



**GenWatch3<sup>®</sup>**  
**GW\_Archiver**  
**Software Version 2.3**  
**Module Book**

---

**GenWatch3<sup>®</sup>**

**600-2.3.0-H.1**  
**4/8/2011**



## 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

Copyright © 2011; 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  
601 Shelley Dr., Suite 202  
Tyler, Texas 75701.

Includes technology licensed from Motorola.

## Disclaimer

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

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

## License

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

Refer to the GenWatch3 Manual Overview for your full license. All license information contained on pages 4-7 (Book 600-2.3.0-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 600-2.3.0-AA.1) for complete support and contact information.

## ***Document History***

<b>Revision</b>	<b>Description</b>	<b>Author</b>
2.0.2	Initial Release	JAW
2.0.3	Updated Screenshots	CBH
2.0.3	Added the Forensic Reporting chapter	JAW
2.0.3	Revision before release	JAW
2.0.3	Added a description for Archived Systems tab	JAW
2.0.4	Added process for repairing orphan users for database restored from one PC to another	JAW
2.0.4	Updated Purging Options	KIH
2.0.5	Revision before release	TDW
2.0.6	Updated screenshots with F1 Help image	REB
2.0.6	Updated screenshots	CLB
2.0.6.6	Changes before release	WRK
2.3	Revision Before Release	CWF

# Table of Contents

---

<i>Trademarks</i> .....	3
<i>The Genesis Group Trademark Information</i> .....	3
<i>Copyright</i> .....	3
<i>Disclaimer</i> .....	3
<i>License</i> .....	3
<i>Support</i> .....	3
DOCUMENT HISTORY .....	4
<b>TABLE OF CONTENTS</b> .....	<b>5</b>
<b>ABOUT THIS MANUAL</b> .....	<b>7</b>
GOALS .....	7
WHO SHOULD READ THIS MANUAL? .....	7
HOW THIS MANUAL IS ORGANIZED .....	7
TERMS .....	9
WHAT IS THE GW_ARCHIVER? .....	9
SYSTEM ID .....	9
PACKET TYPE SETTINGS .....	9
PURGING SETTINGS .....	10
<i>Date-Based Purging</i> .....	10
<i>Log Purging Option</i> .....	12
DATABASE DOWN FUNCTIONALITY .....	12
<b>CHAPTER 2 FORENSIC REPORTING</b> .....	<b>13</b>
LOADING THE SQL SERVER MANAGEMENT STUDIO APPLICATION .....	14
PERFORMING A DATABASE BACKUP.....	15
PERFORMING A DATABASE RESTORE .....	17
<i>Special Case – Restore from One PC to Another</i> .....	19
<i>Restore Cleanup</i> .....	20



### Goals

This document describes the role and function of the GW\_Archiver module in the GenWatch3 solution.

### Who Should Read This Manual?



This manual is written for an expected audience of mid-level PC users. Reporting and archiving personnel should read this manual.

### How This Manual Is Organized

This manual is organized as follows:

- **Overview:** Describes the GW\_Archiver module and options available in the GW\_Archiver GUI (Graphical User Interface).
- **Forensic Reporting:** Describes the process of backing up and restoring the GenWatch3 database in order to satisfy forensic reporting needs.

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 describes the GW\_Archiver module and options available in the GW\_Archiver module configuration screen.

This chapter contains the following sections:

- **Terms:** Describes basic terms related to GW\_Archiver.
- **What is GW\_Archiver?:** Describes the GW\_Archiver module.
- **System ID:** Describes the GW\_Archiver system ID selection feature.
- **Packet Type Settings:** Describes the GW\_Archiver packet type settings.
- **Purging Settings:** Describes the GW\_Archiver purging settings.
- **Database Down Functionality:** Describes GW\_Archiver behavior when disconnected from the database.

## Terms

**Archiving:** Writing data to a database. This data is available through reporting.

**Packet:** Data received from a GenWatch3 input.

**Decode:** The act of converting 0s and 1s into readable data.

**Purging:** Deleting data from the database. This is generally based on time, where all data older than x hours, days, months, etc. is deleted. This operation frees up room in the database and allows reporting to run more efficiently.

