



GW3-TRBO®
Installation & Quickstart Guide
Software Version 2.23.5

GW3-TRBO®

Trademarks

The following are trademarks of Motorola: MOTOTRBO™

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

The Genesis Group Trademark Information

GW3-TRBO® 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 GW3-TRBO 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 GW3-TRBO software, nor for any patent infringements or other rights of third parties who may use the manual or the GW3-TRBO 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 GW3-TRBO 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 GW3-TRBO so that we can make it a better product for everyone.

Refer to the *Troubleshooting & Support* section of the GW3-TRBO Manual Shell (Book 600-2.23.5-AA.1) for complete support and contact information.

Document History

Revision	Description	Author
2.0.5	Initial Release	KIH
2.0.5	Replaced GW3-TRBO trademark with registered trademark.	JAW
2.0.6	Updated screenshots with F1 Help	REB
2.0.6	Added Firewall settings section	JAW
2.0.6.6	Revisions before release	WRK
2.1	Revisions before release	WRK
2.2	Addition to Firewall Settings section	CWF
2.2	Document Reviewed	WRK
2.3	Revision Before Release	CWF
2.4	Revision Before Release	CWF
2.5	Revision 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
2.16.15	Updated Chapter 1 with up-to-date install info.	REB
2.17	Updated hyperlinks	DW
2.17.17	Added GET SNMP option	ATG

Table of Contents

Trademarks	3
The Genesis Group Trademark Information	3
Copyright	3
Disclaimer	3
License	3
Support	3
DOCUMENT HISTORY	4
TABLE OF CONTENTS	5
ABOUT THIS MANUAL	7
GOALS	7
WHO SHOULD READ THIS MANUAL?	7
HOW THIS MANUAL IS ORGANIZED	7
CHAPTER 1 INSTALLING GW3-TRBO	9
WARNINGS	9
USING GW3-TRBO WITHOUT A NETWORK	10
MINIMUM HARDWARE SPECIFICATIONS	11
HARDWARE ENHANCEMENT OPTIONS	11
GW3-TRBO SOFTWARE INSTALL	12
Required Software	12
Preparing to Install	12
Install Screens	14
Installation screen	14
Database Only Screen	14
GW Warehouse Screen	15
Installation Folder screen	15
Configuration Screens	17
Configuration Type Screen	17
Optional Features Screen	18
GenGET Database Options Screen	19
GET SNMP Master Agent Options Screen	20
Database Options Screen	21
Database Names Screen	22
Admin Password Screen	23
Service Account Screen	24
REST API Options Screen	24
Configuration Options Screen	25
Ready To Configure Screen	26
SQL Server Express Installation Screens	27
Installation Complete	28
Setting the Service Account Manually	29
SQL Server Security	32
SNMP Configuration	32
GW3-TRBO CLIENT UPGRADE	35
Required Software	35
Preparing to Install	35
REMOTE DATABASE CONFIGURATION	37
FIREWALL CONFIGURATION	38
Windows 10/Server 2016	38
ADVANCED CLIENT SETUP	39
Creating a domain trust relationship	39
Adding a user to a group	39
Adding a Trusted Group	40

AUDIT LOGGING	40
Overview.....	40
Audit Logging Setup.....	40
Config File Options.....	40
SQL Server Security	41
Setup for the Security Admin User	41
SQL Audit Logging Setup via SQL Script.....	42
Viewing Audit Activity.....	43
CHAPTER 2 GETTING STARTED	45
LOADING ALERT.....	45
LOGGING INTO ALERT	46
LOADING LAUNCH.....	47
ACTIVATING THE GW3-TRBO LICENSE	47
CHAPTER 3 CONFIGURING THE SECURITY MODULE	49
WHAT IS SECURITY?.....	49
LOADING THE SECURITY EDIT WINDOW	49
CHANGING THE PASSWORD FOR THE ADMIN USER.....	49
CHAPTER 4 CONFIGURING THE ARCHIVER MODULE	51
WHAT IS ARCHIVER?.....	51
LOADING THE ARCHIVER GUI.....	51
CHOOSING ARCHIVED PACKET TYPES	51
CHOOSING PURGING OPTIONS	52
CONCLUSION	52

Goals

This document guides you through the GW3-TRBO installation and initial setup process. After you complete the steps in this document, you will be ready to configure the input module(s) that GW3-TRBO 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 GW3-TRBO should read this manual.

How This Manual Is Organized

This manual is organized as follows:

- **Installing GW3-TRBO:** Describes the process of installing GW3-TRBO.
- **Getting Started:** Instructions on logging into Alert and beginning the GW3-TRBO evaluation.
- **Configuring the Security Module:** Instructions on changing the default *Admin* login.
- **Configuring the 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:



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:

- **Warnings:** Provides some warnings about GW3-TRBO configurations.
- **Minimum Hardware Specifications:** Describes where to find the hardware configuration required to support a GW3-TRBO installation.
- **Hardware Enhancement Options:** Describes additional hardware options.
- **GW3-TRBO Software Install:** Provides detailed instructions for installing and licensing the GW3-TRBO 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 change the name of the GW3-TRBO host computer, you must restart the GW3-TRBO service.



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. GW3-TRBO is shipped with a freeware version of Microsoft SQL Server (SQL Server Express). SQL Server Express is limited to a 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 GW3-TRBO machine must use an English-language version of Microsoft Windows.



The GW3-TRBO machine must not use a comma as a decimal symbol in the Number Format under Regional Settings.



The GW3-TRBO machine must not use hyphens in the Date Format under Regional Settings.



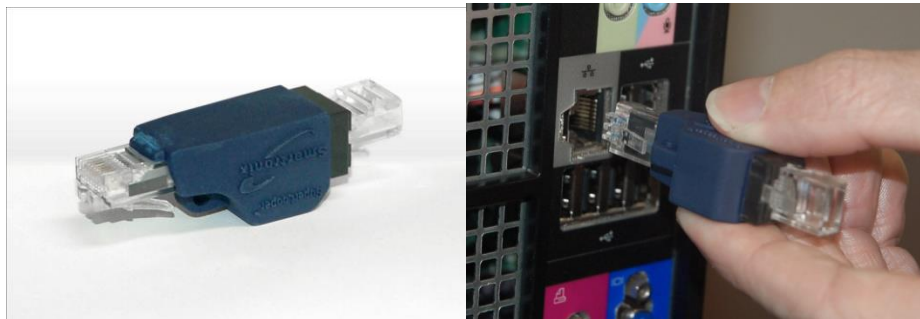
The GW3-TRBO machine (client or host) must be a member of a Microsoft Windows network. GW3-TRBO relies on DNS resolution for the TCP/IP and SQL connections that it uses. If the machine running GW3-TRBO is not a member of a network, the GW3-TRBO software will not function properly unless you follow the instructions below.



The GW3-TRBO service must always be running. Please disable hibernation on the host machine.

Using GW3-TRBO Without a Network

GW3-TRBO requires a network connection. If you need to use GW3-TRBO on a machine that is **not** connected to a network, you must install a loopback adapter. A hardware loopback adapter has been included with your GW3-TRBO host machine. Connect the adapter to the machine's Ethernet port as shown below.



