.

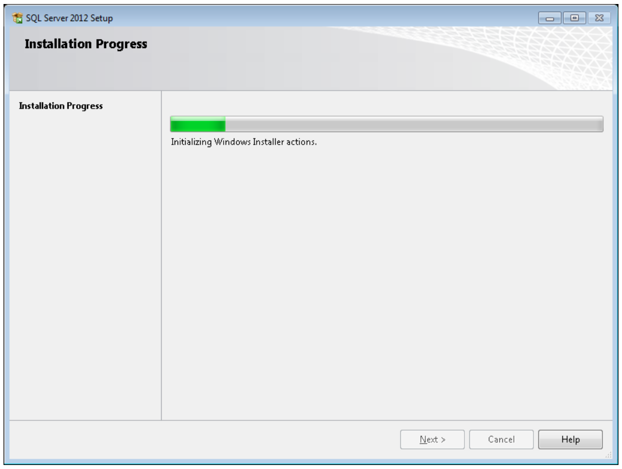


SQL Server Setup will now be installed. If an update for SQL Server Setup is found and specified to be included, the update will also be installed.

SQL Server Setup files are being installed on the system.

Task	Status
Scan for product updates	In Progress
Download Setup files	Not started
Extract Setup files	Not started
Install Setup files	Not started

Figure 1.18 – SQL Server Express Installation

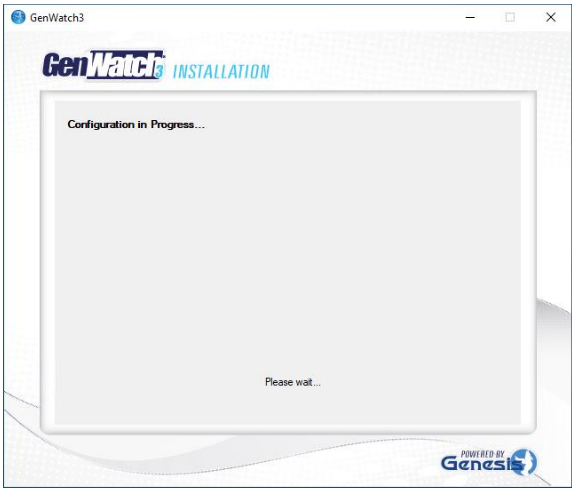


Initializing Windows Installer actions.

Figure 1.19 – SQL Server Express Installation Progress

Configuration in Progress Screen

Please wait while GenWatch3 is configured. You will see the *Configuration in Progress* screen like the one shown in Figure 1.20. You may also see several DOS/Command windows pop up and disappear in the background. They are performing background configuration and are normal.



Configuration in Progress...

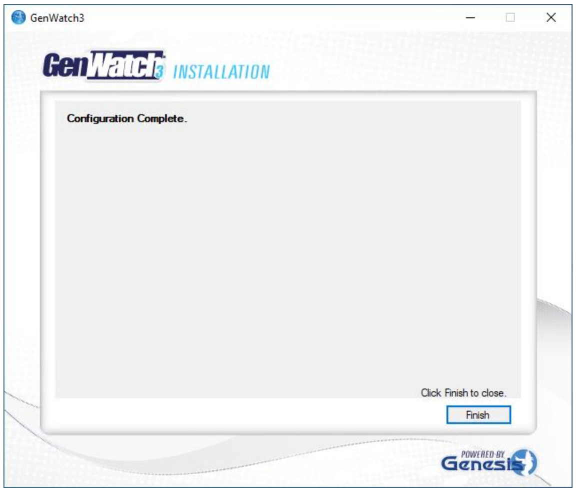
Please wait...

Figure 1.20 – *Configuration in Progress* screen

Configuration Complete

When the configuration finishes, you will see the *Configuration Complete* screen, as shown in Figure 1.21.

Click **Finish** to exit the setup program



Configuration Complete.

Click Finish to close.

Figure 1.21 – *Configuration Complete* screen

You will notice that GenWatch3 shortcuts have been added to your desktop and start menu. GW_Alert has also been added as a Start Up app to ensure the GenWatch3 interfaces start with Windows.

To launch the GW_Alert manually, double-click the **LaunchPad** icon on your desktop, or go to the **Windows Start** menu and navigate to **Programs → Genesis → LaunchPad**.

Please see the following chapters of this document for instructions on launching and configuring GenWatch3.

Positioning Yourself for Client Deployment

For GenWatch3 installs with multiple clients, clients can be automatically upgraded the next time a user logs in from the client.

Setting the Service Account Manually

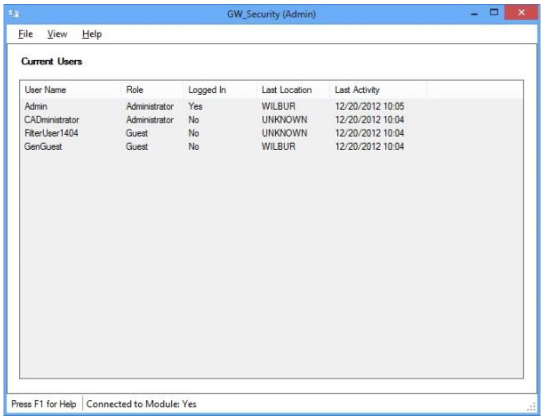
If you wish to change the service account or if you install the Windows Hardening Kit after installation, you must set the service account manually by following the steps below:

Changing the service account will cause any saved passwords to become inaccessible. Be sure to have the passwords readily available. Any connections requiring passwords will not connect after the service account has been changed until the password is reentered in the connection settings. Additionally, if GenGET reports are run via GW_Reports, the GenGET Reports User Password must be updated. Contact Genesis Support to do so.

1. First ensure the desired account has the following privileges:
    a. Windows Privileges
        i. **Full control** of the GenWatch3 program data directory. Refer to Windows documentation for instructions on setting up this privilege.
    b. SQL Server Privileges
        i. A login with the following privileges:
            1. Alter any login
            2. Alter any connection
        ii. A user in the GW database with the following roles:
            1. db_gw3service
            2. db_securityadmin
        iii. A user in the KPI database with the following roles:
            1. db_gw3service
            2. db_securityadmin
        iv. If Trio is in use, a user in the Trio database with the following roles:
            1. db_gw3service
            2. db_securityadmin

Please see the *SQL Server Security* section below for more information on creating a user with the required database permissions.

2. 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 **Security** module. Figure 1.22 shows that only the Admin account is logged in.



Current Users

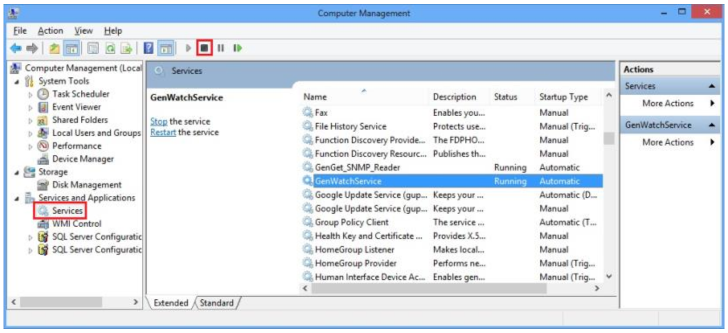
User Name	Role	Logged In	Last Location	Last Activity
Admin	Administrator	Yes	WILBUR	12/20/2012 10:05
CADministrator	Administrator	No	UNKNOWN	12/20/2012 10:04
FilterUser1404	Guest	No	UNKNOWN	12/20/2012 10:04
GenGuest	Guest	No	WILBUR	12/20/2012 10:04

Press F1 for Help | Connected to Module: Yes

Figure 1.22 – Current Users List

    c. Close all modules on the host machine and exit GW_Alert.

3. Stop the GenWatchService.
    a. Right-click **My Computer** and select **Manage**.
    b. Select **Services** then select the **GenWatchService.**
    c. Click the **Stop** button**.** (Figure 1.23)
    d. Leave this window open.