## What is the GW\_Archiver?

The GW\_Archiver module *archives decoded* GenWatch3 input *packets* to an SQL database. The GW\_Archiver GUI allows you to manipulate the following categories of GW\_Archiver settings on a per-system basis:

- **Packet Types:** The types of packets that are archived.
- **Purging:** Options for *purging* archived data. Purging data manages the amount of hard drive space the database consumes.

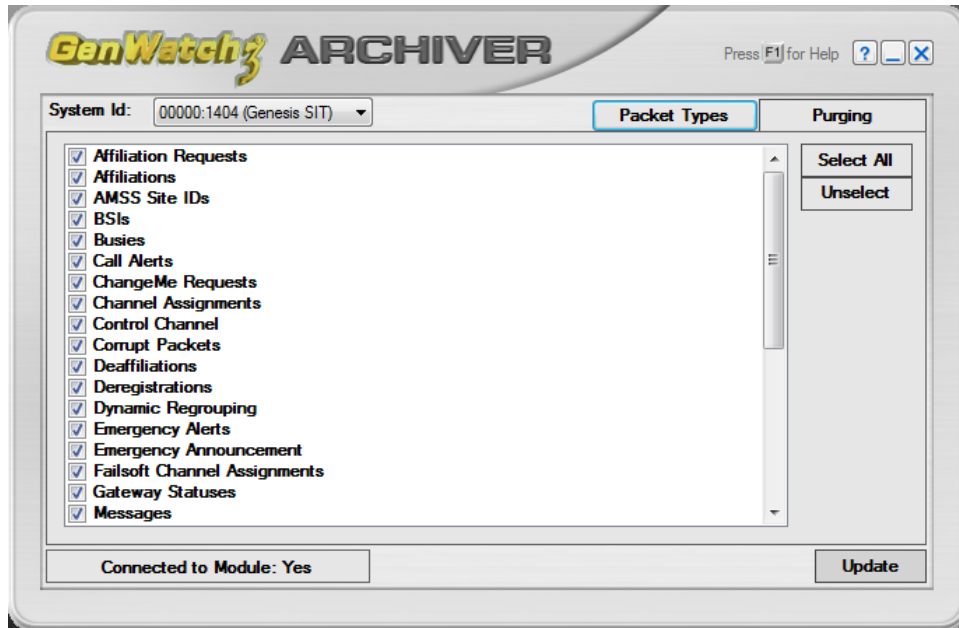
## System ID

This feature allows you to choose separate GW\_Archiver options for each of your licensed systems. The **System ID** list contains a System ID and alias for each of your licensed systems. GW\_Archiver's **Packet Types** and **Purging** panels show the GW\_Archiver options for the system ID selected in the **System ID** list.

## Packet Type Settings

The packet type list, under the **Packet Types** tab, contains an entry for each archived packet type. If a packet type in this list is checked, then that packet type

is archived to the SQL database by the GW\_Archiver module. If it is not checked, then it is not archived.



**Figure 1.1** – GW\_Archiver Packet Types Options



Many of the GenWatch3 reports rely on the data in the Channel Assignments table. If these packets are not archived, then many of the reports will not show data. Genesis recommends archiving all packet types.

## **Purging Settings**

### **Date-Based Purging**


The purging settings inform the GW\_Archiver module when data should be deleted from the archive tables in the SQL database. Tables in the GW database that begin with the prefix ARC\_ are archive tables. The purging table list, in the **Purging** tab, contains an entry for each archive table in the GW database.