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

Windows 10

1. Right-click the **Start** menu icon and select **Run**.
2. Enter the text "hdwwiz.exe" and click **OK**. This will load the *Add Hardware Wizard*.
3. Click the **Next** button.
4. Select **Install the hardware that I manually select from a list (Advanced)** and click **Next**.
5. Select **Network Adapters** from the list and click **Next**.
6. Select **Microsoft** from the list of manufacturers.
7. Select **Microsoft KM-TEST Loopback Adapter** from the **Model** list and click **Next**.
8. Click **Next**. Windows will install the loopback adapter.
9. Click **Finish**.

Minimum Hardware Specifications

See <https://genesishworld.com/resources/specs-trbo/>

Hardware Enhancement Options

There is no such thing as *too much power*. The following hardware options will improve the performance of GW3-TRBO:

- **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 GW3-TRBO 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 1,000 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 speed will increase the performance of the machine.

GW3-TRBO Software Install

To begin the software installation process, browse to the installer directory and double-click on *Start.hta*.

Required Software

In order to support GW3-TRBO, 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.

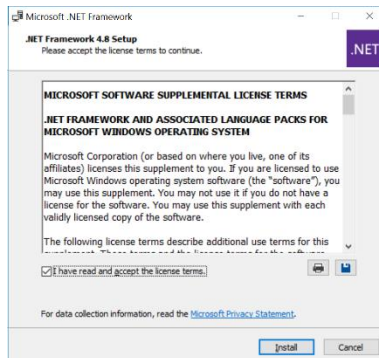


Figure 1.1 – .NET Framework Installer

GW3-TRBO 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 GW3-TRBO installation process.

Preparing to Install

After the .NET Framework is installed, the **GW3-TRBO Installer** will launch. The *Welcome* window in Figure 1.2 allows you to begin the installation process or launch any of the installation guides included with the installer.



Figure 1.2 – GW3-TRBO Welcome window

When you click **Launch Setup**, the GW3-TRBO 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 installer 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.

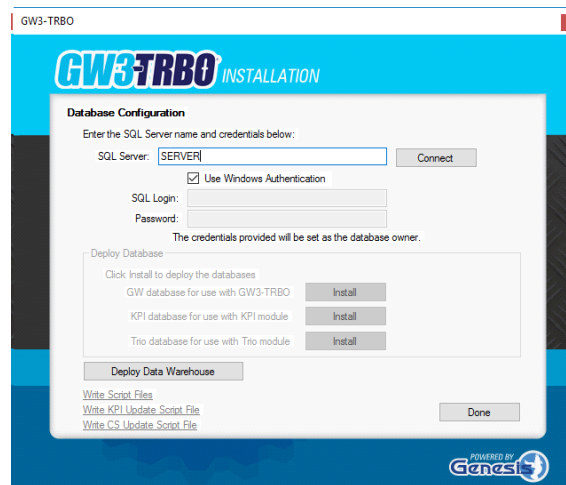


Figure 1.4 – Database Only screen

- **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 GW3-TRBO 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.

Figure 1.5 – GW Warehouse screen

Installation Folder screen

If you select **GW3-TRBO 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.

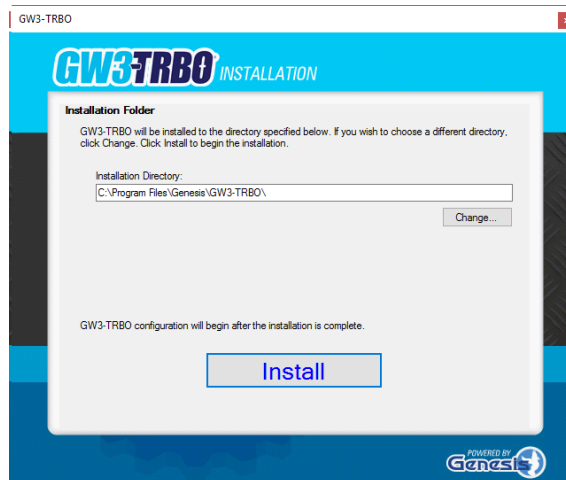


Figure 1.6 – Installation Folder Screen

Click **Install** to install the GW3-TRBO application files to the chosen directory. You will see a progress bar as GW3-TRBO is installed. Once complete, you will be able to configure the installation and the *Setup Type* screen will be shown.

Configuration Screens

Configuration Type Screen

At the *Configuration Type* screen (Figure 1.7) choose the type of GW3-TRBO installation you wish to perform: **Host** or **Client**.

- **Host:** Select **Host** to install the GW3-TRBO service and the GW3-TRBO interfaces. If GW3-TRBO will be installed on one machine, select **Host**.
- **Client:** Select **Client** to install only the GW3-TRBO interfaces. These are used to display information processed and stored by a GW3-TRBO host.

Click **Next** to continue.



Figure 1.7 – Configuration Type screen

Optional Features Screen

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

Additional features:

- **Trio:** This option should be selected if the Trio module has been purchased to use on this GW3-TRBO installation.
- **Setup SNMP Master Agent:** This option should be selected if this GW3-TRBO installation needs to be able to send SNMP messages.
- **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.



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 displays only if the **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**
 - **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 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.



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 displays only if the **Setup SNMP Master Agent** option was selected on the *Optional Features* screen.

Click **Next** to continue.

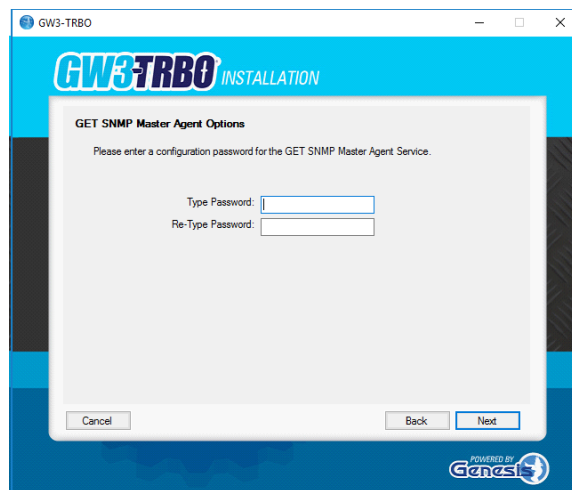


Figure 1.10 – GET SNMP Master Agent Options screen

Database Options Screen

The *Database Options* screen (Figure 1.11) allows you to choose a 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 GW3-TRBO data warehouse. Refer to the *GW Warehouse Screen* section earlier in this chapter for details.

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

Click **Next** to continue.