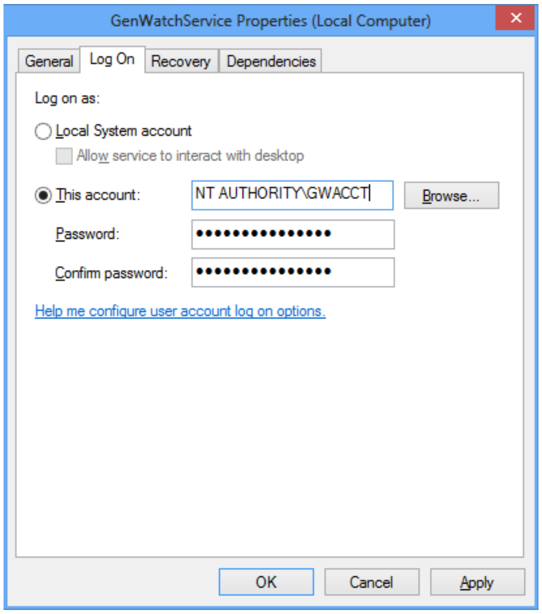
GenWatchService

Stop the service
Restart the service

Name	Description	Status	Startup Type
Fax	Enables you...		Manual
File History Service	Protects use...		Manual (Trig...
Function Discovery Provide...	The FDPHO...		Manual
Function Discovery Resourc...	Publishes th...		Manual
GenGet_SNMP_Reader		Running	Automatic
GenWatchService		Running	Automatic
Google Update Service (gup...	Keeps your ...		Automatic (D...
Google Update Service (gup...	Keeps your ...		Manual
Group Policy Client	The service ...		Automatic (T...
Health Key and Certificate ...	Provides X.5...		Manual
HomeGroup Listener	Makes local...		Manual
HomeGroup Provider	Performs ne...		Manual (Trig...
Human Interface Device Ac...	Enables gen...		Manual (Trig...

Figure 1.23 – Computer Management →Services

4. Update the GenWatchService logon credentials.
    a. Within the *Computer Management* screen, right-click **GenWatchService** and select **Properties** then go to the **Log On** tab.
    b. Type the username and password into the appropriate fields. (Figure 1.24)


GenWatchService Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.
OK
Cancel
Apply

Log on as:

○ Local System account

□ Allow service to interact with desktop

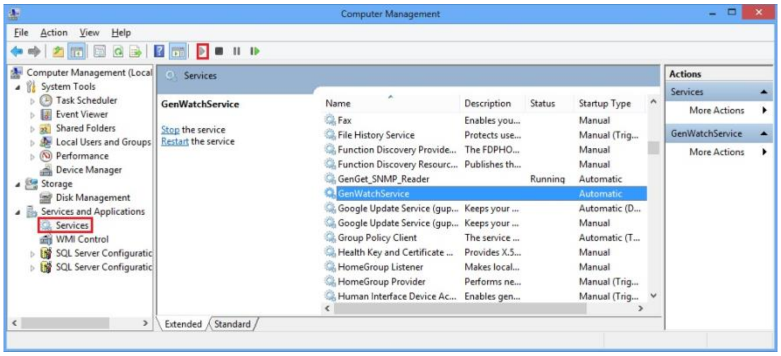
● This account: NT AUTHORITY\GWACCT

Password: •••••••••••••••

Confirm password: •••••••••••••••

Figure 1.24 – Update the Account credentials

5. Start the GenWatchService.
    a. Within Computer Management, select the **GenWatchService**.
    b. Click the **Play** button**.** (Figure 1.25)



Name	Description	Status	Startup Type
Fax	Enables you...		Manual
File History Service	Protects use...		Manual (Trig...
Function Discovery Provide...	The FDPHO...		Manual
Function Discovery Resourc...	Publishes th...		Manual
GenGet_SNMP_Reader		Running	Automatic
GenWatchService			Automatic
Google Update Service (gup...	Keeps your ...		Automatic (D...
Google Update Service (gup...	Keeps your ...		Manual
Group Policy Client	The service ...		Automatic (T...
Health Key and Certificate ...	Provides X.5...		Manual
HomeGroup Listener	Makes local...		Manual
HomeGroup Provider	Performs ne...		Manual (Trig...
Human Interface Device Ac...	Enables gen...		Manual (Trig...

Figure 1.25 – Starting the GenWatchService

6. Login to the GenWatch3 host and ensure the service is running properly.
7. Update any saved passwords for connections and the GenGET Reports User.
8. Inform GenWatch3 clients that they may now launch GW_Alert and connect to the host machine.

SQL Server Security

The GenWatchService requires the Windows user to exist in SQL Server's security. To add a Windows user to SQL Server security, follow the steps below:

1. Open SQL Server Management Studio.
2. Login to the SQL server as *sa* or a user with the *securityadmin* role.
3. Under the *Security* folder, right-click on the *Logins* folder and choose *New Login…*
4. In *Login Name*, enter the Windows username, including the domain (i.e. myDomain\GenWatchServiceTheWindowsUser). You can click **Search…** to search for domain users.
5. Choose *Windows authentication*.
6. For *Default database*, choose GW.
7. On the *User Mapping* page under *Users mapped to this login*, check the GW database.
8. In the *Database role membership for: GW* choose only *db_gw3service, db_securityadmin* and *public*.
9. On the *Securables* page, click the **Search…** button.
10. Choose *The server 'Servername'* and click **OK**.
11. Check the *Grant* boxes for *Alter any connection*, *Alter any login*, and *Connect SQL*.
12. Click **OK**.
13. Follow steps 7-13 for the KPI database.
14. If Trio is in use, follow steps 7-13 for the Trio database.

SNMP Configuration

This section describes the process of setting up the *GET SNMP Master Agent Service* (GSMAS) for use with GenWatch3. If you do not intend to use SNMP functionality within GenWatch3, you may skip this section.

Install the Windows features for SNMP available in Control Panel > Programs and Features > Turn Windows features on or off

- Simple Network Management Protocol (SNMP) (also known as the SNMP Service) is required
- WMI SNMP Provider is not required

Stop any other SNMP agent applications on the machine and set their Start Up type to Disabled.

- Microsoft’s SNMP agent applications can be stopped in the Windows service manager. They are called “SNMP Trap” and “SNMP Service”. The GSMAS loads their associated application libraries so that any applications depending on them can instead depend on GSMAS.

Now, start the *GETSNMPMasterAgentService* via the *Computer Management* window (Figure 1.26). To access this window, right-click on **My Computer** and select **Manage.** Then expand **Services and Applications** and select **Services.** Select the *GETSNMPMasterAgentService* and click **Start.**

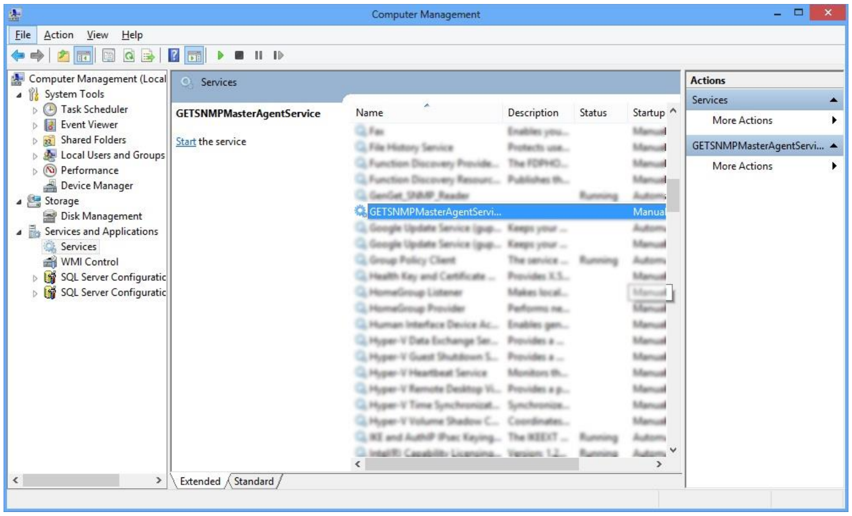
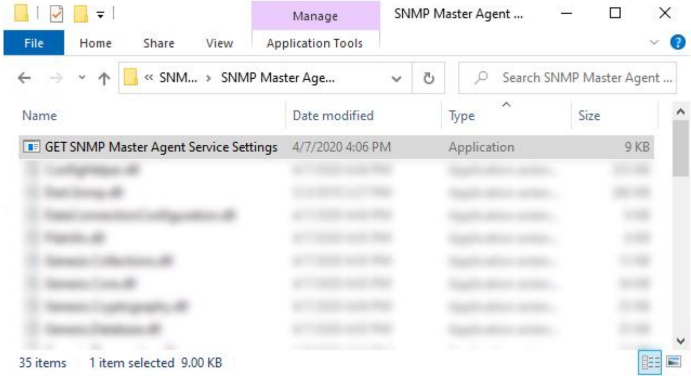


