GenWatch3®
Disaster Recovery Plan
Software Version 4.26.1

600-4.26.1-DRP.1
2/24/2026

Trademarks

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 © 2012-2026; Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks. All rights are reserved. No part of this publication or the associated program may be reproduced, transmitted, transcribed, in whole or in part, in any form or by any means, whether it is mechanical, magnetic, optical, electronic, manual, or otherwise, without the prior written consent of Burks GenCore Co., Inc. D.B.A:
The Genesis Group and Phil Burks
5800 Eagles Nest Blvd
Tyler, Texas 75703

Includes technology licensed from Motorola.

Disclaimer

The GenWatch3 Disaster Recovery Plan 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 600-4.26.1-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 this manual for complete support and contact information.

Document History

Revision	Description	Author
Revision #1.0	Initial Release	Michael Rainer
2.6	Version Update	CWF
2.7	Revisions Before Release	JAW
2.8	Revisions Before Release	WRK
2.9	Revisions Before Release	KIH
2.9	Revisions Before Release	JAW
2.9	Revisions Before Release	TDW
2.10	Revisions Before Release	JPS
2.11	Revisions Before Release	JPS
2.12	Revisions Before Release	JPS
2.13	Conversion to docx	BCY
2.14	Revisions Before Release	JAW
2.15	Revisions Before Release	REB
2.16	Revisions Before Release	JPS
2.17	Add Appendix F PC Name Change Procedures	JPS
2.17	Update formatting	DEW

Table of Contents

Trademarks *3*
The Genesis Group Trademark Information *3*
Copyright *3*
Disclaimer *3*
License *3*
Support *3*
DOCUMENT HISTORY 5

TABLE OF CONTENTS 7

ABOUT THIS MANUAL 9

GOALS 9
WHO SHOULD READ THIS MANUAL? 9
HOW THIS MANUAL IS ORGANIZED 9

CHAPTER 1 INTRODUCTION 11

PREAMBLE 12
OBJECTIVES 13
UNDERPINNING PRINCIPLES 13
UPDATING THIS PLAN 13
DISTRIBUTION OF THIS PLAN 13
DEFINITIONS 13

CHAPTER 2 PREVENTION AND PREPAREDNESS 15

PREVENTION 16
Possible Threats *16*
Network Loss 16
Database Loss 16
Software/PC Loss 16
PC Name Change 17
Prevention Summary 17
PREPAREDNESS 17
Identification of the Disaster Response Team *17*
Training of a Disaster Response Team *17*
Identification of Recovery Work Areas *18*
Ensuring availability of equipment and software *18*

CHAPTER 3 REACTION 19

IMMEDIATE RESPONSE 20
Identify the Emergency *20*
Assess the Situation *20*
Report the Emergency Incident (using the contact information in Appendix B) *20*
Immediate Actions *20*
Role of Data Recovery Personnel *21*
Immediate Stabilization *21*
PLANNING THE RECOVERY 21

CHAPTER 4 RECOVERY 23

IMPORTANT PRINCIPLES FOR ALL RECOVERY PERSONNEL 24
ROLES 24
Data Recovery Personnel *24*
Data Backup Personnel *24*
IT Staff Main Contact(s) *24*
Hardware Recovery Personnel *25*

Network Recovery Personnel *25*
RECOVERY SCENARIOS 25
GenWatch3 ..... *25*
Database Loss 25
PC Name Change 25
Hardware/Software Loss 25
Network Loss 25
iVista *26*
Database Loss 26
PC Name Change 26
Hardware/Software Loss 26
Network Loss 26
Trio *26*
Database Loss 26
Hardware/Software Loss 26
Network Loss 26

CHAPTER 5 RESTORATION, REHABILITATION, AND RE-EVALUATION 27

REHABILITATION 28
Role of Hardware Recovery Personnel *28*
Role of the Network Recovery Personnel *28*
RESTORATION 28
Role of the Database Backup Personnel *28*
RESTORATION PROCEDURES 28
GenWatch3 ..... *28*
iVista *28*
Trio *28*
POST-EMERGENCY AND RE-EVALUATION 29

APPENDIX A REFERENCES 31

REFERENCES 31

APPENDIX B PLAN DISTRIBUTION LIST 33

DISTRIBUTION LIST 33

APPENDIX C DISASTER RESPONSE TEAM 35

DISASTER RESPONSE TEAM 35

APPENDIX D SOFTWARE SYSTEM ELEMENT LOCATIONS 37

ELEMENT LOCATIONS 37

APPENDIX E DATABASE BACKUP AND RESTORE PROCEDURES 39

LOADING THE SQL SERVER MANAGEMENT STUDIO APPLICATION 40
PERFORMING A DATABASE BACKUP 40
PERFORMING A DATABASE RESTORE 42
CREATE SQL LOGINS FOR EACH GENWATCH3 SECURITY USER 45
Special Case – Restore from One PC to Another (GenWatch3 and Trio only) *47*

APPENDIX F PC NAME CHANGE PROCEDURES 49

GENWATCH3 HOST INSTRUCTIONS 50
GENWATCH3 DATA WAREHOUSE INSTRUCTIONS 52
IVISTA INSTRUCTIONS 53
Reconfigure iVista *53*
Update Genwatch3 Webserver Connection *53*

Goals

This manual describes the Disaster Recovery Plan for the GenWatch3 solution including information for iVista and Trio.

Who Should Read This Manual?

This manual is written for the intended audience of novice to mid-level Motorola trunked radio system and novice to mid-level PC users. The personnel performing the Recovery must be a trusted and secure user of the system.

How This Manual Is Organized

This manual is organized as follows:

- **Introduction**: Provides information about the objectives, underpinning principles, and generic definitions.
- **Prevention and Preparedness**: Describes recommended policies for prevention of a disaster and preparation for a disaster.
- **Reaction**: Describes the immediate actions and recovery preparation.
- **Recovery**: Describes roles and recovery procedures.
- **Restoration, Rehabilitation, and Re-Evaluation**: Describes post recovery activities such as restoration and re-evaluation.
- **Appendices**: Supporting documentation.