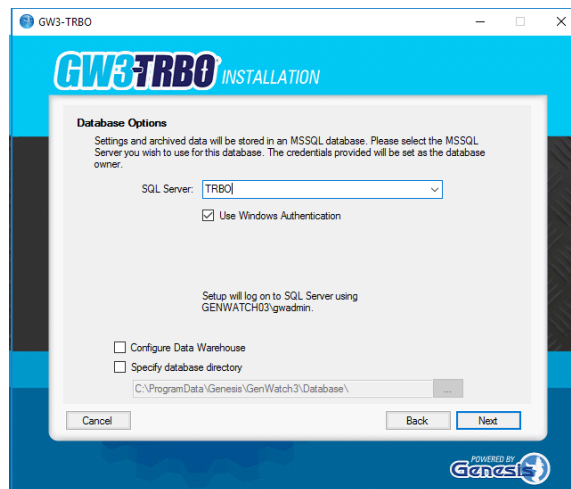


Figure 1.11 – Database Options screen



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 GW3-TRBO. Renaming the databases is optional and you can continue the setup without changing them.

Click **Next** to continue.

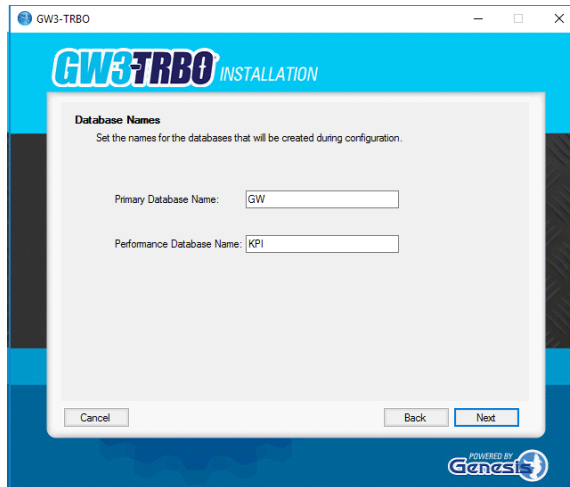
The image shows a software installation window titled "GW3-TRBO". The window has a blue header with the "GW3TRBO" logo and the word "INSTALLATION". The main content area is titled "Database Names" and contains the instruction "Set the names for the databases that will be created during configuration." There are two text input fields: "Primary Database Name:" with the value "GW" and "Performance Database Name:" with the value "KPI". At the bottom of the window, there are three buttons: "Cancel", "Back", and "Next". The "Next" button is highlighted in blue. In the bottom right corner, there is a logo that says "POWERED BY Genesys".

Figure 1.12 – Database Names screen

Admin Password Screen

The *Admin Password* screen (Figure 1.13) prompts you to set the *Admin* account password. The *Admin* account is created during the installation and is used to log in to GW3-TRBO when the installation is complete.

Click **Next** to continue.

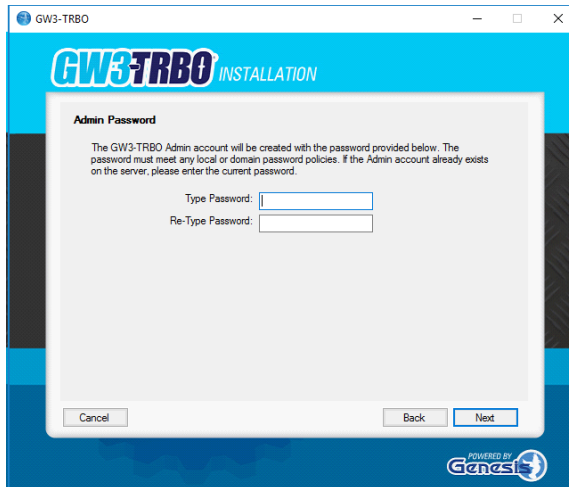


Figure 1.13 – Admin Password screen



The password provided must meet the password policy in SQL Server. Some policies require a combination of uppercase, lowercase and numeric values.



GW3-TRBO creates the *Admin* login on the SQL Server instance and associates it with the *Admin* user it also creates in the Primary and Performance (and Trio, if selected) GW3-TRBO databases. This is not a Windows login user.

Service Account Screen

The *Service Account* screen (Figure 1.14) prompts you to set the credentials for the GW3-TRBO service. The same credentials are used for the GET SNMP Master Agent service if it is installed. A SQL login is automatically added for the credentials specified.

Click **Next** to continue.

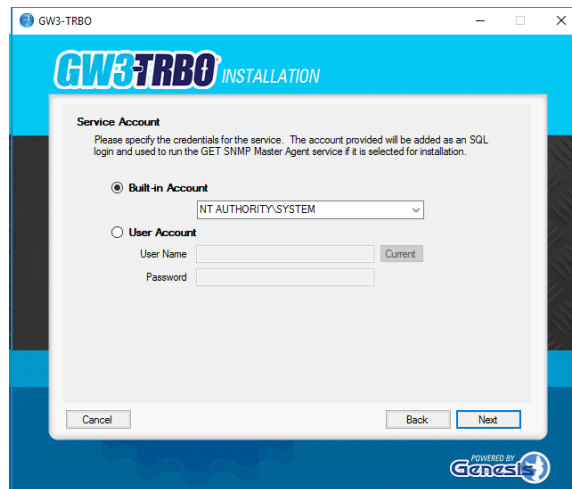


Figure 1.14 – Service Account screen

REST API Options Screen

The *REST API Options* screen (Figure 1.15) prompts you to set the port for the REST API. This API is used for communication between GW3-TRBO and the Genesis iVista and GenGET products.

Click **Next** to continue.

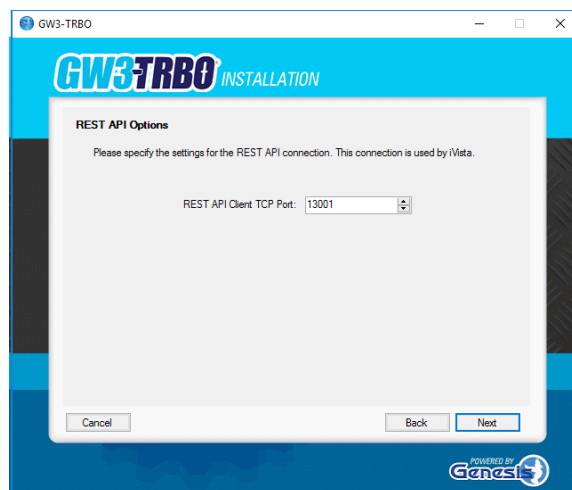


Figure 1.15 – REST API screen

Configuration Options Screen

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

Click **Next** to continue.

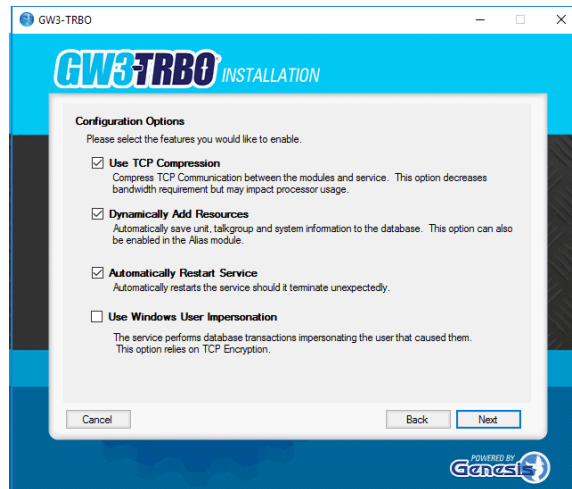


Figure 1.16 – Configuration Options screen



The **Use Windows User Impersonation** option requires any Windows user that logs into GW3-TRBO to have the same SQL server and database permissions as that of the account under which the GW3-TRBO service runs. These permissions are listed below:

- For each of the databases created by GW3-TRBO (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 GW3-TRBO.
- 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 GW3-TRBO service account, as SQL Server will prevent the service from impersonating a user with more permissions than itself.