Figure 1.26 – Computer Management

Browse to the SNMP Master Agent Config directory using Windows Explorer as shown in Figure 1.27. This directory may be hidden by default. Run the GET SNMP Master Agent Service Settings **As Administrator**: *C:\Program Files\Genesis\GenGET\SNMP Master Agent\SNMP Master Agent Config*

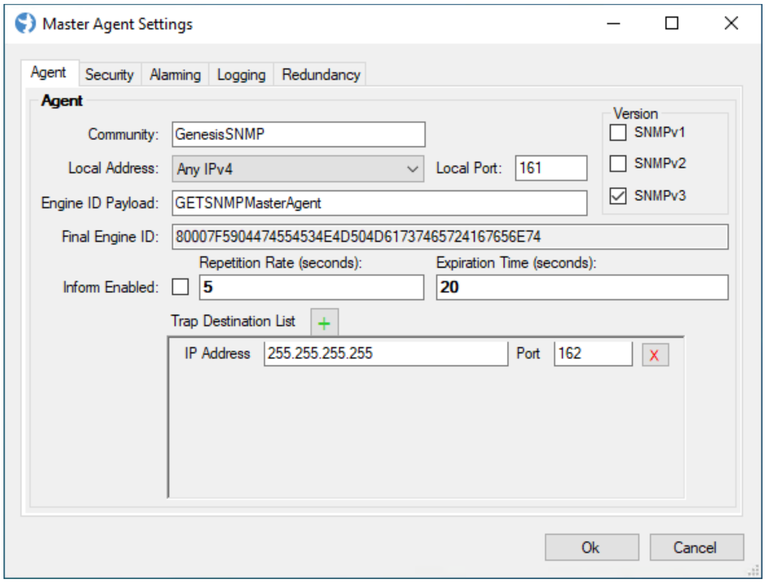


Name	Date modified	Type	Size
GET SNMP Master Agent Service Settings	4/7/2020 4:06 PM	Application	9 KB

35 items 1 item selected 9.00 KB

Figure 1.27 –Master Agent Config Directory

The *Master Agent Settings* (Figure 1.28) window will be displayed after you select the configuration file. Set the **Local Address** setting to the machine IP address. Then, click **Add User** under the **Security** tab to create the SNMPv3 user. Click **OK** to save the changes.



Community: GenesisSNMP

Local Address: Any IPv4

Local Port: 161

Engine ID Payload: GETSNMPMasterAgent

Final Engine ID: 80007F5904474554534E4D504D61737465724167656E74

☐ SNMPv1
☐ SNMPv2
☑ SNMPv3

Inform Enabled: ☐

Repetition Rate (seconds): 5

Expiration Time (seconds): 20

IP Address 255.255.255.255 Port 162

Figure 1.28 – Master Agent Settings

Engine ID Payload field is ASCII text and the preview shows the **Final Engine ID** in Hexadecimal.

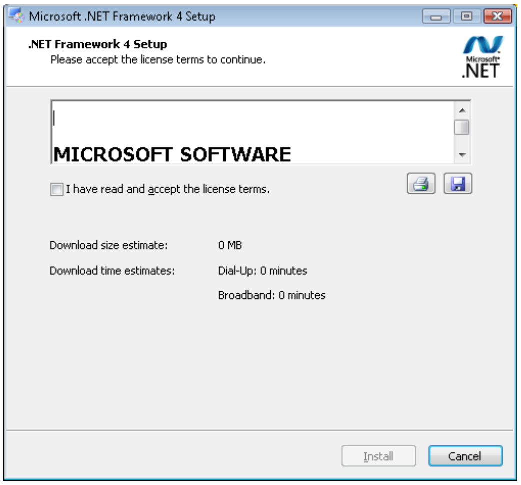
This completes the setup process for the GET SNMP Master Agent Service.

GenWatch3 Client Upgrade

To begin the client upgrade process, insert (if on DVD or USB) or browse to the GenWatch3 installation media. If the GenWatch3 setup program does not launch automatically, browse to the installation media's root directory and double-click on *Start.hta*.

Required Software

In order to support GenWatch3, Microsoft's .NET Framework 4.8 or later must be installed on your computer. If it is not already installed, you will see a window like the one shown in Figure 1.29. Click **Install** to begin installing or upgrading .NET Framework.



.NET Framework 4 Setup
Please accept the license terms to continue.

MICROSOFT SOFTWARE

□ I have read and accept the license terms.

Download size estimate: 0 MB
Download time estimates: Dial-Up: 0 minutes
Broadband: 0 minutes

Figure 1.29 – .NET Framework Installer.

Preparing to Install

After the .NET Framework is installed or upgraded as needed, the **GenWatch3 Installer** will launch. The *Welcome* screen in Figure 1.30 allows you to begin the upgrade process.

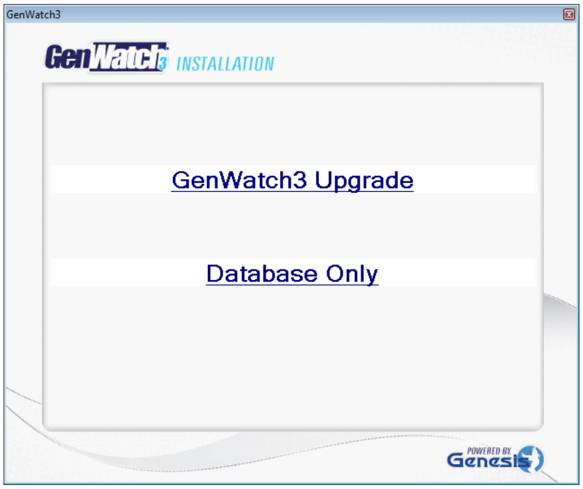
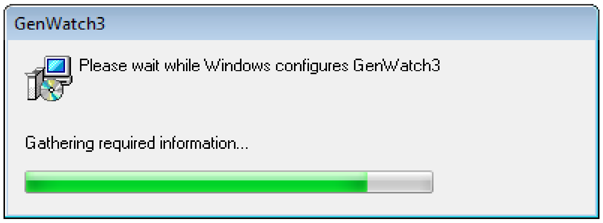


Figure 1.30 – Upgrade Screen

Click on **GenWatch3 Upgrade** to begin the upgrade process. Please wait for the process to complete upgrading.

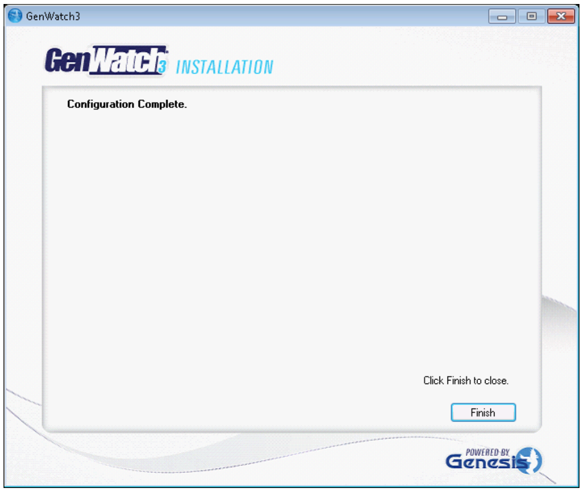

GenWatch3

Please wait while Windows configures GenWatch3

Gathering required information...