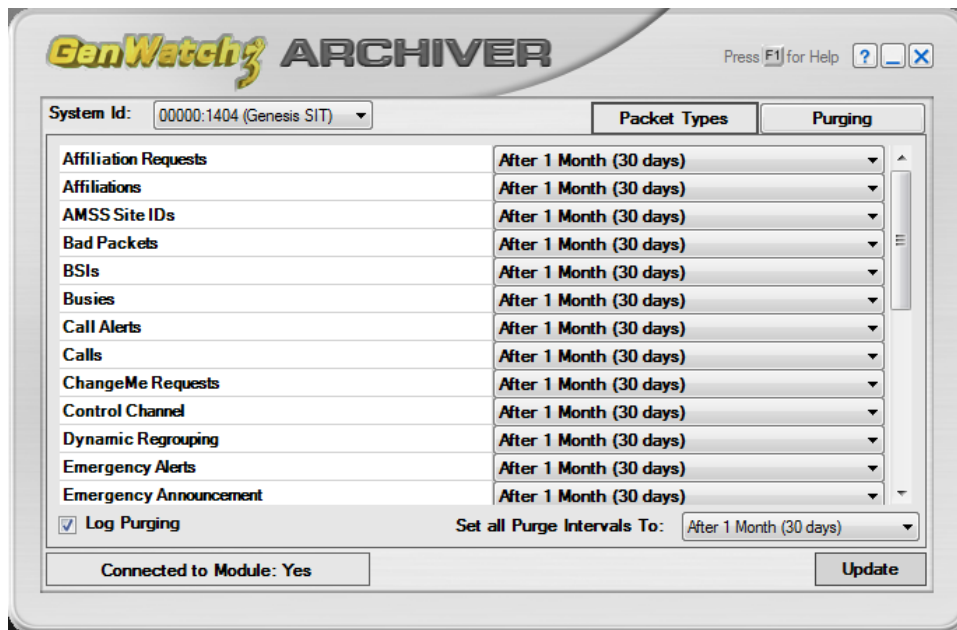
Each table has its own separate purge setting. The GW\_Archiver module performs purging when the module is started and every hour after it is started. If a table contains records older than its purging option, then these records are permanently deleted during the hourly purging operation.

Purge duration options include:

- -- Never --
- After 1 hour
- After 4 hours
- After 12 hours
- After 1 day
- After 2 days
- After 1 week
- After 2 weeks
- After 1 month (30 days)
- After 3 months (90 days)
- After 6 months (180 days)
- After 1 year (365 days)

Your purging options should reflect your reporting needs. If your biggest report is a monthly report, then set purging to occur every 3 months. If your biggest report is a bi-weekly report, then set purging to occur every month. Regular purging will allow your reports to run more quickly.

 Packet types with a purging interval of After 2 Weeks or longer are kept for an additional 7 days. This allows you to set the purge interval to After 1 Month and still have 6-7 days to run your monthly reports before data is purged.



**Figure 1.2** – GW\_Archiver Screen – Purging Options

Select a purge interval in the **Set All Purge Intervals To** list to set all of the above purge intervals to the selected purge interval.

## Log Purging Option

Each hour GW\_Archiver performs a purge operation. This operation compares the timestamp of the archived data with the current time of the GenWatch3 machine that is hosting the GenWatch3 service. GW\_Archiver deletes each record with a timestamp that differs from the machine time by greater than the date-based purging option selected for the record's type.

For example, if you selected *After 6 months (180 days)* for *Affiliations*, each hour GW\_Archiver will delete each affiliation record archived more than 187 days ago (down to the second, and including the 7 days of padding applied to all intervals greater than 2 weeks).

If the **Log Purging** option is checked on this screen, GW\_Archiver module will report:

- When the purging operation begins.
- When the purging operation ends, reporting the results of the purging operation (number of records purged for each archive table purged).

These results will show in the Windows event viewer (in the *GenWatch* event log) and are sent via the GW\_SysLog module. See the GW\_SysLog section of the *GenWatch3 Core manual* for more information on GW\_SysLog.

Chapter 2 describes how to backup data so that you can do forensic reporting on data more than your allowed archiving time period.

## Database Down Functionality

In remote database configurations of GenWatch3, GW\_Archiver is designed to continue operation while the database is down or unreachable due to network issues. While the database is unavailable, GW\_Archiver queues archive records in memory and, if needed, to the disk drive. Once the database is restored, the queued records are written to the database.

As described in the previous chapter, GW\_Archiver limits the amount of time archived data is stored in the GW database. This section contains detailed instructions on how to backup data and restore backed up data, so that you may report on data that is older than your allowed archiving time period.

This chapter contains the following sections:

- **Loading the SQL Server Management Studio Application:** Describes the steps required to load the SQL Server Management application.
- **Performing a Database Backup:** Describes the steps required to perform a GenWatch3 database backup.
- **Performing a Database Restore:** Describes the steps required to perform a restore of a GenWatch3 database backup.

## Loading the SQL Server Management Studio Application

Backups and restores are performed in the SQL Server management studio application. These steps are referenced in the Performing a Database Backup section and Performing a Database Restore sections of this chapter.