Ready To Configure Screen

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

Click **Apply** to begin configuring GW3-TRBO.

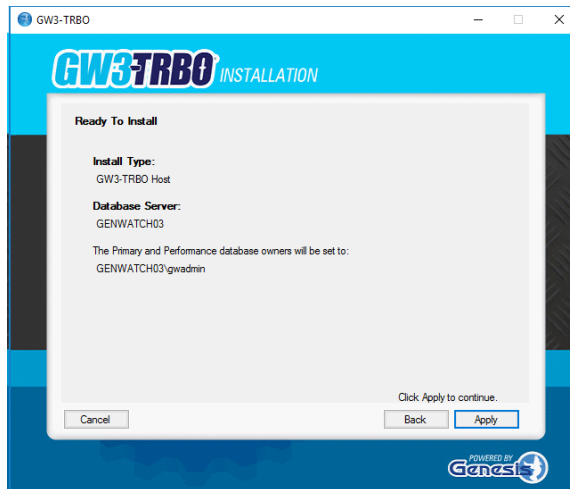


Figure 1.17 – *Ready to Configure* screen

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.

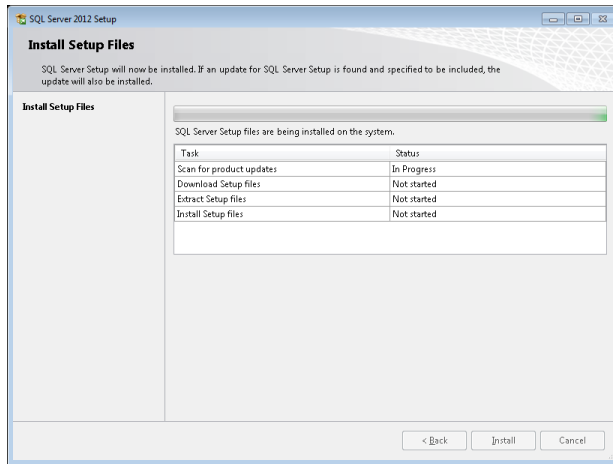


Figure 1.18 – SQL Server Express Installation

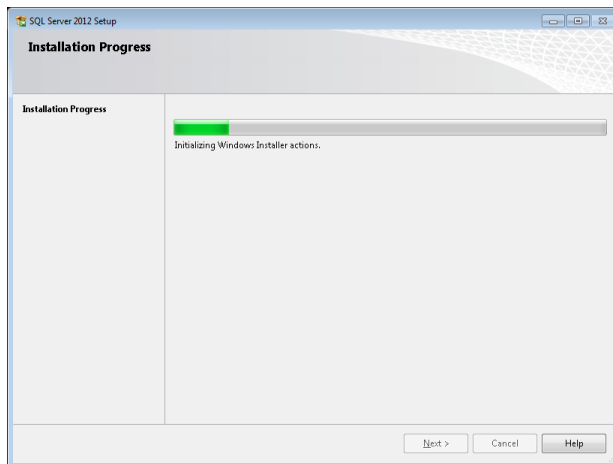


Figure 1.19 – SQL Server Express Installation Progress

Please wait while the configuration completes. You will see the *Configuration in Progress* screen (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.

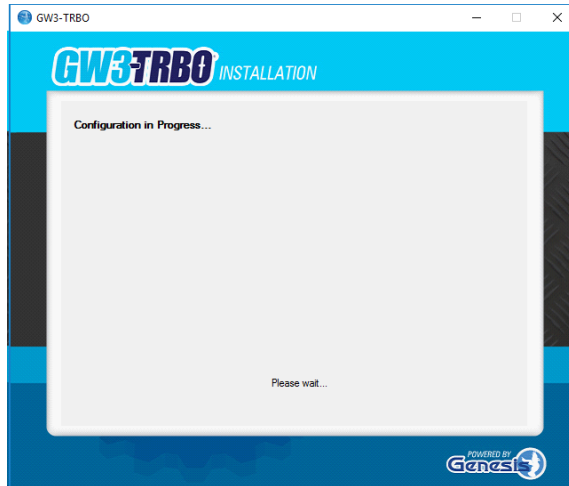


Figure 1.20 – *Configuration in Progress* screen

Installation Complete

When the configuration finishes, you will see the *Configuration Complete* screen (Figure 1.21).

Click **Finish** to exit the setup program.

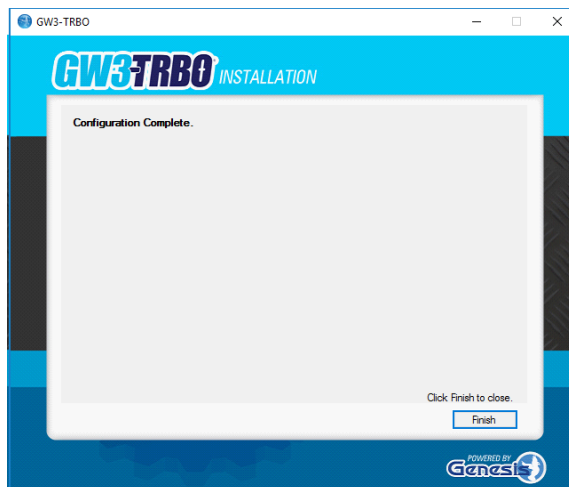


Figure 1.21 – *Configuration Complete* screen

You will notice that GW3-TRBO shortcuts have been added to your desktop and start menu. Alert has also been added as a Start Up app to ensure the GW3-TRBO interfaces start with Windows.

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

Please see the following chapters of this document for instructions on launching and configuring GW3-TRBO.

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.

1. First ensure the desired account has the following privileges:
 - a. Windows Privileges
 - i. **Full control** of the GW3-TRBO 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 GW3-TRBO clients connected to the GW3-TRBO host.
 - a. Each GW3-TRBO client must close all modules and exit Alert.
 - b. Verify from the GW3-TRBO 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.

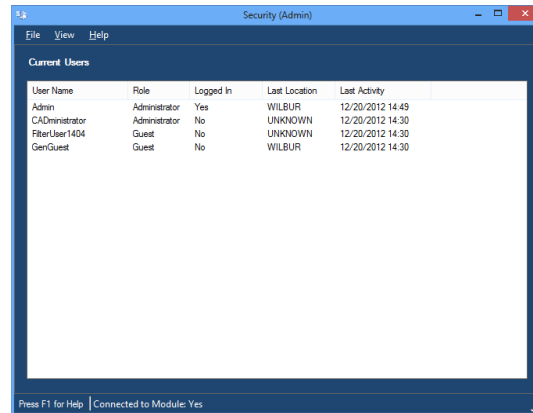


Figure 1.22 – Current Users List

- c. Close all modules on the host machine and exit Alert.
3. Stop the GW3-TRBO service.
 - a. Right-click the **Start** menu and select **Computer Management**.
 - b. Select **Services** under **Services and Applications**, then select **GenWatchService**.
 - c. Click the **Stop Service** button. (Figure 1.23)
 - d. Leave this window open.