Figure 1.31 – Upgrade in progress

Click **OK** to exit the Client Upgrade program.



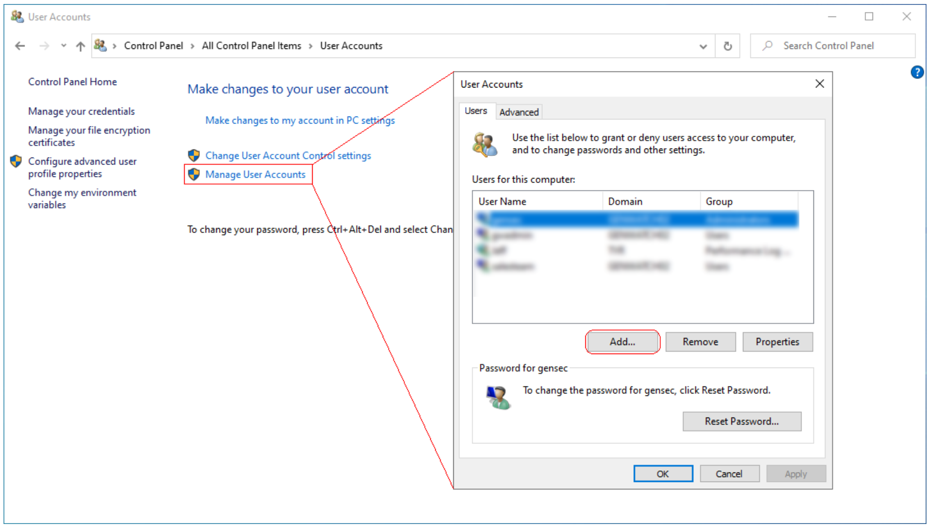
Configuration Complete.

Click Finish to close.

Figure 1.32 – Configuration Completed screen

Remote Database Configuration

Remote database configurations require a dedicated user for the GenWatch3 service. If the installation is on a domain, this user must be added to the **Domain Users** group. If this is a workgroup installation, the user must be created on both the GenWatch3 host and database machines. To create this user, open the *Control Panel* and select *User Accounts*, then open *Manager User Accounts* and click **Add.** (Figure 1.33)


User Accounts
Control Panel › All Control Panel Items › User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Make changes to my account in PC settings
Change User Account Control settings
Manage User Accounts
User Accounts
Users
Advanced
Users for this computer:
User Name
Domain
Group
Add...
Remove
Properties
Password for gensec
Reset Password...
OK
Cancel
Apply

To change your password, press Ctrl+Alt+Del and select Chan

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

To change the password for gensec, click Reset Password.

Figure 1.33 – Navigation to User Accounts

Allow the GenWatch3 service user and any additional client users to access the database machine over the network. On the database machine, open the control panel and launch the *Administrative Tools*. Then, launch the *Local Security Policy* window and select *User Rights Assignment* under *Local Policies*. (Figure 1.34)

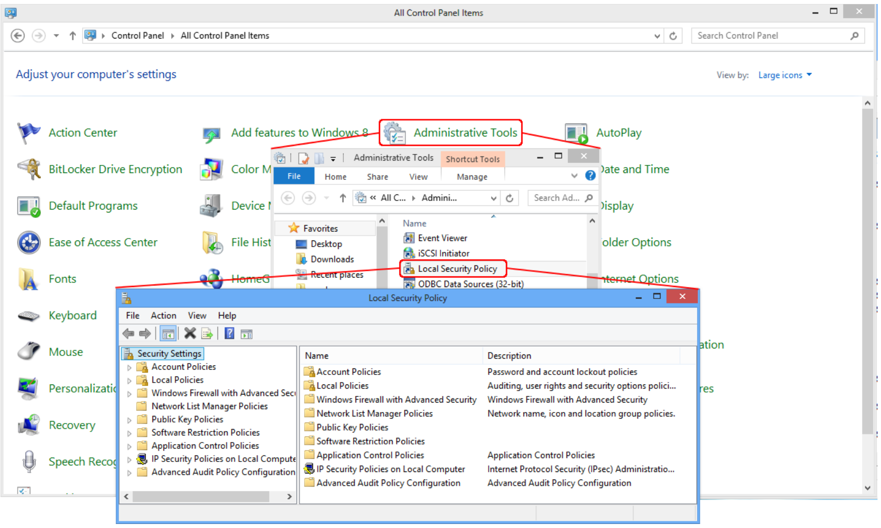
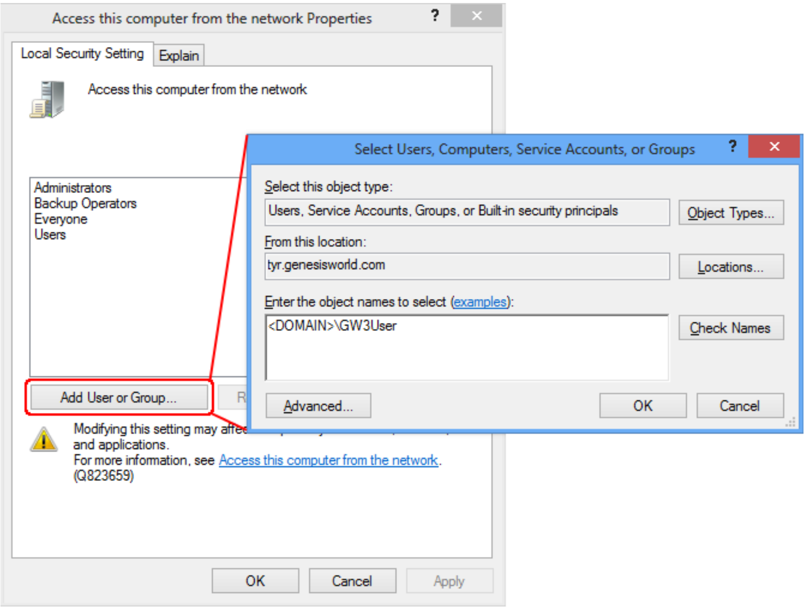

All Control Panel Items
Control Panel > All Control Panel Items
Search Control Panel
Adjust your computer's settings
View by: Large icons
Action Center
Add features to Windows 8
Administrative Tools
AutoPlay
BitLocker Drive Encryption
Date and Time
Default Programs
Display
Ease of Access Center
Folder Options
Fonts
Internet Options
Keyboard
Mouse
Personalization
Recovery
Speech Recognition
Administrative Tools
Shortcut Tools
File
Home
Share
View
Manage
Favorites
Desktop
Downloads
Recent places
Name
Event Viewer
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Description
Password and account lockout policies
Auditing, user rights and security options polici...
Windows Firewall with Advanced Security
Network name, icon and location group policies.
Application Control Policies
Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration

Figure 1.34 – Navigation to Local Security Policy

Double-click on *Access this computer from the network* to display the list of allowed users. Then, click **Add User or Group** to add the desired users to this policy thus allowing the users to access this machine. (Figure 1.35)


Access this computer from the network Properties
Local Security Setting
Explain
Access this computer from the network
Add User or Group...
OK
Cancel
Apply
Select Users, Computers, Service Accounts, or Groups
Object Types...
Locations...
Check Names
Advanced...
OK
Cancel

Administrators
Backup Operators
Everyone
Users

Modifying this setting may affe... and applications.
For more information, see Access this computer from the network. (Q823659)

Select this object type: Users, Service Accounts, Groups, or Built-in security principals

From this location: tyr.genesisworld.com

Enter the object names to select (examples): <DOMAIN>\GW3User

Figure 1.35 – Adding users to the policy

If you have many users to add, consider creating a new group for GenWatch3 users. You can then add that group to the policy above thus, giving all its members access.