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 function.

Chapter 1 Introduction

This chapter will provide information about the objectives, underpinning principles, and generic definitions for the GenWatch3 disaster recovery plan.

This chapter contains the following sections:

- **Preamble:** Describes the structure of this Disaster Recovery Plan.
- **Objectives:** Describes the goals of this Disaster Recovery Plan.
- **Underpinning Principles:** Describe the principles and purpose for this document.
- **Updating this Plan:** Describes actions for the user of this document.
- **Distribution of this Plan:** Describes possible distribution scenarios for this document regarding trusted and secure personnel.
- **Definitions:** A list of terms and definitions used within this manual.

Preamble

This Disaster Recovery Plan is for GenWatch3, iVista, and Trio.

This plan aims to minimize the downtime incurred during a disaster, by providing guidelines for a rapid and effective response to a disaster. The disaster plan consists of five sections: 'Introduction', 'Prevention and Preparedness', 'Reaction', 'Recovery', and 'Restoration, Rehabilitation, and Re-evaluation'.

The introduction describes how the plan is structured and how it should be used, as well as recommending where copies of the plan should be stored and who should be responsible for updating sections of the document.

The second section, 'Prevention and Preparedness', outlines steps to minimize the risk of a disaster and measures that can be taken to ensure the organization is prepared and equipped to deal with a disaster, should one occur.

'Reaction' covers the most important actions that should be taken when an emergency is first discovered. It outlines the process for assessing the situation and determining what immediate action should be taken to stabilize the emergency and protect the data. Actions will depend upon the type of disaster and scale of the emergency.

'Recovery' details procedures for salvaging damaged data once the emergency has been stabilized. Recovery includes the initial cleanup of the PCs and the stabilization network.

'Restoration, Rehabilitation, and Re-evaluation' outlines the long-term restoration procedures for data that can be carried out once all databases and PCs have been stabilized in the Recovery phase. Before data can be restored, the PCs should be properly restored (rehabilitated), involving in some instance a complete restore, reinstalling where necessary.

The plan is designed to complement procedures laid down elsewhere concerning best practices for IT staff, regular maintenance of databases and networks and backup procedures in case of emergency. Nothing in this plan is to be taken as contrary to guidelines and procedures laid down elsewhere concerning these matters. The plan assumes that:

- All operating systems are updated regularly.
- Backups are created and stored offsite.
- Disaster prevention hardware is in place. For example, UPSs are connected and maintained.
- IT staff with basic IT knowledge are trained and up to date on basic network recovery procedures.
- Antivirus software is used as per customer policy.

The emphasis of the Plan is therefore on Reaction, Recovery and Restoration, with Prevention and Preparedness measures only covering those actions that are specific to the protection of data, which are not accounted for in other arrangements.

Objectives

The objectives of the disaster plan are to:

- Minimize data loss
- Recover and repair any damaged data
- Return to normal operation as soon as possible

These objectives are facilitated by the Plan through provision of a framework and guidelines for the following:

- Rapid and effective response to an emergency
- Good communication
- Ensuring IT staff are well trained
- Ensuring appropriate equipment and software are available
- Enabling assistance from outside organizations

Underpinning Principles

The minimization of data loss is most important. This is most helped by reconnecting to data sources quickly. Getting the data pathways back to the Genesis software should be priority, such as reestablishing and stabilizing the network.

Updating this Plan

It is recommended that the following parts of this plan be updated (where necessary) bi-annually or upon major update of the Genesis software:

- Appendices B-D

This should be the responsibility of the customer's disaster readiness personnel.

Distribution of this Plan

Copies of this Disaster Recovery Plan should be distributed to multiple tiers within the customer's company hierarchy. For example, this should not only be distributed to IT personnel, but to upper management as well. At least one copy should be stored offsite. Refer to Appendix B for the distribution list.

Definitions

GenWatch3 – Core GenWatch3 software distributed by The Genesis Group
IT – Information Technology. A customer's technical staff.
iVista – The GenWatch3 web interface software.

NIC – Network Interface Card. Allows connectivity to a customer network.
Trio – A module of GenWatch3 that is the core customer billing and management functionality.
UPS – Universal Power Supply.

Chapter 2 Prevention and Preparedness

This chapter outlines steps to minimize the risk of a disaster and measures that can be taken to ensure the organization is prepared and equipped to deal with a disaster, should one occur.

This chapter contains the following sections:

- **Prevention:** Describes steps for preventing possible disasters.
- **Preparedness:** Describes steps for preparing for a disaster.

Prevention

Prevention involves identification of possible threats and taking steps to minimize the chances of any such threats eventuating. Many prevention measures have become standard practice in IT best practice guidelines, basic IT prevention practices will not be duplicated here. However, prevention also involves ongoing awareness among staff about any signs of deterioration in standards of prevention measures in place, and a consciousness about any extra steps that could be taken to further reduce risks. This involves an awareness of the potential threats to the data. For this reason, the most likely threats to the data at the current time are outlined below for IT staff to consider. IT staff should raise any concerns or suggestions about risk minimization and disaster prevention measures with the proper channels of the customer's organization.

Possible Threats

This plan considers only threats to the data that result from a disaster. The plan does not consider action to be taken in the case of catastrophic events from terrorism, acts of war, etc.

The main threats to the data can be divided into 4 main categories: loss of network, database loss, software/PC loss, and PC name change.

Network Loss

This can occur when the host machine can no longer communicate to the data source, such as GenGET or the host machine can no longer communicate to the database server. This can occur for GenWatch3, Trio, and iVista.

Risks of network loss are ever present due the evolving nature of technology. Bad NIC cards or failing routers are likely causes. A change in network configuration is another possible scenario.