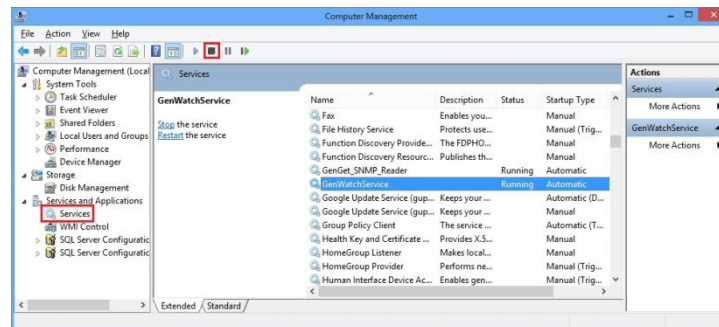


Figure 1.23 – Computer Management → Services

4. Update the GW3-TRBO service 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)

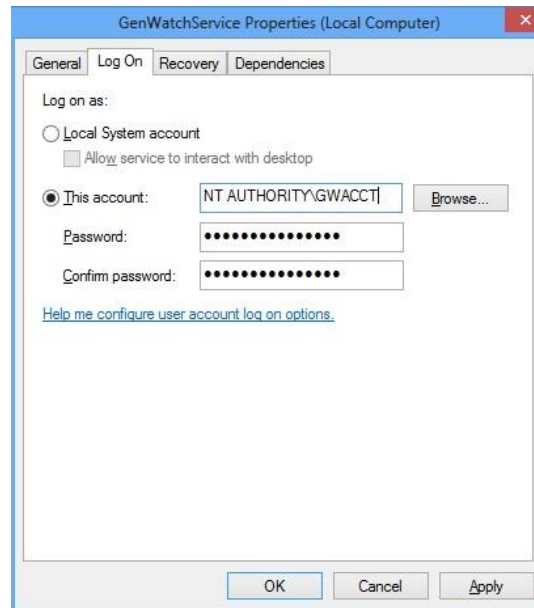


Figure 1.24 – Update the Account credentials

5. Start the GW3-TRBO Service.
 - a. Within Computer Management, select **GenWatchService**.
 - b. Click the **Start Service** button. (Figure 1.25)

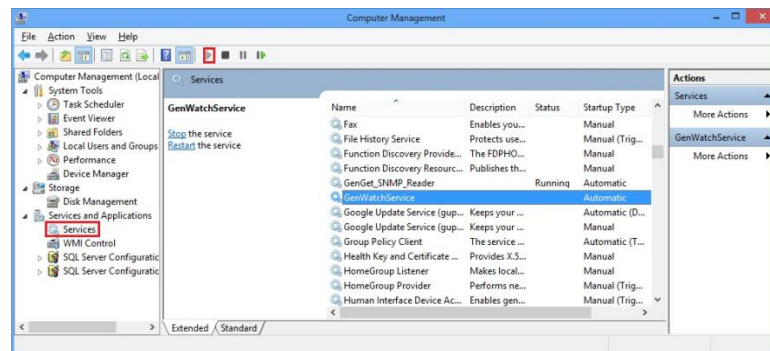


Figure 1.25 – Starting the GW3-TRBO Service

6. Log in to the GW3-TRBO host and ensure the service is running properly.
7. Update any passwords saved in connections in GW3-TRBO.
8. Inform GW3-TRBO clients that they may now launch Alert and connect to the host machine.

SQL Server Security

The GW3-TRBO service 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. Log in 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* box 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* for use with GW3-TRBO. If you do not intend on using SNMP functionality within GW3-TRBO, you may skip this section.

Install the Windows features for SNMP available in **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, you can start the *GETSNMPMasterAgentService* via the *Computer Management* window (Figure 1.26). To access this window, right-click on the **Start** menu **Computer Management**. Then expand **Services and Applications** and select **Services**. Select the *GETSNMPMasterAgentService* and click the **Start Service** button.

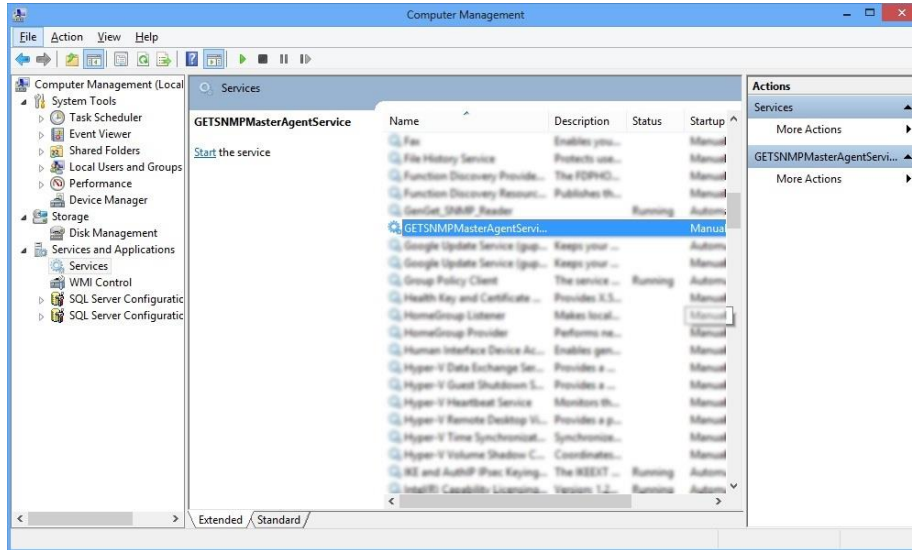


Figure 1.26 – Computer Management

Browse to the GenGET Master Agent Settings directory using Windows Explorer (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*

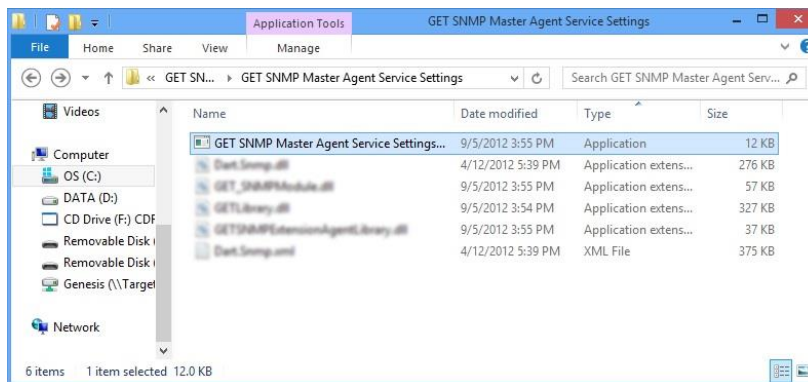


Figure 1.27 –Master Agent Settings Directory

The *Master Agent Settings* window (Figure 1.28) will be displayed after you select the configuration file. Set the **Local Address** setting to the machine's IP address. Then, click **Add User** under the **Security** tab to create the SNMP v3 user. Click **OK** to save the changes.