Finally, during the GenWatch3 Host installation, specify the GenWatch3 service user on the *Service Account* screen (Figure 1.14). This will automatically add a SQL Server login for the user.

Firewall Configuration

Windows 10/Server 2016

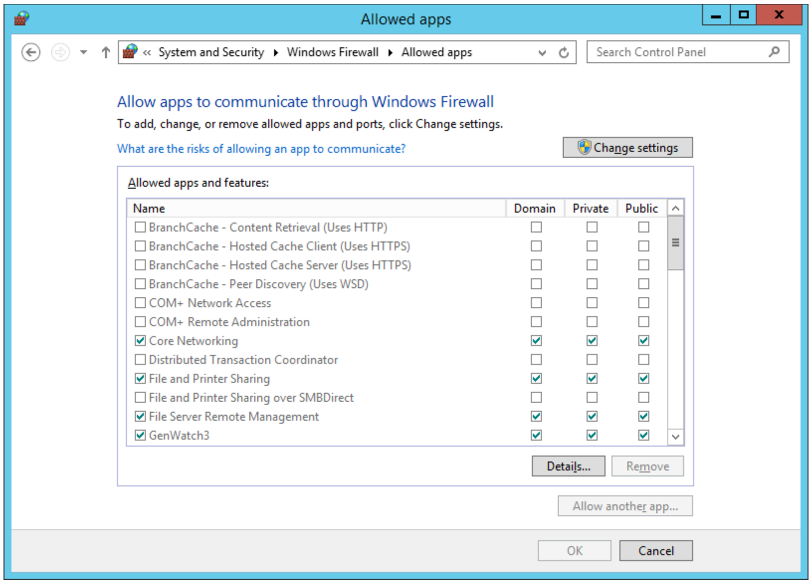
The following programs must be allowed through the Windows Firewall:

- GenWatch.exe – This is the GenWatch3 service executable.
  C:\Program Files\Genesis\Genwatch3\GenWatch.exe
- SqlServer.exe
  C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe
- SqlBrowser.exe
  C:\ Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe

SqlBrowser is required if the databases are installed on a named SQL instance.

To access the Windows Firewall setting within Windows 10/Server 2016:

Control Panel → System and Security → Windows Firewall → Allow an app through Windows Firewall



Allowed apps

« System and Security ▸ Windows Firewall ▸ Allowed apps

Search Control Panel

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Domain	Private	Public
☐ BranchCache - Content Retrieval (Uses HTTP)	☐	☐	☐
☐ BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Peer Discovery (Uses WSD)	☐	☐	☐
☐ COM+ Network Access	☐	☐	☐
☐ COM+ Remote Administration	☐	☐	☐
☑ Core Networking	☑	☑	☑
☐ Distributed Transaction Coordinator	☐	☐	☐
☑ File and Printer Sharing	☑	☑	☑
☐ File and Printer Sharing over SMBDirect	☐	☐	☐
☑ File Server Remote Management	☑	☑	☑
☑ GenWatch3	☑	☑	☑

Details... Remove

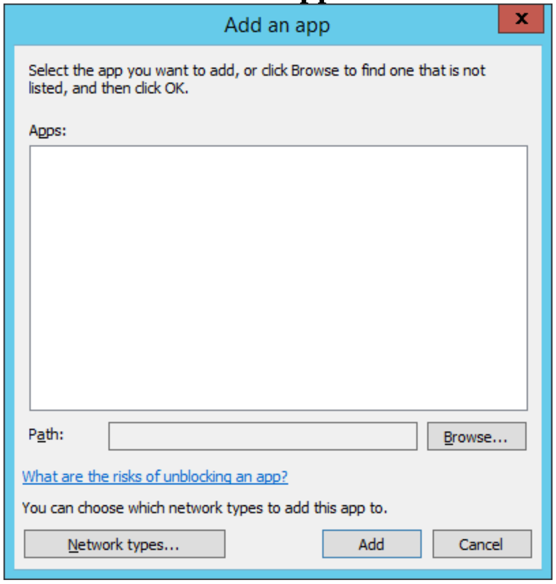
Allow another app...

OK Cancel

Figure 1.36 – Allowed apps

To add a program to the Windows Firewall exception list:

1. Click the **Change Settings** button to enable changes.
2. Click **Allow another app…** to launch the *Add an app* window

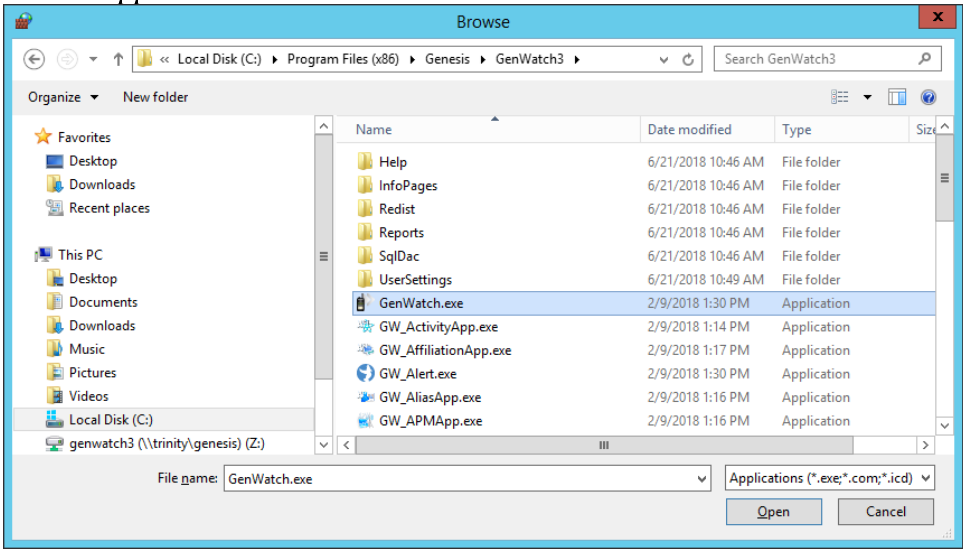


Select the app you want to add, or click Browse to find one that is not listed, and then click OK.

What are the risks of unblocking an app?

You can choose which network types to add this app to.

3. If the desired app does not display in the Apps list click on the **Browse...** button to navigate to program executable desired (ex. C:\Program Files\Genesis\GenWatch3\GenWatch.exe). Select the .exe file of the program you would like to add then click **Open**, this returns you to the *Add an app* window.



« Local Disk (C:) ▸ Program Files (x86) ▸ Genesis ▸ GenWatch3 ▸

Name	Date modified	Type
Help	6/21/2018 10:46 AM	File folder
InfoPages	6/21/2018 10:46 AM	File folder
Redist	6/21/2018 10:46 AM	File folder
Reports	6/21/2018 10:46 AM	File folder
SqlDac	6/21/2018 10:46 AM	File folder
UserSettings	6/21/2018 10:49 AM	File folder
GenWatch.exe	2/9/2018 1:30 PM	Application
GW_ActivityApp.exe	2/9/2018 1:14 PM	Application
GW_AffiliationApp.exe	2/9/2018 1:17 PM	Application
GW_Alert.exe	2/9/2018 1:30 PM	Application
GW_AliasApp.exe	2/9/2018 1:16 PM	Application
GW_APMApp.exe	2/9/2018 1:16 PM	Application

File name: GenWatch.exe

Applications (*.exe;*.com;*.icd)

4. Click **Add**. This adds the program to the exception list and checks it to be exempt.

Please see the following chapters of this document for instructions on launching and configuring GenWatch3.

Advanced Client Setup

On host installs using encryption (this is the default) clients that are not on the same domain as the host require Windows permission to be configured before the client will be able to connect to the host. The following steps will add a client's domain to the host's list of trusted domains and allow encrypted communication between host and client.

Creating a domain trust relationship

In order to complete the steps below, if there are multiple domains involved, the domains must have a pre-defined trusted relationship. Setting up this trusted relationship is outside of the scope of this documentation.