Database Loss

This can occur when database files become corrupted or hardware failure prevents recovery of database files.

Risks of database loss can come from external or internal sources. Power loss while performing database operations could result in corruption. Hard disk failure could result in database loss.

Software/PC Loss

This can occur when parts of a PC become nonfunctional. Depending on the hardware malfunction the recovery could be simple and swift or could require a whole new PC altogether. Software or operating system loss is at risk of computer viruses or corruption due to power loss.

PC Name Change

This can occur when a PC hosting Genesis software has its name changed. Depending on the hardware and software configuration, the recovery could be simple and swift or could require more significant configuration changes.

Prevention Summary

The greatest threats to the data are from network loss and software/PC loss. Database loss and PC name changes are less likely. However, a worst-case scenario could involve all threats occurring simultaneously. IT staff should be mindful of any signs of problems arising in these areas. The actions described in this Plan can be broadly applied to a range of different circumstances involving any or all these three primary threats.

Preparedness

Preparedness involves:

- Identification of a disaster response team.
- Training of a disaster response team.
- Identification of recovery work areas.
- Ensuring availability of equipment and software.

Identification of the Disaster Response Team

(See Appendix C for contact details and chapter 4 for specific duties of the disaster response team)

The **Data Recovery Personnel** should be familiar with Microsoft SQL data restoration procedures.

The **Data Backup Personnel** should be performing and monitoring the regular scheduled backups and know where to retrieve the backup when needed.

The **IT Staff Main Contact(s)** are the trusted and secure contacts that should have access to the accounts and passwords necessary for database, network, and PC recovery.

The **Hardware Recovery Personnel** are familiar with diagnosing and resolving hardware issues.

The **Network Recovery Personnel** are familiar with diagnosing and resolving network related issues.

Training of a Disaster Response Team

Proper industry expected training for personnel is expected and assumed. Best practices should be followed with consideration for security.

Identification of Recovery Work Areas

(Refer to Appendix D for element location details)

The basic principle here is to know where parts of the system are located. For example, if the host and database are separate PCs, then where is each PC located?

GenWatch3 Host – This is the core GenWatch3 service machine.
iVista Server – This server hosts the iVista website.
GenWatch3 Client – This is any client PC that has the GenWatch3 client software installed.
GenWatch3 GW Database – This is the main GenWatch3 database.
iVista Genesis Database – This is the main iVista database.
GenGET Database – This is the main database used for GenGET and iVista reporting
Trio Database – This is the primary billing database.

In addition, it is necessary to know the location of the offsite backup storage locations. This should be detailed in Appendix B.

Ensuring availability of equipment and software

Industry standard diagnostics and recovery tools should be available to IT Staff and will not be enumerated here. Examples include backup hubs, routers, switches, cabling, command line diagnostic software, WireShark, etc.

In addition, the following are needed:

- Genesis Product installation CDs/files.
- Microsoft SQL Server installation media.
- Operating system recovery media.
- In the case of PC loss, alternate PCs or virtual PCs as necessary.
- Account and Password information (for Trusted and Secure personnel only).
- Database backups where necessary.

Chapter 3 Reaction

This chapter covers the most important actions that should be taken when an emergency is first discovered. It outlines the process for assessing the situation and determining what immediate action should be taken to stabilize the emergency and protect the data. Actions will depend upon the type of disaster and scale of the emergency.

This chapter contains the following sections:

- **Immediate Response:** Describes the very first actions in a disaster.
- **Planning the Recovery:** Describes the assessment and strategy for dealing with a disaster.

Immediate Response

This is the first action to be taken after determining that a disaster has occurred. In all regards, do not panic. By performing regular database backups and maintaining this plan accordingly, the recovery process should be quick and painless. At any time contact your software support personnel for guidance through this process.

Identify the Emergency

An emergency event is any sudden loss of Genesis software functionality.

Assess the Situation

Determine the location of the incident. Examples include:

- Is the incident isolated to a GenWatch3 client or are all GenWatch3 clients experiencing the issue?
- Are remote iVista clients unable to access the iVista web server?
- Did you receive a database down notification from GenWatch3?
- Are any PCs malfunctioning?
- Does data appear to be corrupt?
- Is there a disconnect from the data source?

Report the Emergency Incident (using the contact information in Appendix B)

Depending on the scale and scope of the emergency, notify the relevant personnel:

- Network loss, loss of connection from the data source – contact the Network Recovery Personnel.
- Database down or data corruption – contact the Database Recovery and Database Backup Personnel.
- Hardware Malfunction – contact the Hardware Recovery Personnel.
- In all cases the IT staff main contact(s) should be contacted.

In addition, depending on scale or absence of personnel then upper Administration may need to be notified.

Immediate Actions

- Verify that databases are working properly by running a simple query on the suspect database within Microsoft SQL Management Studio on the Database server. (See Appendix D for Element Locations).
- Verify that the suspect service is running.
- Test network connectivity using IT best practices and procedures not defined here.
- Review Microsoft Windows Application and Security logs.

Role of Data Recovery Personnel

Upon receiving report of an incident, the Data Recovery Personnel should assess the situation by asking the following questions of the person reporting:

- Are you still receiving live streaming data? (Applicable for GenWatch3 only)
- Did you receive a database down notification? (Applicable for GenWatch3 and Trio only)
- Have all the appropriate Disaster Recovery Team been notified?
- Are you experiencing corrupted data? What is the indication of this?
- What PCs are affected?
- Have any actions already been taken?

Immediate Stabilization

These actions may include the following:

- Verify that all appropriate cables are connected and secure.
- Reboot the suspect machine.