To load this application, follow the steps below:

1. Click the Windows **Start** button: This will show the Start menu.
2. Click the **All Programs** or **Programs** item: This will show the program folders and programs installed on this machine.
3. Click the **Microsoft SQL Server** item: This will show the program folders and programs under this category.
4. Click on **SQL Server Management Studio Express** or **SQL Server Management Studio**: This entries name will vary between SQL Server Express and SQL Server for Workgroups. This will load the SQL Server management application.



5. The SQL Server management application will show the *Connect to Server* dialog. Enter the Server Name (GenWatch3 database machine name), select *Windows Authentication* for *Authentication* and click the **Connect** button. This will connect you to the SQL Server instance on the selected server name.



**Figure 2.1** – Connect to Server dialog

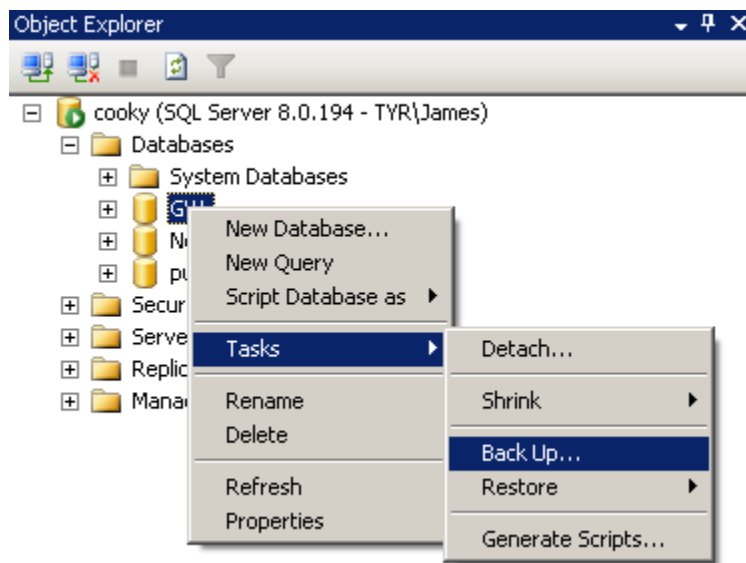
## Performing a Database Backup

A database backup is a snapshot of your database at a given point in time. This operation creates a copy of your database while it is still archiving data. This process will result in a single file. This file can be 3.5 gigabytes or greater in size, depending on your system activity.

It is best to store these files off-site or at least off of the GenWatch3 machine, as they can act as a complete database backup as well as a forensic reporting archive.

To backup your GenWatch3 database, follow the steps below:

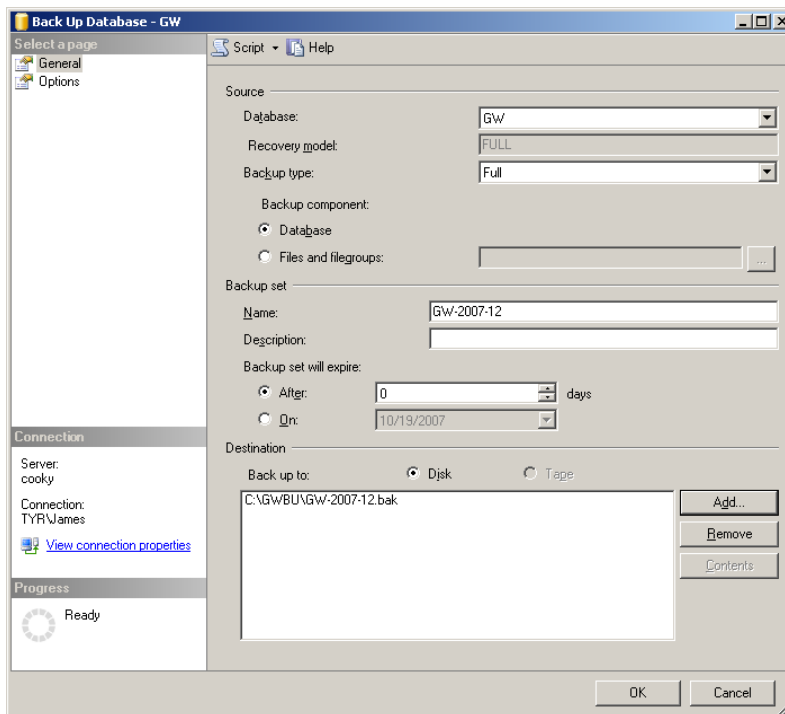
1. Load the SQL Server management application: This is described in the *Loading the SQL Server Management Studio Application* section of this chapter.
2. In the **Object Explorer** section of the SQL Server management screen, expand the **Databases** item: This will show all of the databases under this SQL Server instance, including the **GW** database.
3. Right-click on the **GW** database: This will show the database options menu.
4. Click the **Tasks** option: This will show the Tasks options menu.