Adding a user to a group

1. Open the Computer Management tool:
   - Windows 10: Right click on the **Start** button → Right click **Computer** → Click **Computer Managment** (click **Yes** if permission is required).
2. Click on **Groups** located under Computer Management → System Tools → Local Users and Groups in the tree view in the left pane.
3. Double click the group you would like to add the Client(s) username(s) to.
4. Click **Add** on the Administrators Properties and enter the username(s) to be used on the client machine(s) and click **OK**.
5. Close the Computer Management tool and proceed to the *Adding a Trusted Group* section.

Adding a Trusted Group

1. On the host machine open Control Panel and launch Administrative Tools.
   - Windows 10: Control Panel → System and Security → Administrative Tools
2. Double click on **Local Security Policy** in the Administrative Tools folder.
3. Navigate to "Access this Computer from the network."
   - Windows 10: Security Settings → Local Policies (located on the left hand menu).
   - User Rights Assignment → Access this Computer from the network.
4. If a desired local group is not already in the list, you will need to add a local group to the list by selecting the **Add User or Group…** button and entering the group name.

Audit Logging

NOTE: For SQL Server 2016 RTM, 2014 and earlier, Audit logging is only available on Microsoft SQL Server Enterprise edition. For SQL Server 2016 SP1 and later, it is available on all editions.

Overview

SQL audit logging stores detailed information regarding pre-determined categories of SQL activity, such as adds, inserts, deletes. Each time-stamped activity is tied to a Windows user and describes the target table and action taken on that table.

Audit Logging Setup

Audit logging consists of two parts: server audits and database audit specifications. The server audit contains the rules regarding logging type (event log or file), maximum log size, roll-over, etc. The database audit specification contains the rules on what types of events to audit on a specific database.

Config File Options

In order to associate a Windows user with the SQL actions, you must edit the GenWatch3.config file. The GenWatch3.config file is in the following folder:
<ProgramData>\Genesis\GenWatch3

In the GenWatch3.config file, set the following options:

```
<UseTcpEncryption>1</UseTcpEncryption>
 <Impersonate>1</Impersonate>
```

❌ Before enabling the above config file options, each Windows user that runs the GenWatch3 client must be setup in SQL Server security. The process of setting up these users is described below.

SQL Server Security

SQL impersonation (executing SQL statements on behalf of the Windows user) requires the Windows user or a Windows Security Group assigned to the Windows user to exist in SQL server's security and as a user on the GW database. To add a Windows user or a Windows Security Group to SQL security and the GenWatch3-related databases, follow the steps below:

1. Open SQL Server Management Studio.
2. Login to the SQL server as *sa* or a user with the *securityadmin* role.
3. Under the *Security* folder, right-click on the *Logins* folder and choose *New Login…*
4. In *Login Name*, enter the Windows username or Windows Security Group, including the domain (i.e. myDomain\GenWatchServiceTheWindowsUser or myDomain\Gw3Users). You can click **Search…** to search for domain users.
5. Choose *Windows authentication*.
6. For *Default database*, choose GW.

7. On the *User Mapping* page under *Users mapped to this login*, check the GW database.
8. In the *Database role membership for: GW* choose only *db_gwuser*
9. Follow steps 7-8 for the KPI database.
10. If Trio is in use, follow steps 7-8 for the Trio database.
11. Execute the following SQL query to grant impersonation permissions for the Windows login. Replace <Windows login> with the Windows login created above. Replace <GenWatch Service Account> with the account under which the GenWatch3 service runs:

```
USE [master]
GRANT IMPERSONATE ON LOGIN::[<Windows login>] to [<GenWatch Service
Account>];
```

Setup for the Security Admin User

When using impersonation, to allow a Windows user to add, update and delete SQL logins in GenWatch3, you must add the Windows user as a login to SQL. To add a Windows user for security administration in GenWatch3 to SQL, follow the steps below:

1. Open SQL Server Management Studio.
2. Login to the SQL server as *sa* or a user with the *securityadmin* role.
3. Under the *Security* folder, right-click on the *Logins* folder and choose *New Login…*
4. In *Login Name*, enter the Windows username or Windows Security Group, including the domain (i.e. myDomain\GenWatchServiceTheWindowsUser or myDomain\Gw3Users). You can click **Search…** to search for domain users.
5. Choose *Windows authentication*.
6. For *Default database*, choose GW.
7. On the *User Mapping* page under *Users mapped to this login*, check the GW database.
8. In the *Database role membership for: GW* choose only *db_gw3service*, *db_securityadmin* and *public*.
9. On the *Securables* page, click the **Search…** button.
10. Choose *The server 'Servername'* and click **OK**.
11. Check the *Grant* boxes for *Alter any connection*, *Alter any login*, and *Connect SQL*.
12. Click **OK**.
13. Follow steps 7-12 for the KPI database.
14. If Trio is in use, follow steps 7-12 for the Trio database.
15. Execute the following SQL query to grant impersonation permissions for the Windows login. Replace <Windows login> with the Windows login created

above. Replace <GenWatch Service Account> with the account under which the GenWatch3 service runs:

```
USE [master]
GRANT IMPERSONATE ON LOGIN::[<Windows login>] to [<GenWatch Service
Account>];
```

SQL Audit Logging Setup via SQL Script

The following script creates a server audit and database audit specifications that:

- Writes to files in path *C:\SQLAuditFiles* with a maximum size of 1 GB.
- The account includes up to 30 files. Once the thirty-first 1GB file is created, the oldest audit file is purged.
- Allows SQL server to continue if the auditing feature experiences a failure.
- Logs delete, update and insert actions taken on tables in the GW database by any user.

```
USE [GW]
ALTER DATABASE AUDIT SPECIFICATION [GwAuditSpec-27f07a15-61bd-4f9d-8034-
5221880b543c]
       WITH (STATE = OFF)
DROP DATABASE AUDIT SPECIFICATION [GwAuditSpec-27f07a15-61bd-4f9d-8034-
5221880b543c]
GO
```

```
USE [MASTER]
ALTER SERVER AUDIT [GwAudit-27f07a15-61bd-4f9d-8034-5221880b543c] WITH
(STATE = OFF)
DROP SERVER AUDIT [GwAudit-27f07a15-61bd-4f9d-8034-5221880b543c];
GO
CREATE SERVER AUDIT [GwAudit-27f07a15-61bd-4f9d-8034-5221880b543c]
TO FILE
(       FILEPATH = N'C:\SQLAuditFiles\'
       ,MAXSIZE = 1 GB
       ,MAX_ROLLOVER_FILES = 30
       ,RESERVE_DISK_SPACE = OFF
)
WITH
(       QUEUE_DELAY = 0
       ,ON_FAILURE = CONTINUE
       ,AUDIT_GUID = '27f07a15-61bd-4f9d-8034-5221880b543c'
)
ALTER SERVER AUDIT [GwAudit-27f07a15-61bd-4f9d-8034-5221880b543c] WITH
(STATE = ON)
GO
```

```
USE [GW]
CREATE DATABASE AUDIT SPECIFICATION [GwAuditSpec-27f07a15-61bd-4f9d-8034-
5221880b543c]
FOR SERVER AUDIT [GwAudit-27f07a15-61bd-4f9d-8034-5221880b543c]
ADD (DELETE ON DATABASE::[GW] BY [public]),
ADD (UPDATE ON DATABASE::[GW] BY [public]),
ADD (INSERT ON DATABASE::[GW] BY [public])
WITH (STATE = ON)
GO
```

The file specified in the FILEPATH in the second query box must exist before running the query.

Viewing Audit Activity

Audit log events are viable via an SQL query. The query targets the path and file name of a specific audit log file. You can find the audit files in the FILEPATH specified when we created the server audit. In the above example, it is *C:\SQLAuditFiles*. You will need to replace the file path and name, highlighted red in the below examples, with the FILEPATH used when creating the audit log (see section above) and name of the specific audit file you are reporting on.