Planning the Recovery

After the initial assessment, or after the emergency has been stabilized, the Data Recovery Personnel, should contact the IT Main Staff contact(s) and appropriate administration. In consultation with these members of the Disaster Response Team, the Date Recovery Personnel should devise a plan for the Recovery operation. The plan should consider:

- What is the nature and total extent of the malfunction of the software system?
- Recovery Teams - Can the issue be resolved by the in-house Recovery Team(s), or will outside help be required?
    - How many in-house people will be required?
    - Who will oversee contacting Team members?
    - Who will contact external organizations to request assistance?
- What resources are required?
    - What is available in-house?
    - What can be borrowed?
    - What will have to be bought?
- What are the PC hardware and data recovery priorities?
- What is the accessibility of Trusted and Secure Personnel for account recovery?
- What public relations concerns are there?
- What documentation of the incident is needed?

Chapter 4 Recovery

This chapter details procedures for recovering databases once the emergency has been stabilized. Recovery includes the initial cleanup of the PCs and the stabilization of the network.

This chapter contains the following sections:

- **Important Principles for All Recovery Personnel:** Describes the basic understandings and principles for the recovery process.
- **Roles:** Describes possible roles for recovery personnel and their respective duties.
- **Recovery Scenarios:** Describes lists of recovery procedures for given disasters.

Important Principles for All Recovery Personnel

- Think before acting! Taking time to consider best practices, principles and recovery priorities is vital to effectively minimizing the loss of data.
- Staff should be properly rested and mentally prepared.
- Keep records of all expenses.

Roles

Data Recovery Personnel

- Perform the database restore (refer to Appendix E for a description of database restoration).
- Assess data integrity.
- Diagnose database down scenarios.
- Request the database backup from the Data Backup Personnel when needed.

Data Backup Personnel

- Perform regular database backups (refer to Appendix E for a description of database backup).
- Store backups offsite (recommended).

IT Staff Main Contact(s)

- Coordinator of the recovery process.
- Maintain a list of procedures taken and times for each.
- Keep a log of procedure failures for Lessons Learned.
- Ability to do rudimentary diagnosis of the Genesis software.
- Contact appropriate software support when necessary.
    - Maintain software support contact information.
- Schedule operating system updates for critical patches.
- Other IT best practices and procedures.
- Contact other administration for purposes of escalation.
- Knowledge of the hardware and software topology of the system.
- Securely maintain account information necessary for all elements of the system.
- Perform the backup of the iVista configuration file located in the following folder wherever iVista is installed:
    - **Configuration\web.config**
- Perform the backup of the GenWatch3 configuration files located at:
    - Backup this folder **c:\ProgramData\Genesis**
    - Backup this folder **c:\Users\$USER$\Documents\Genesis** **Note: $USER$ is the user logged into the Host Machine

Hardware Recovery Personnel

- Have knowledge of PC hardware.
- Diagnose PC hardware issues.
- Can acquire new hardware.
- Can contact hardware support when needed.
- Regularly review Microsoft Windows Application and Security logs for proactive prevention.

Network Recovery Personnel

- Maintain the network (this is beyond the scope of this document and will not be detailed here).
- Have knowledge of data pathways and the ability to diagnose stoppages.

Recovery Scenarios

GenWatch3

NOTE: If you plan to reinstall GenWatch3 as a part of your recovery, you must complete the steps in the Database Loss section below before reinstalling GenWatch3. If your installation includes Trio, look for the steps below that include the Trio database.

Database Loss

Restore the database from a backup: Follow the steps in the Performing a Database Restore section of Appendix E.

PC Name Change

See Appendix F PC Name Change Procedures for steps and considerations to undertake when the GenWatch3 Host PC has its name changed.

Hardware/Software Loss

1. Contact the software vender for support in this operation if a complete restore is necessary.
2. Reinstall the GenWatch3 software per the GenWatch3 Quickstart Guide.
3. Stop the GenWatchService from the services application in Windows. (You may need to temporarily disable the auto restart option).
4. Restore the config files (if these were previously backed up) (minus the database files, do not copy over these).
    a. Restore this folder **c:\ProgramData\Genesis**
    b. Restore this folder **c:\Users\$USER$\Documents\Genesis**
    NOTE: $USER$ is the Windows user logged into the Host Machine
5. Restart the GenWatchService.
6. Start GenWatch3 LaunchPad and relicense.

Network Loss

This is the responsibility of the Network Recovery Personnel and goes beyond the scope of this document.

iVista

Database Loss

See Appendix E for instructions on backing up and restoring databases.

PC Name Change

See Appendix F PC Name Change Procedures for steps and considerations to undertake when the iVista PC has its name changed.

Hardware/Software Loss

- Reinstall the iVista software
- Reconfigure iVista with the configuration utility and the same XML files as the original configuration.
- Remove the fresh Genesis database and restore the backup Genesis database by performing the database recovery steps in Appendix E.
- Restore the iVista configuration file (web.config) to the following path:
    - **Configuration\web.config**

Network Loss

This is the responsibility of the Network Recovery Personnel and goes beyond the scope of this document.

Trio

Database Loss

Follow the instructions for GenWatch3 Database loss to restore the Trio database.

Hardware/Software Loss

Follow the instructions for GenWatch3 Hardware/Software loss to restore the Trio software.

Network Loss

This is the responsibility of the Network Recovery Personnel and goes beyond the scope of this document.

Chapter 5 Restoration, Rehabilitation, and Re-Evaluation

This chapter outlines the long-term restoration procedures for data that can be carried out once all databases and PCs have been stabilized in the Recovery phase. Before data can be restored, the PCs should be properly restored (rehabilitated), involving in some instances a complete restore, reinstalling where necessary.

This chapter contains the following sections:

- **Rehabilitation:** Describes steps necessary for recovery personnel after recovery.
- **Restoration:** Describes steps for recovering to the same capacity before recovery.
- **Restoration Procedures:** Describes a list of restoration scenarios and their procedures.
- **Post-Emergency Re-Evaluation:** Describes actions to be taken after the emergency has ended.