**Figure 2.2** – Tasks options

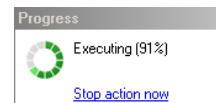
5. Click the **Backup...** option: This will show the *Back Up Database* screen.
6. Under the **Backup set** section, change the **Name** to GW-<yyyy-mm> where yyyy = the 4-digit year and mm = the 2-digit month: For example, a backup performed on 12-31-2007 would be named GW-2007-12.

- In the **Destination** section, click the **Remove** button: This will remove the default destination entry.



**Figure 2.3** – Back Up Database dialog

- In the **Destination** section, click the *Add...* button: This will show the *Select Backup Destination* screen.
- In the **File name** section, type the backup destination. The destination drive can be any writeable hard drive, such as local hard disk or an external hard disk. The drive must be local to this machine. Network drives are not supported. The folder that you choose must already exist on the drive that you choose. Name the backup file *GW-yyyy-mm.BAK* where yyyy is the 4-digit year and mm is the 2-digit month. For example, a backup performed on 12-31-2007 would have a destination named *GW-2007-12.BAK*.
- Click **OK** to confirm the file name: This will close the *Select Backup Destination* screen and return you to the *Back Up Database* screen.
- Click the **OK** button: This will perform the backup process. (Notice the progress of this operation in the Progress section)
- Once this process is complete, you are ready to move your GenWatch3 database backup file from the destination location to an off-site location.



## Performing a Database Restore

A database restore is a process used to make forensic data temporarily available for reporting. This process restores a database backup file to the GenWatch3 machine's SQL Server instance. After a restore, you may use GW\_Reports to select the restored database as the data source.



If you are restoring a GW database that was backed up on a different PC than you are restoring to, please see the Special Case section below.

To perform a GenWatch3 database restore, follow the steps below:

1. Load the SQL Server management studio application: This is described in the *Loading the SQL Server Management Studio Application* section.
2. In the *Object Explorer* section of the SQL Server management screen, right-click in the *Databases* item: This will show the Databases options menu.
3. Click the *Restore Database...* option: This will show the *Restore Database* screen.

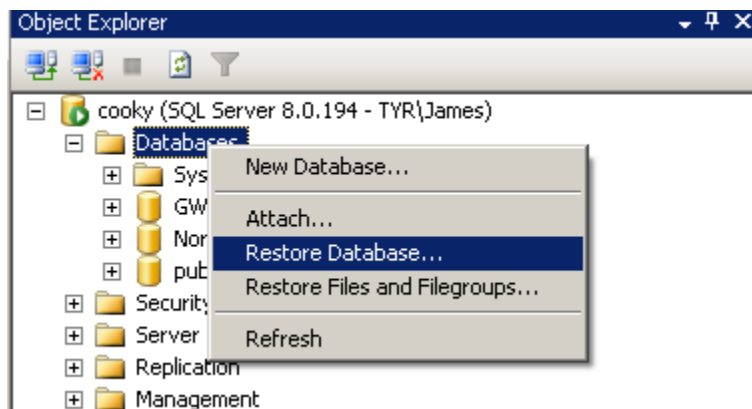
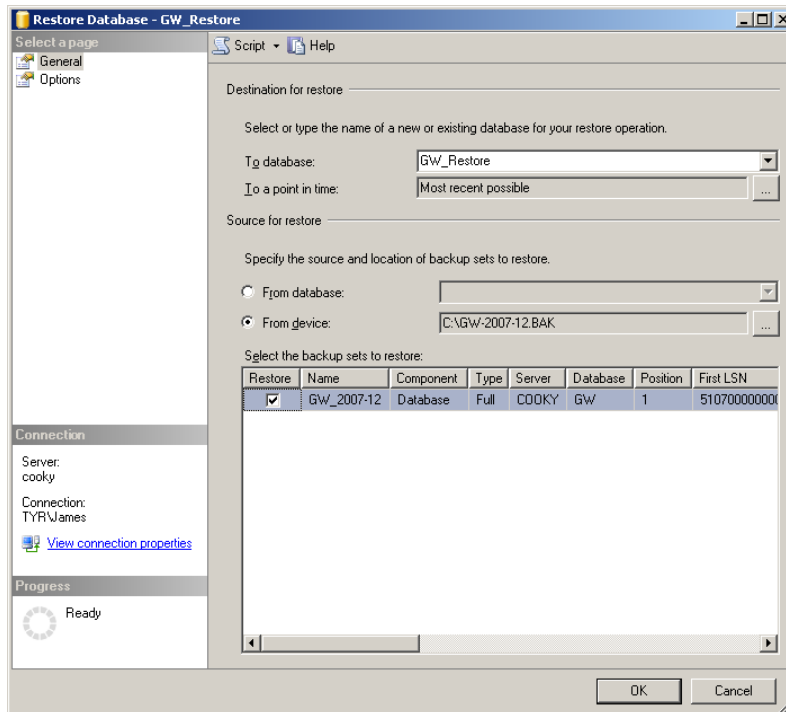