Example 1: All actions, ordered newest to oldest, from the targeted audit file.

```
SELECT
       *
FROM
       sys.fn_get_audit_file('C:\SQLAuditFiles\GwAudit-27f07a15-61bd-4f9d-
8034-5221880b543c_27F07A15-61BD-4F9D-8034-
5221880B543C_0_130129429718070000.sqlaudit', default, default)
ORDER BY
       event_time DESC
```

Example 2: Specific columns from all successful actions performed on behalf of user *myDomain\BobTheWindowsUser*, ordered newest to oldest, from the targeted audit file.

```
SELECT
       event_time,
       action_id,
       session_server_principal_name,
       server_principal_name,
       object_name,
       statement
FROM
       sys.fn_get_audit_file('C:\SQLAuditFiles\GwAudit-27f07a15-61bd-4f9d-
8034-5221880b543c_27F07A15-61BD-4F9D-8034-
5221880B543C_0_130129429718070000.sqlaudit', default, default)
WHERE
       succeeded = 1
       AND server_principal_name = 'myDomain\BobTheWindowsUser'
ORDER BY
       event_time DESC
```

After you install GenWatch3 on your machine, you are ready to configure your GenWatch3 modules for operation on your system. Follow the steps below to configure GenWatch3:

- **Chapter 2**: Loading GW_Alert
- **Chapter 2**: Logging into GW_Alert
- **Chapter 2**: Loading GW_LaunchPad
- **Chapter 2**: Activating the GenWatch3 license (skip if your machine came pre-licensed)
- **Chapter 3**: Configuring the GW_Security module
- **Chapter 4**: Configuring the GW_Archiver module (if you purchased GW_Archiver)

Loading GW_Alert

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

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

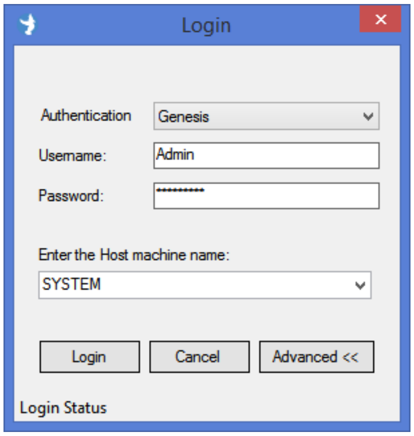
The GenWatch3 Installer add GW_Alert to the Windows Startup Apps. This means that when Windows starts up (after reboot, power off, etc.), Windows loads GW_Alert automatically.

If you do not see one of the above icons in your Windows System Tray, you may need to start GW_Alert. To start GW_Alert 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 **Genesis**
4. Click the **LaunchPad** icon: This will load GW_Alert and show one of the above icons in the System Tray.

Logging into GW_Alert

The first step to running GW_Alert is logging in. After you (or Windows) load GW_Alert, you will see the following window (shown in Figure 2.1 after the user has optionally clicked **Advanced**):



Authentication: Genesis

Username: Admin

Password: *********

Enter the Host machine name: SYSTEM

Figure 2.1 – GenWatch3 Login Window

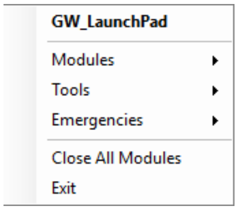
This window contains the following items or note:

- **Authentication:** Type of authentication used to log into GenWatch3. Options include Genesis and Windows.
- **Username:** GenWatch3 username you wish to login with. This box will contain the username that last logged in.
- **Password:** Password of the GenWatch3 user entered in the **Username** field.
- **Host Machine Name:** Enter the GenWatch3 Host machine name here. This entry is "remembered" after the initial login.
- **Cancel:** Click this button to cancel login and not load GW_Alert
- **Login:** Click this button once you have entered or verified the **Username** and **Password**.
- **Advanced:** Displays or hides the host entry field.

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

Loading GW_LaunchPad

GW_LaunchPad is your entry point for GenWatch3 and is therefore important to all GenWatch3 users. From it you will launch all modules, configure database and host settings, and manage your license. GW_LaunchPad will automatically load each time you login to GW_Alert.



To load GW_LaunchPad, follow the steps below:

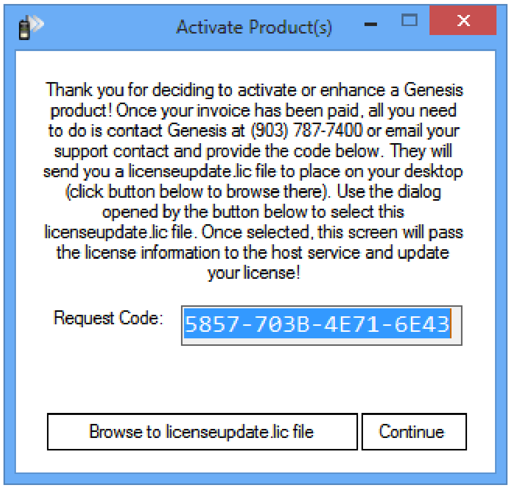
1. Right-click on the GW_Alert icon in the Windows System Tray (see above section for more information on GW_Alert): This will show the GW_Alert menu.
2. Click **GW_LaunchPad** in the GW_Alert menu: This will load GW_LaunchPad. (If you have not activated your license the GenWatch3 License Manager will load in place of GW_LaunchPad. See the section below to activate your license)

You can also load GW_LaunchPad by double-clicking the GW_Alert icon in the Windows System Tray.

Activating the GenWatch3 License

You must activate the GenWatch3 license in order to evaluate GenWatch3 or to set the product as Released after you purchase a license. To activate your license for GenWatch3, follow the steps below:

1. Login to GW_Alert. If GenWatch3 is not licensed, the *Activate Product(s)* window will load directly. If GW_LaunchPad loads, click the **View License** button and then **Activate Product(s)**.
2. Select the ENTIRE code in the **Request Code** box.
3. Right-click on the selected code: This will show an edit pop-up menu with options including **Copy**.
4. Choose **Copy** from the edit pop-up menu.
5. Open your email application and create a new email to support@genesisworld.com.
6. Right-click in the body of the email: This will show an edit pop-up menu with options including **Paste**.
7. 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.
8. Also include in the email your company name and your contact information and/or GenWatch3 PO number.
9. Send the email.
10. Contact Genesis support (see the *Support* section of this manual): They will assist you with the rest of the activation process.



Thank you for deciding to activate or enhance a Genesis product! Once your invoice has been paid, all you need to do is contact Genesis at (903) 787-7400 or email your support contact and provide the code below. They will send you a licenseupdate.lic file to place on your desktop (click button below to browse there). Use the dialog opened by the button below to select this licenseupdate.lic file. Once selected, this screen will pass the license information to the host service and update your license!

Request Code: 5857-703B-4E71-6E43

Figure 2.2 – Activate Product(s)

Chapter 3 Configuring the GW_Security Module

What is GW_Security?

The GW_Security module provides functionality for managing users of your GenWatch3 software. This includes creating, deleting, editing, and managing roles for users.

The GW_Security module provides the user *Admin* with a password specified during install. The role of this user is to allow you to log into GW_LaunchPad and GW_Security with full administrator access. The first step here will be to consider changing the password for the user Admin. This may be desired because all systems shipped with GenWatch3 pre-installed will have the same Admin password.

❌ As with all passwords, keep your GenWatch3 password in a safe place! If you do lose or forget your Administrator password, you will need to get your Database administrator to log into SQL Server and reset the password for the Admin login.