Rehabilitation

Role of Hardware Recovery Personnel

- Ensure that affected PCs are performing as expected
- Review Microsoft Application and System logs for problem indications.
- Replace any reserve equipment.

Role of the Network Recovery Personnel

- Details of network recovery are beyond the scope of this document. Network recovery personnel should use secure industry standard best practices.
- After network recovery, verify that live streaming data in present.
    - For GenWatch3 open the Activity window.
    - For Trio run a report and verify that new data exists.
    - For iVista open a remote client to test connectivity.

Restoration

Role of the Database Backup Personnel

- After the restoration of the database, it will be necessary to test the integrity of the restored data. Run reports as necessary.
- Verify that new data is being stored in the database.
- If backup media was retrieved from offsite, then that media may need to be replaced.

Restoration Procedures

Data restoration procedures:

GenWatch3

- Ensure all live streaming data source connection properties are up to date since the last backup that was restored. This information is found in the appropriate input module documentation. Opening the Activity window and verifying the presence of streaming data is the easiest way to test this.
- Ensure all security logins are present and configured in the Security module. GenWatch3 Client users may not be able to login until this is corrected.

iVista

- Ensure that the saved web.config file is placed in the iVistaInstaller\Configuration folder where iVista is installed.

Trio

- Ensure that the GenWatch3 Restoration Procedures have been completed.

Post-Emergency and Re-Evaluation

A detailed post-emergency assessment should be carried out to determine the extent of loss and to determine successes and failings. All members of the team should have input to the post-disaster assessment process. A written report should be produced including details on the following:

- Cause of the disaster
- Scope and scale of data loss
- Effects of lost data
- Staff time expended during the operation
- Cost of recovery (new PCs, etc.)
- Cost of recovery equipment and supplies
- Notable successes and/or failings at each stage of the recovery process

The report should make recommendations for any improvement of data management procedures deemed necessary and propose changes to the Disaster Plan where necessary. The report should have a summary of lessons learned.

The PCs/data affected should be monitored for at least one year after the event to make sure no further issues arise.

Any exhausted resources should be replaced.

Appendix A References

List the supporting documentation.

This appendix contains the following sections:

- References: A list of documents used to create this document.

References

The following articles have been consulted during the preparation of this manual:

DISACT (2004) 'Preparedness and Recovery' notes on disaster plans (http://www.cpbr.gov.au/disact/index.html)

Appendix B Plan Distribution List

Detail a list of Disaster Recovery Plan document copy distribution.

This appendix contains the following sections:

- Distribution List: A list of persons/places to hold a copy of this Plan.

Distribution List

IT Personnel:

Administration Personnel:

Offsite Location:

Appendix C Disaster Response Team

Identify the disaster response team personnel.

This appendix contains the following sections:

- Disaster Response Team: A list of persons involved in disaster recovery.

Disaster Response Team

Data Recovery Personnel: _____

_____

_____

_____

Data Backup Personnel: _____

_____

_____

_____

IT Staff Main Contact(s): _____

_____

_____

_____

Hardware Recovery Personnel: _____

_____

_____

_____

Network Recovery Personnel: _____

_____

_____

_____

Appendix D Software System Element Locations

Identify the locations for all parts of the Genesis software system that will be necessary for recovery in the event of a disaster.

This appendix contains the following sections:

- Element Locations: A list of software system elements and their respective physical locations.

Element Locations

GenWatch3 Host:

iVista Server:

GenWatch3 Client(s):

GenWatch3 GW Database:

iVista Genesis Database:

GenGET Database:

Trio Database:

Appendix E Database Backup and Restore Procedures

This appendix details the procedures for successfully backing up and restoring a database.

This appendix contains the following sections:

- **Loading the SQL Server Management Studio Application:** Detailed procedure for loading the necessary tools for backing up and restoring a database.
- **Performing a Database Backup:** Detailed procedure for backing up a database.
- **Performing a Database Restore:** Detailed procedure for restoring a database that was previously backed up.
- **Create SQL Logins for Each GenWatch3 Security User:** Steps to create an SQL login for each GenWatch3 security user in the restored GenWatch3 database.

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**. 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.

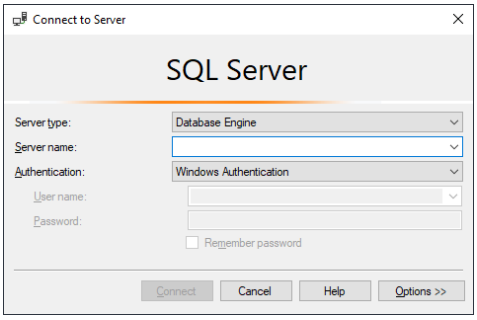


Figure E.1 – Connect to Server dialog

The Windows user must have SQL sysadmin privileges in order carry out the backup and restore procedures.

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 not on the GenWatch3 database machine, as they are a complete database backup.

To back up your GenWatch3, Trio, or iVista 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 window, expand the **Databases** item: This will show all the databases under this SQL Server instance, including the GenWatch3 databases. This includes the ***GW*** database for GenWatch3 installations. For iVista installations, this will display ***Genesis***. For Trio installations this will also display ***Trio***.
3. Right-click on the database you wish to backup: This will show the database options menu.
4. Click the **Tasks** option: This will show the Tasks options menu.