The screenshot shows the 'Master Agent Settings' window with the 'Agent' tab selected. The 'Community' field is set to 'GenesisSNMP'. The 'Local Address' is set to 'Any IPv4' and the 'Local Port' is '161'. The 'Engine ID Payload' is 'GETSNMPMasterAgent'. The 'Final Engine ID' is a long hexadecimal string. The 'Inform Enabled' checkbox is unchecked, with a 'Repetition Rate (seconds)' of '5' and an 'Expiration Time (seconds)' of '20'. The 'Trap Destination List' contains one entry with 'IP Address' '255.255.255.255' and 'Port' '162'. The 'Version' section on the right has 'SNMPv3' selected. 'Ok' and 'Cancel' buttons are at the bottom right.

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.

GW3-TRBO Client Upgrade

To begin the client upgrade process, insert (if on DVD or USB) or browse to the GW3-TRBO installation media. If the GW3-TRBO 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 GW3-TRBO, 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.

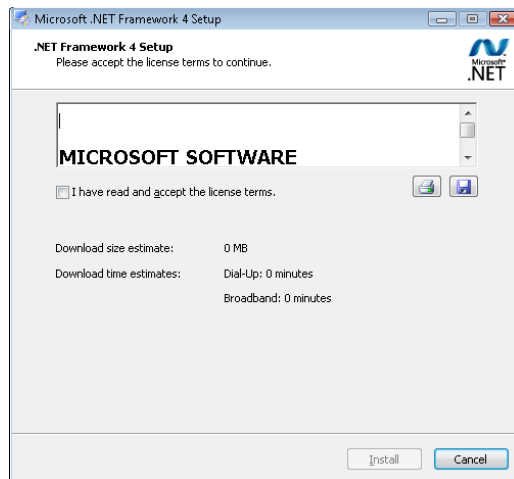


Figure 1.29 – .NET Framework Installer.

Preparing to Install

After the .NET Framework is installed or upgraded as needed, the **GW3-TRBO Installer** will launch. The *Upgrade* screen in Figure 1.30 allows you to begin the upgrade process.



Figure 1.30 – Upgrade Screen

Click on **GW3-TRBO Upgrade** to begin the upgrade process. Please wait for the process to complete upgrading.

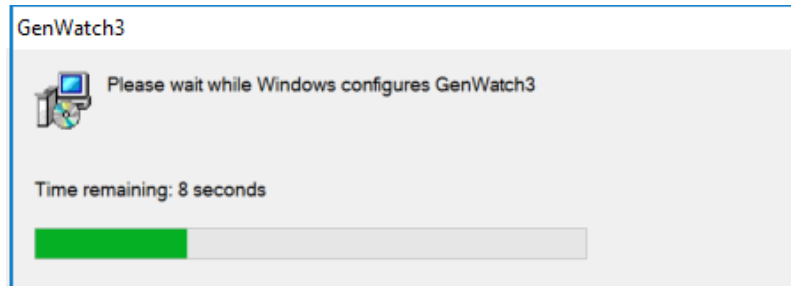


Figure 1.31 – Upgrade in progress

Click **Finish** to exit the client upgrade program.

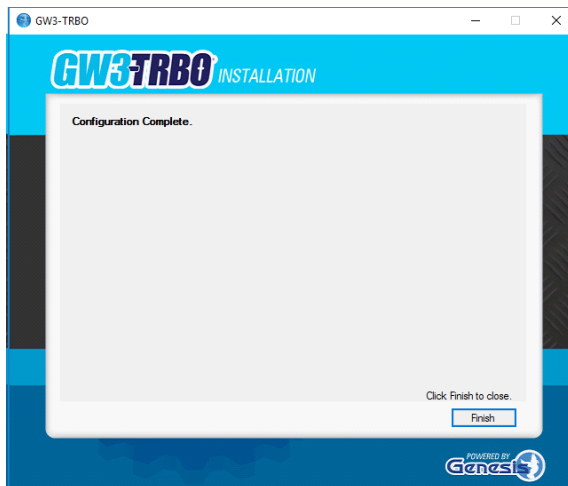


Figure 1.32 – Upgrade Complete

Remote Database Configuration

Remote database configurations require a dedicated user for the GW3-TRBO 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 GW3-TRBO host and database machines. To create this user, open the **Control Panel** and select **User Accounts**, then **User Accounts** (this menu has the same name as the previous one), then open **Manage another account** and click **Add a user account** (Figure 1.33).

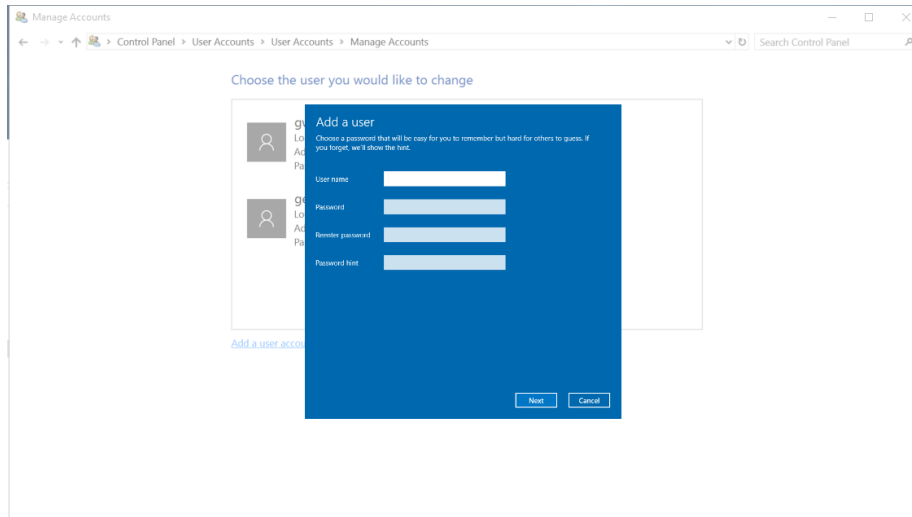


Figure 1.33 – Navigation to User Accounts

You must allow the GW3-TRBO service user and any additional client users to access the database machine over the network. On the database machine, open the **Control Panel** and select **System and Security**, then launch the **Administrative Tools**. Then, launch the *Local Security Policy* window and select **User Rights Assignment** under **Local Policies** (Figure 1.34).