Loading the GW_Security Edit Window

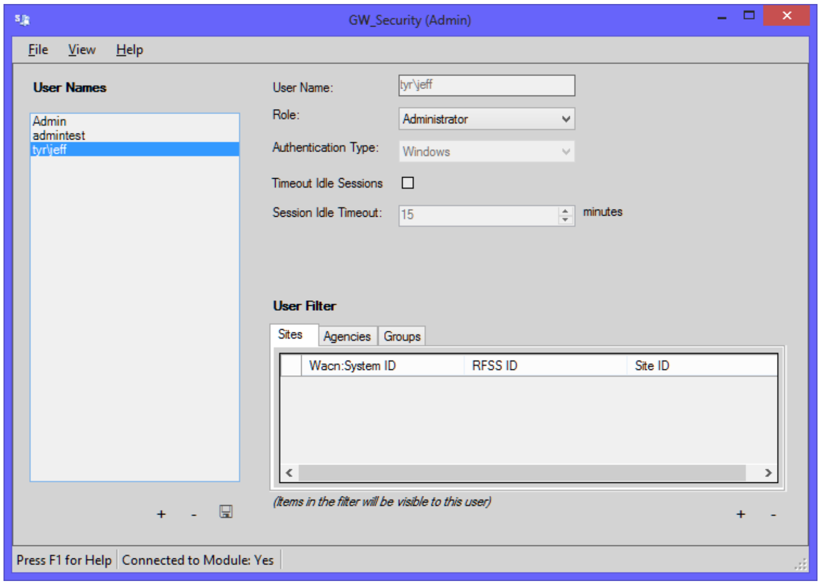
Load the edit window for the GW_Security module by following the steps below:

1. Load GW_LaunchPad (see *Loading GW_LaunchPad* in *Chapter 2 – Getting Started* of this book).
2. Locate the GW_Security module icon in the *Modules* list.
3. Double-click the GW_Security icon: This will load the GW_Security window.

Changing the Password for the Admin User

Change the password for the Admin user by following the steps below:

1. Load the GW_Security GUI (see the above section).
2. Select **Users** from the View menu: This will show the user administration panel.
3. Select the *Admin* user from the **User Names** list.
4. Click on the **Change Password** button.
5. When prompted, enter the current (initial) password for *Admin* (specified during install).
6. Next, enter the desired new password and confirm the password.
7. Click **OK** to finish changing the password.
8. Close the GW_Security window by clicking the **X** button or by clicking **Exit** under the **File** menu.



User Name: tyr\jeff

Role: Administrator

Authentication Type: Windows

Timeout Idle Sessions ☐

Session Idle Timeout: 15 minutes

(Items in the filter will be visible to this user)

Press F1 for Help | Connected to Module: Yes

Figure 3.1 – GW_Security Window

At this time, you can create any other users that are necessary for your system. If you do not create them now, you can always come back to the GW_Security module and create them later. For more information on the GW_Security module, see the *GenWatch3 Core Manual*.

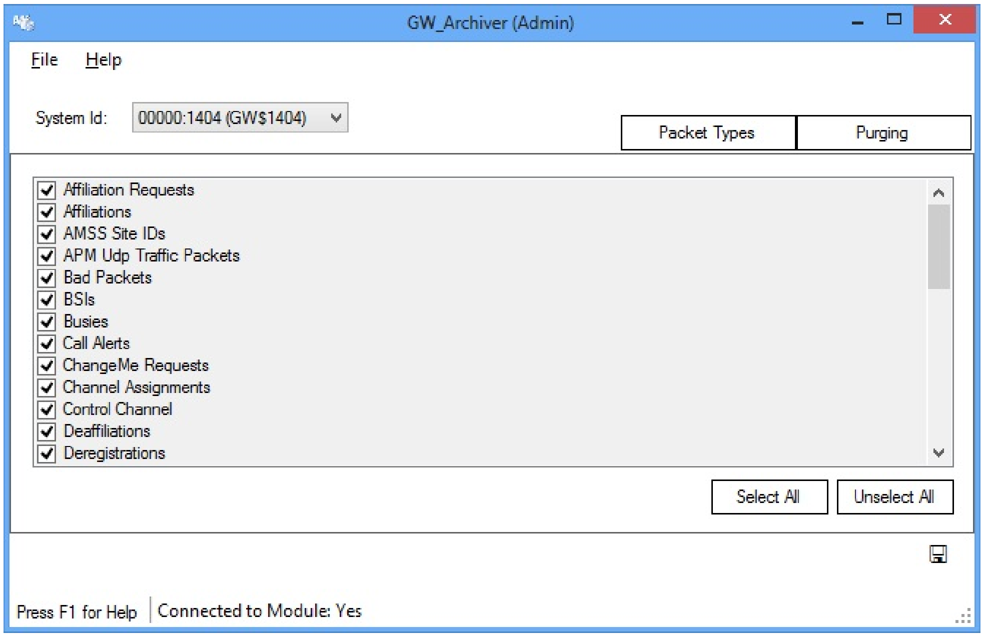
Chapter 4 Configuring the GW_Archiver Module

What is GW_Archiver?

The GW_Archiver module stores control channel packets into data files. Each type of packet is stored in its own table within an SQL database. These databases are queried by the GenWatch3 Reporting Tools.

Since archiving is disk-intensive and can easily consume a large portion of your hard drive, all packet types are set not to archive by default. You will need to activate archiving for the packet types that you wish to store.

The section below describes how to activate archiving.



System Id: 00000:1404 (GW$1404)

☑ Affiliation Requests
☑ Affiliations
☑ AMSS Site IDs
☑ APM Udp Traffic Packets
☑ Bad Packets
☑ BSIs
☑ Busies
☑ Call Alerts
☑ ChangeMe Requests
☑ Channel Assignments
☑ Control Channel
☑ Deaffiliations
☑ Deregistrations

Connected to Module: Yes

Figure 4.1 – GW_Archiver Window

Loading the GW_Archiver Edit Window

Launch the edit window for the GW_Archiver module by following the steps below:

1. Launch the GW_LaunchPad (see *Loading GW_LaunchPad* in *Chapter 2 – Getting Started* of this book).
2. Locate the GW_Archiver module icon in the *Modules* list.
3. Double-click the GW_Archiver icon: This will load the GW_Archiver GUI.

Choosing Archived Packet Types

The GW_Archiver GUI allows you to choose which packet types to archive. Selecting which packets to archive allows you to store the information you want for longer periods of time than if you were archiving everything. For instance, if you only cared about emergency alerts, you could likely store them for many times the life of your system, where if you were archiving everything, you could only store six months' to a year's worth, depending on your system activity.

Follow the steps below to select your archived packet types:

1. Select the system to archive on from the **System Id** drop down list if this installation is licensed for multiple systems.
2. Click the **Packet Types** button. This will show the **Packet Types** panel.
3. Check the box for each packet type that you wish to archive. You can also click the **Select All** button to select all packet types.
4. Click the **Update** button.

Choosing Purging Options

The GW_Archiver module can purge each table in its SQL database at different intervals. Purging is the process by which old information is removed from the database in order to conserve disk space and to increase query efficiency. If you never want to purge a table, then leave that table's purging option as —*Never*—, otherwise, select the interval on which you wish to purge the table.

The options available in the **Purging** tab are limited by the GW_Archiver section of your GenWatch3 license. If you would like to archive data longer than your options allow, please contact GenWatch3 support to learn how to increase your archiving options.

In most situations, setting all tables to be purged at the same time is the best option, as it will give you a consistent view of your database (you will have the same timeframe in the database for all types of data). However, like with selectively archiving packets, you may be able to get more out of your disk space by selectively purging. For instance, if you really care about emergency alarms, you could set them to purge every year, and then set high throughput data, like calls and affiliations, to purge at one month. By purging high throughput data sooner, you can store other data types for longer periods.

Follow the steps below to setup archived data purging:

1. Click the **Purging** button. This will show the **Purging** panel.
2. Select the interval for each archive table or set all purge intervals the same at the bottom of the panel.
3. Click the **Update** button.

Conclusion

Your GenWatch3 solution is now ready for input. Please refer to the GenWatch3 module book that pertains to your system’s data stream. Refer to the list below for a list of system types and their related module books:

- **Motorola Astro P25 or Dimetra via ATIA:** *GenWatch3 GW_ATIA Book*.
- **P25:** *GenWatch3 GW_RSP25 Book*.

If your GenWatch3 package includes the GW_Halcyon module (for RCM and CAD), please reference the following book for additional setup:

GenWatch3 GW_Halcyon Book