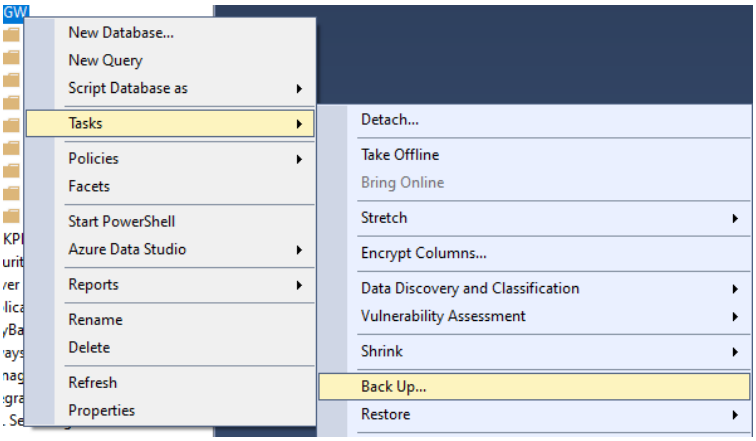


Figure E.2 – Tasks options

5. Click the **Backup…** option: This will show the *Back Up Database* window.

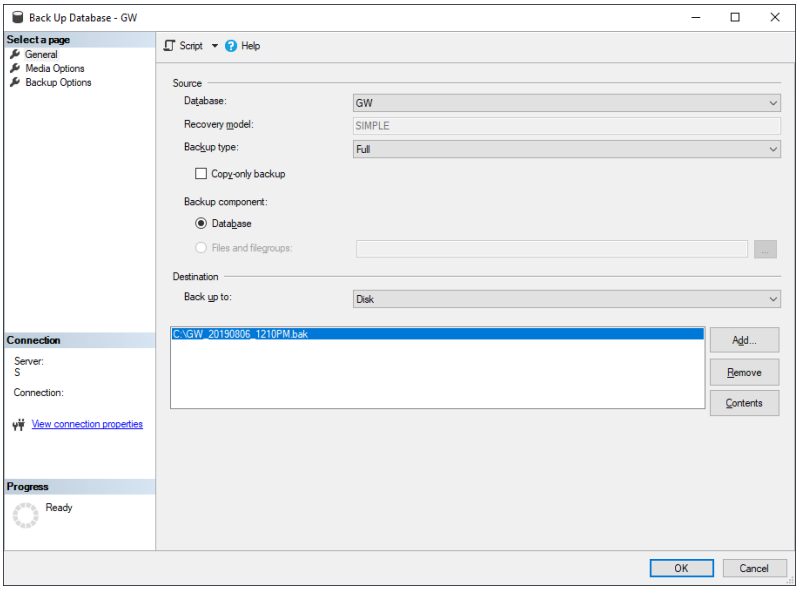


Figure E.3 – Back Up Database dialog

6. In the **Destination** section, click the **Remove** button: This will remove the default destination entry.
7. In the **Destination** section, click the **Add…** button: This will show the *Select Backup Destination* window.
8. 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 with the date. For example, *GW-yyyy-mm.BAK* where *yyyy* is the 4-digit year and *mm* is the 2-digit month. For example, a backup performed on 12-31-2019 would have a destination named *GW-2019-12.BAK.*

9. Click **OK** to confirm the file name: This will close the *Select Backup Destination* window and return you to the *Back Up Database* window.
10. In the *Select a page* section, click on **Backup Options**.
11. Under the **Backup set** section, change the **Name** to include the date. For instance, *GW-yyyy-mm* where *yyyy* is the 4-digit year and *mm* is the 2-digit month: For example, a backup performed on 12-31-2019 would be named *GW-2019-12*.
12. Click the **OK** button: This will perform the backup process. (Notice the progress of this operation in the Progress section.)
13. Once this process is complete, you are ready to move your 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 a previous backup available for use. This process restores a database backup file to the machine's SQL Server instance.

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

To restore a database, 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 window, right-click in the *Databases* item: This will show the Databases options menu.

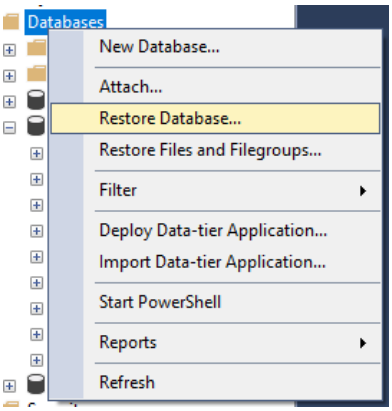


Figure E.4 - Object Explorer

Click the **Restore Database…** option: This will show the *Restore Database* window.

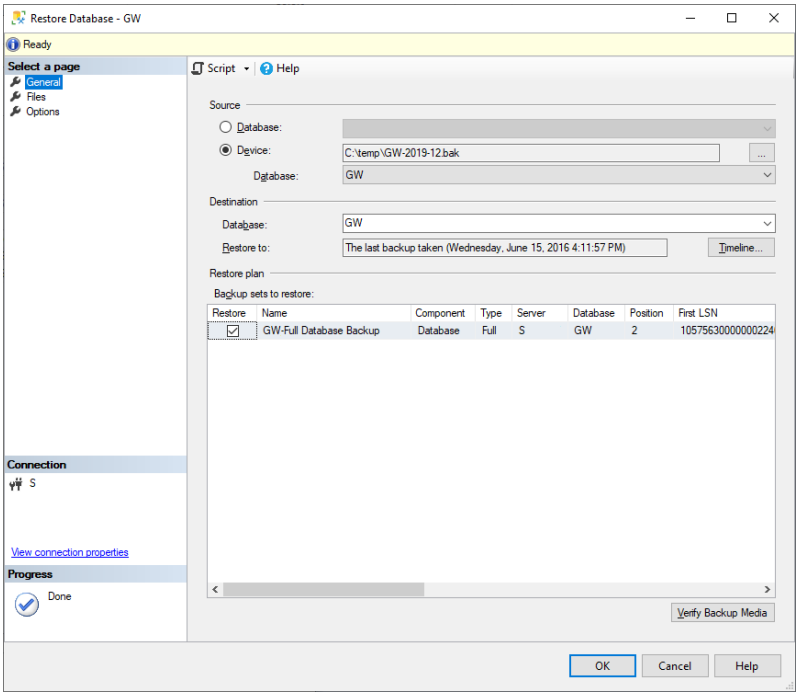


Figure E.5 – Restore Database dialog – General page

3. In the *Source* section, select the *Device* option.
4. Click the … button at the end of the *Device* option: This will load the *Specify Backup* window.
5. In the *Select backup devices* window, for the *Backup media* option, choose ***File***.
6. Click the **Add** button: This will show the *Locate Backup File* window.
7. Click on your backup file (created via the Database Backup process) and press the **OK** button: This will return you to the *Select backup devices* window.