Figure 2.4 - Object Explorer

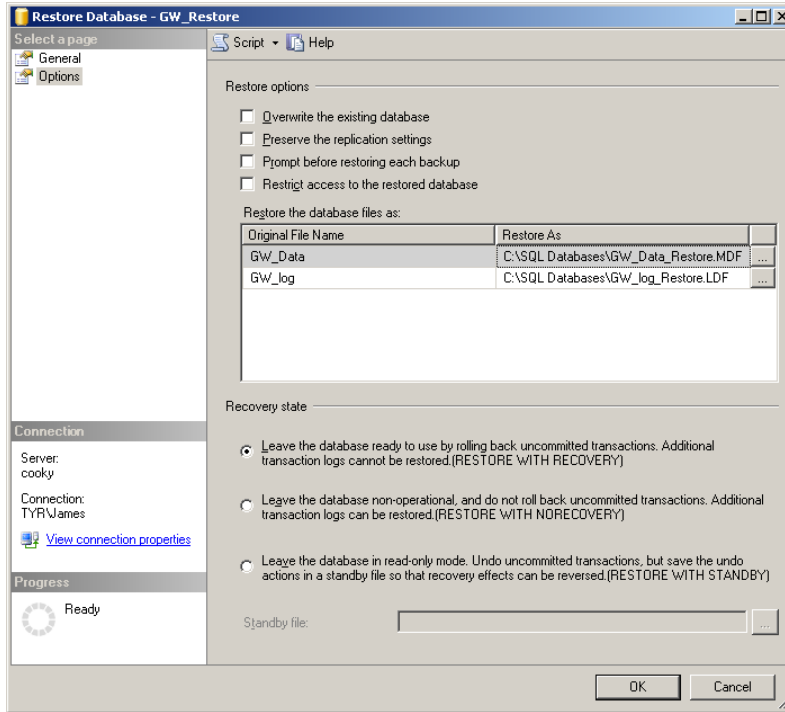
4. Under the *Destination for restore* section, type **GW\_Restore**.
5. In the *Source for restore* section, select the *From device* option.
6. Click the  button at the end of the *From device* option: This will load the *Specify Backup* screen.
7. In the *Specify Backup* screen, for the *Backup media* option, choose **File**.
8. Click the *Add* button: This will show the *Locate Backup File* screen.
9. Click on your backup file (created via the Database Backup process) and press the *OK* button: This will return you to the *Specify Backup* screen.
10. Click *OK* in the *Specify Backup* screen: This will return you to the *Restore Database* screen and populate the *Select the backup sets to restore* list with one entry.

- Click the checkbox in the *Restore* column of the *Select the backup sets to restore* list.



**Figure 2.5** – Restore Database dialog

- In the *Select a page* section, click on the *Options* item: This will show the Restore options panel.
  - In the *Restore the database files as* section, click on the *Restore As* column for the *GW\_Data* entry: This will allow you to modify the file name.
  - Change the Restore As file name to **GW\_Data\_Restore.MDF**.
  - Click on the *Restore As* column for the *GW\_Log* entry. This will allow you to modify the file name.
  - Change the *Restore As* file name to **GW\_Log\_Restore.LDF**.
-  Ensure that the files *GW\_Data\_Restore.MDF* and *GW\_Log\_Restore.LDF* files do not already exist in the Restore As folder.