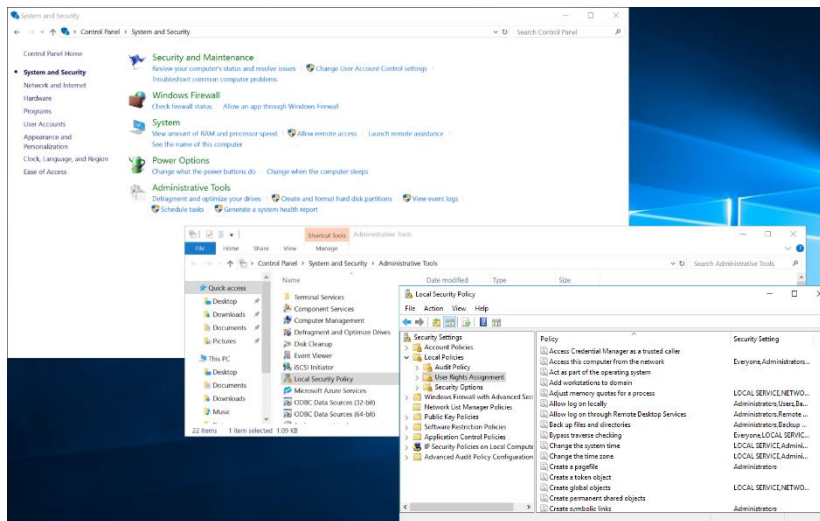


Figure 1.34 – Navigation to Local Security Policy

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)

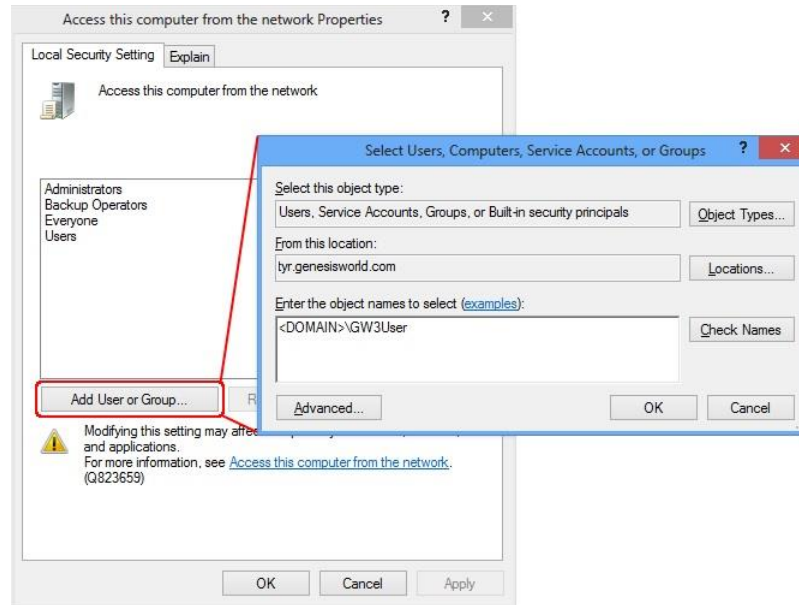



Figure 1.35 – Adding users to the policy

 If you have many users to add, consider creating a new group for GW3-TRBO users. You can then add that group to the policy above, thus giving all its members access.


Finally, during the GW3-TRBO Host installation, specify the GW3-TRBO service user on the *Service Account* screen (Figure 1.13). 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 GW3-TRBO 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:

Control Panel → System and Security → Windows Firewall (or Windows Defender Firewall) → Advanced Settings

To add a program or port range to the Windows Firewall exception list:

1. Click **Inbound Rules** to display the inbound exceptions list.
2. Click **New Rule...** to launch the *New Inbound Rule Wizard*.
3. Follow the instructions within the *New Inbound Rule Wizard*. When complete, the new program or port exception will appear within the inbound exceptions list.

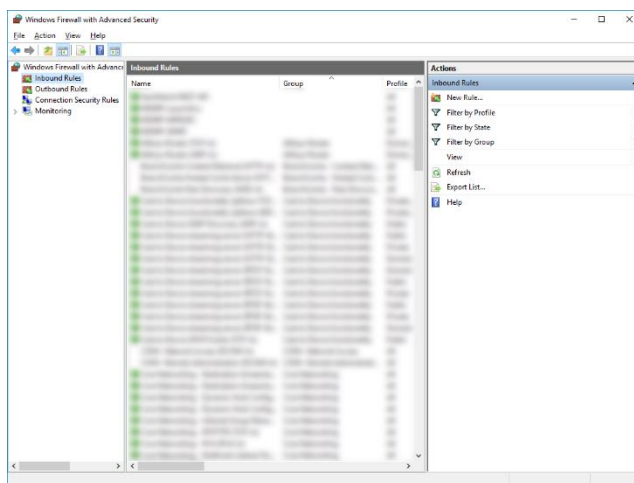


Figure 1.36 – Windows Firewall Advanced Settings



A rule for the SQL Server Browser service may be necessary if the instance of SQL GW3-TRBO is running in is not the default instance.