8. Click **OK** in the *Select backup devices* window: This will return you to the *Restore Database* window and populate the *Backup sets to restore* list with one entry.
9. Under the *Destination* section, type ***[DatabaseName]***. For GenWatch3 it will be ***GW***. For iVista it will be ***Genesis***. For Trio it will be ***Trio***.
10. Verify that the checkbox in the *Restore* column of the *Backup sets to restore* list is checked.
11. In the *Select a page* section, click on the **Files** item.

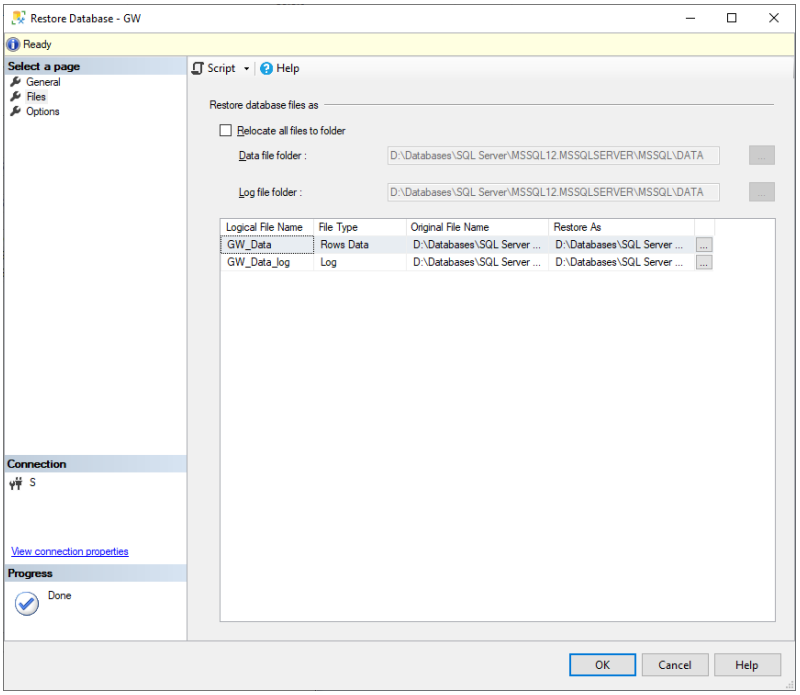
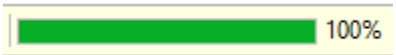


Figure E.6 – Restore Database dialog – Files page

12. In the *Restore database files as* section, click on the *Restore As* column for the *[DatabaseName]_Data* entry: This will allow you to modify the file name.
13. Change the Restore As file name to **[DatabaseName].MDF**.
14. Click on the **Restore As** column for the *[DatabaseName]_Log* entry. This will allow you to modify the file name.
15. Change the *Restore As* file name to ***[DatabaseName].LDF***.

    Ensure that the files [DatabaseName].MDF and [DatabaseName].LDF files do not already exist in the Restore As folder.

16. Click the **OK** button: This will perform the restore process. (Notice the progress of this operation in the status bar the top of the window.)



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

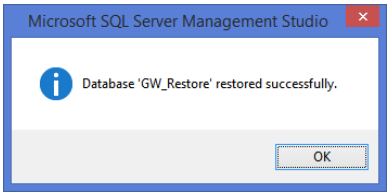


Figure E.7 – Restore Complete dialog

Create SQL Logins for Each GenWatch3 Security User

Steps in this section step will create an SQL Server login for each GenWatch3 Security user. These logins must exist for the GenWatch3 user to have access to the information in the database:

1. Open SQL Server Management Studio
2. Log in as a user that has administrator privileges on the SQL instance.
3. Get a list of GenWatch3 Security users: In SQL Server Management Studio run the following query:

   ```
   Select [Name] from SEC_Users.
   ```

   This will return the list of logins that need to be created.
4. Create an SQL Server Login for each Name in the GenWatch3 Users list:
   a. Right-click on the Security->Logins folder and choose **New Login…**

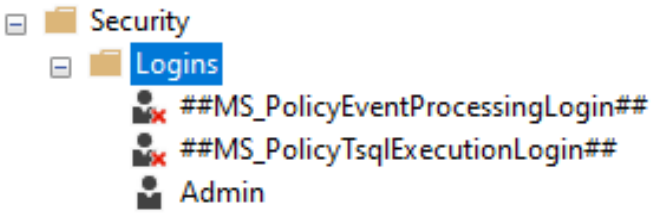


Figure E.8 – SQL Logins folder

b. On the General tab, in the Login Name box, enter the next name from the GenWatch3 Security Users list.

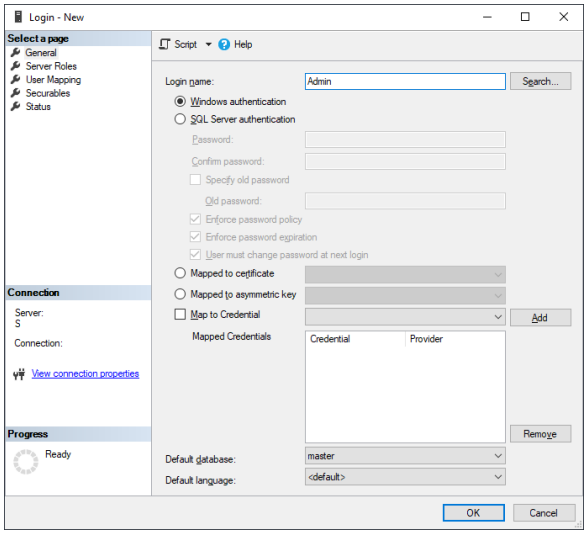


Figure E.9 – Login - New General Tab

c. On the User Mapping tab:
   i. Select the GW database
   ii. Select the db_gw3user database role member.
   iii. Repeat the two steps above on the Trio database if Trio was restored.
   iv. Click **OK**.