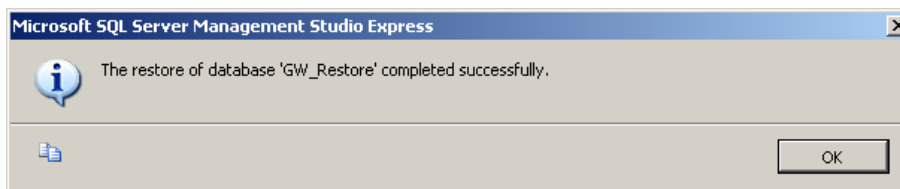


**Figure 2.6** – Restore Database dialog

17. Click the **OK** button: This will perform the restore process. (Notice the progress of this operation in the Progress section)



18. Upon completion, SQL Server management shows a dialog stating that the restore is complete.



**Figure 2.7** – Restore Complete dialog

19. You can now choose the *GW\_Restore* database as a reporting source in GW\_Reports.

### Special Case – Restore from One PC to Another

If you backup a GW database on one PC and restore it to another, you must perform additional setup to map the SQL Server Logins to the users in the restored database. Restoring the GW database to a machine that has never hosted the GW database will require even further setup. Please contact GenWatch3 support for further instructions.

## Restore Cleanup

Once you have completed your forensic reporting, cleanup is required. This process ensures that the next time you need forensic reporting, you can perform a restore without having to worry about pre-existing restored databases.



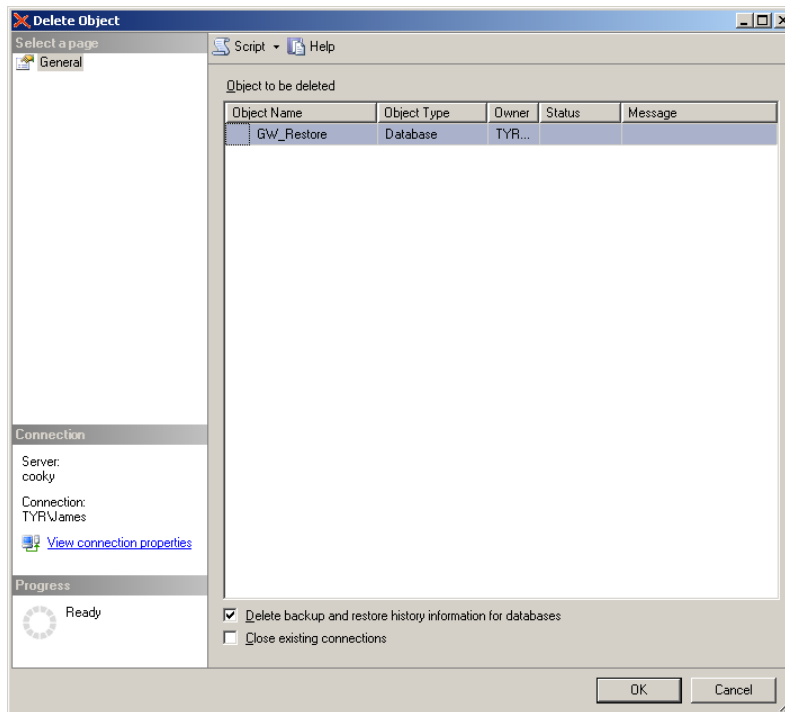
If the Restore Cleanup process is not performed, the Restore Database process may fail.



You must close the GW\_Reports screen and all Microsoft Excel instances that reported on the GW\_Restore database before performing these steps

To perform restore cleanup, follow the steps below:

1. Load the SQL Server management studio application: This is described in the *Loading the SQL Server Management Studio Application* section.
2. In the **Object Explorer** section of the SQL Server management screen, right-click on the *GW\_Restore* database: This will show the Databases options menu.
3. Click on the **Delete** option: This will show the *Delete Object* screen.



**Figure 2.8** – Delete Object dialog

4. Uncheck the **Delete backup and restore history information for databases** option.
5. Click the **OK** button: This will detach the database from the SQL Server instance and delete the files created in the *Restore Database* process.