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 predefined 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/Server 2016: Right-click on the **Start** button → Click **Computer Management** (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 to.
- 4. Click **Add** on the properties window and enter the username to be used on the client machine(s) and click **OK**.
 - 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/Server 2016: **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/Server 2016: **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 available only 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 predetermined categories of SQL activity, such as adds, inserts and deletes. Each timestamped 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, rollover, 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 GW3-TRBO 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 GW3-TRBO-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 GW3-TRBO, you must add the Windows user as a login to SQL. To add a Windows user for security administration in GW3-TRBO 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* box 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.
15. Execute the following SQL query to grant impersonation permissions for the Windows login. Replace <Windows login> with the Windows login created above. Replace <GW3-TRBO Service Account> with the account under which the GW3-TRBO service runs:

```
USE [master]
GRANT IMPERSONATE ON LOGIN::[<Windows login>] to [<GW3-TRBO 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 GW3-TRBO on your machine, you are ready to configure your GW3-TRBO modules for operation on your system. Follow the steps below to configure GW3-TRBO:

- **Chapter 2:** Loading Alert
- **Chapter 2:** Logging into Alert
- **Chapter 2:** Loading Launch
- **Chapter 2:** Activating the GW3-TRBO license (skip if your machine came pre-licensed)
- **Chapter 3:** Configuring the Security module
- **Chapter 4:** Configuring the Archiver module (if you purchased Archiver)

Loading Alert

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). Alert will show one of the following icons:

- : This icon indicates that the Alert application is running and is currently connected to the GW3-TRBO service.
- : This icon indicates that the Alert application is running and is not currently connected to the GW3-TRBO service.

The GW3-TRBO Installer places a shortcut to Alert to the Windows Startup Apps. This means that when Windows starts up (after reboot, power off, etc.), Windows loads Alert automatically.

If you do not see one of the above icons in your Windows System Tray, you may need to start Alert. To start Alert take the following steps:

1. Click on the Windows **Start** menu.
2. Click on **Genesis**
3. Click the **Launch** icon. This will load Alert and show one of the above icons in the System Tray.

Logging into Alert

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

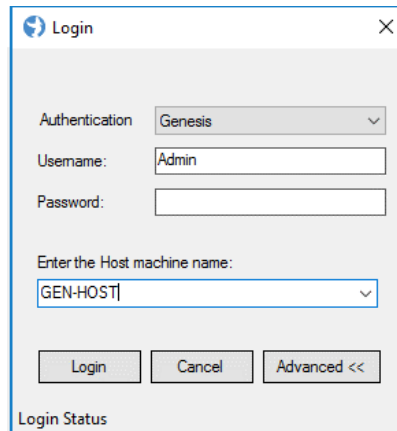


Figure 2.1 – GW3-TRBO Login Window

This window contains the following items or note:

- **Authentication:** Type of authentication used to log into GW3-TRBO. Options include **Genesis** and **Windows**.
- **Username:** GW3-TRBO username you wish to log in with. This box will contain the username that last logged in.
- **Password:** Password of the GW3-TRBO user.
- **Host Machine Name:** Enter the GW3-TRBO host machine name here. This entry is “remembered” after the initial login.
- **Cancel:** Click this button to cancel login and not load Alert.
- **Login:** Click this button once you have entered or verified the **Username** and **Password**.
- **Advanced:** Displays or hides the host entry field.



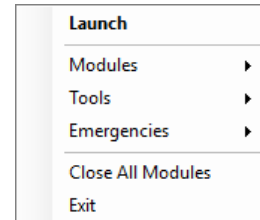
GW3-TRBO uses your login information provided in this *Login* window for Launch and all other GW3-TRBO windows. In Launch, click the **Switch User** item under the **File** menu to log in as a different user.

Loading Launch

Launch is your entry point for GW3-TRBO and is therefore important to all GW3-TRBO users. From it you will launch all modules, configure database and host settings, and manage your license. Launch will automatically load each time you log in to Alert.

To load Launch, follow the steps below:

1. Right-click on the Alert icon in the Windows System Tray (see above section for more information on Alert). This will show the Alert menu.
2. Click **Launch** in the Alert menu. This will load Launch. (If you have not activated your license, the GW3-TRBO License Manager will load in place of Launch. See the section below to activate your license.)



You can also load Launch by double-clicking the Alert icon in the Windows System Tray.

Activating the GW3-TRBO License

You must activate the GW3-TRBO license in order to evaluate GW3-TRBO or to set the product as Released after you purchase a license. To activate your license for GW3-TRBO, follow the steps below:

1. Log in to Alert. If GW3-TRBO is not licensed, the *Activate Product(s)* window will load directly. If Launch loads, click the **View License** button and then **Activate Product(s)** (Figure 2.2).
2. Select the ENTIRE code in the **Request Code** box.
3. Right-click on the selected code. This will show a context menu with options including **Copy**.
4. Choose **Copy** from the context menu.
5. Open your email application and create a new email to support@genesishworld.com.
6. Right-click in the body of the email. This will show a context menu with options including **Paste**.
7. Choose **Paste** from the context 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 GW3-TRBO 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.

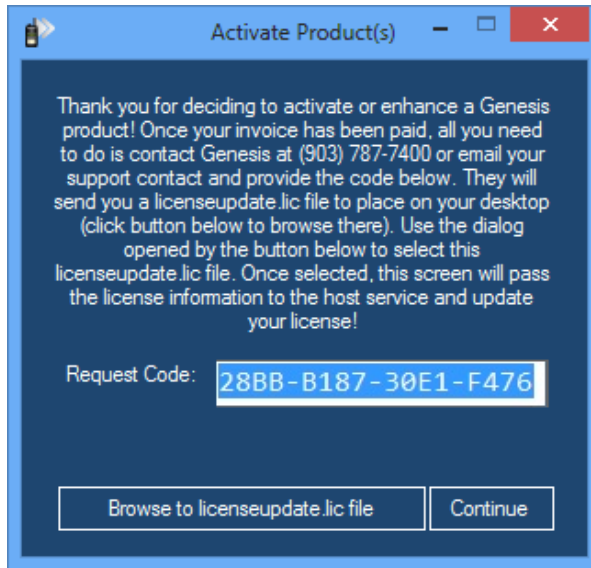


Figure 2.2 – Activate Product(s) window

What is Security?

The Security module provides functionality for managing users of your GW3-TRBO software. This includes creating, deleting, editing, and managing roles for users.

The Security module provides the user *Admin* with a password specified during install. The role of this user is to allow you to log into Launch and 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 GW3-TRBO pre-installed will have the same *Admin* password.



As with all passwords, keep your GW3-TRBO 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 Security Edit Window

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

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

Changing the Password for the Admin User

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

1. Load the Security GUI.
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 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 Security GUI by clicking the **X** button or by clicking **Exit** under the **File** menu.

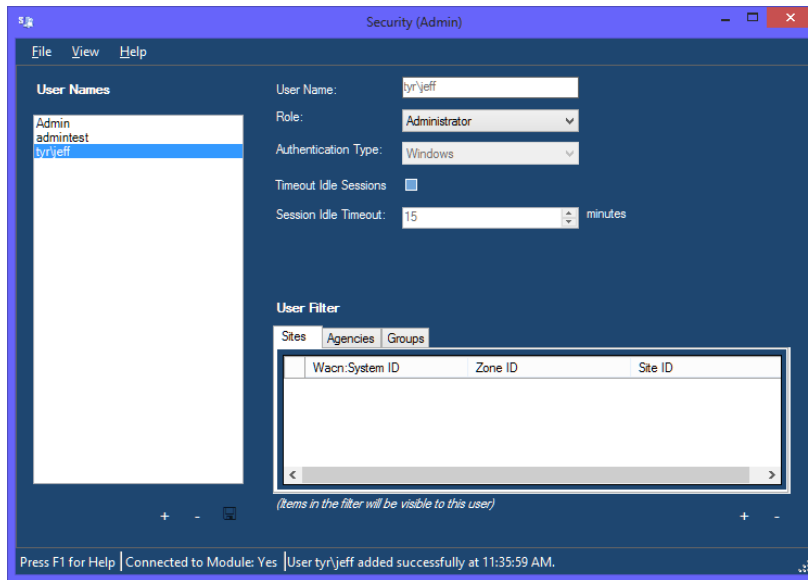


Figure 3.1 – Security GUI



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 this GUI and create them later. For more information on the Security GUI, see the *GW3-TRBO Core Manual*.

What is Archiver?

The Archiver module stores activity packets into data files. Each type of packet is stored in its own table within an SQL database. These databases are queried by the GW3-TRBO 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 when shipped. You will need to activate archiving for the packet types that you wish to store.

The section below describes how to activate archiving.



Figure 4.1 – Archiver GUI

Loading the Archiver GUI

Launch the GUI for the Archiver module by following the steps below:

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

Choosing Archived Packet Types

The 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, whereas if you were archiving everything, you could store only six months' to a year's worth, depending on your system activity.

Follow the steps below to select your archived packet types:

1. Click the **Packet Types** button. This will show the **Packet Types** panel.
2. 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.
3. Click the **Update** button.

Choosing Purging Options

The 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 Archiver section of your GW3-TRBO license. If you would like to archive data longer than your options allow, please contact GW3-TRBO 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 time frame 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, 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 set up 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 GW3-TRBO solution is now ready for input. Please refer to the *Trbo Module Book* or *Connect Module Book* to set up your system's data stream.