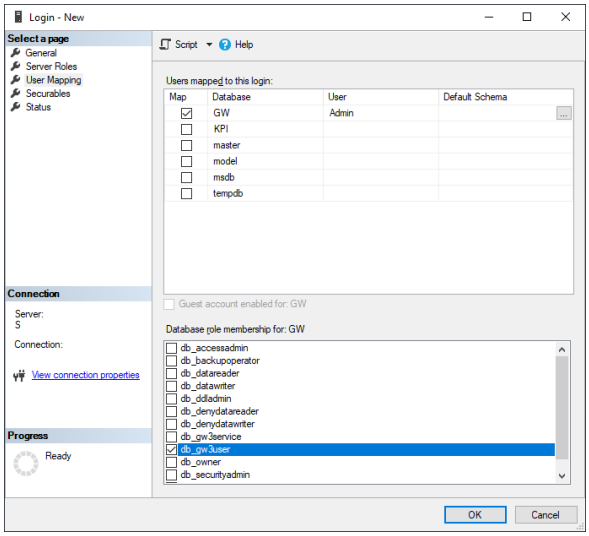


Figure E.10 – Login – New User Mapping Tab

Special Case – Restore from One PC to Another (GenWatch3 and Trio only)

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.

Appendix F PC Name Change Procedures

This appendix details the procedures for successfully recovering from a GenWatch3 or iVista PC having its name changed.

This appendix contains the following sections:

- **GenWatch3 Host Instructions:** Detailed procedure for updating GenWatch3 to be aware of the new computer name.
- **GenWatch3 Data Warehouse Instructions:** Detailed procedure for updating a data warehouse database.
- **iVista Instructions:** Detailed procedure for updating iVista to be aware of the new computer name.

GenWatch3 Host Instructions

If possible, carry out the following before the computer's name has been changed. Do not start the GenWatch3 service until after the name has been changed and the computer restarted as necessary. It may even be best to set the service to manual start until all changes have been made.

1. Stop the GenWatch3 service
2. Update GW database with new name:
    a. MachineName column in [LP_Tools] table
    b. ComputerName column in [Modules] table
    c. FieldValue column in [ModuleSettings] table where the FieldName is *ModuleComputerName*.
    d. FieldValue column as appropriate in [ModuleSettings] table where the FieldName has *Name* in it
        i. Run this query (replacing <old_name> with the old computer name:
        ii.
```
SELECT
  *
FROM
  dbo.ModuleSettings
WHERE
  FieldValue LIKE '%<old_name>%' OR
  FieldName LIKE '%Name%'
```
        iii. Review the results and update any rows referencing the old computer name.
3. Update KPI database with new name:
    a. Name column in [DataSources] table
4. Service GenWatch3.config file (ProgramData\Genesis\GenWatch3)
    a. Several settings may refer to the Host computer name (not a comprehensive list):
        i. GW3HostMachine
        ii. ServerName
        iii. TrioDBServerName
        iv. GW3HostMachineList
        v. GW3ServerName
5. Client/GUI GenWatch3.config file (<User>\Documents\Genesis\GenWatch3)
    a. This is not required to change, but users will need to change the Host manually the next time they log in.
    b. If desired though, any occurrences of the old name in settings can be changed.

After the computer's name has been changed, carry out the following:

1. SQL Server
    a. Carry out only if SQL is installed on the computer whose name is being changed.

b. While SQL Server detects and handles computer name changes inherently, there may be additional manual changes necessary.
c. The sys.servers system table may need to be updated to reflect the new computer/instance name:
    i. If all is well the below query returns the same value for all fields (where you are connected to the default server instance)

```
SELECT SERVERPROPERTY('Machinename') [machinename]
       , SERVERPROPERTY('ServerName') [ServerName]
       , @@SERVERNAME [@@Servername]
```

    ii. If the *@@ServerName* is the only different one, it needs to be fixed:

```
EXEC sp_dropserver 'value from the @@Servername';
GO

EXEC sp_addserver 'value from either Machinename or
ServerName', 'local';
GO
```

    iii. Restart SQL Server
d. Local Windows Users
    i. Local Windows users which exist in SQL Server as a login may need to be dropped and re-added.
    ii. They will show as <old_name>\gwadmin or equivalent
    iii. It may not present any issues until the next upgrade when GW may not correctly correlate the same user (but with a new fully qualified name like <new_name>\gwadmin) with an existing SQL login still named as <old_name>\gwadmin.

2. REST API Port
    a. Contact the software vendor to recreate and rebind the SSL certificate to the REST API port.
    b. This is required as the certificate created when installing GenWatch3 specifies the computer name as a Subject Name / Subject Alternate Name in the certificate.
    c. Without regenerating and binding the certificate, connections to the REST API port will likely result in an invalid certificate error.

Once the changes have been made, start the GenWatch3 service.

GenWatch3 Data Warehouse Instructions

Follow the GenWatch3 Host instructions, making any necessary changes on the GenWatch3 host where the old Data Warehouse name is found. Additionally:

1. On the GenWatch3 host database, update the Server column in the [PullServers] table.
2. Using the GenWatch3 Host instructions as a guide, make any corresponding changes on the Data Warehouse database or computer where the old Data Warehouse computer name is referenced.

iVista Instructions

Reconfigure iVista

Locate and launch the iVista Configuration (iVistaConfiguration.exe) in the Genesis install folder path (i.e C:\Program Files\Genesis\iVista). Apply the following steps:

- Click “Configure iVista” and go through the configuration process just like you would on an install/upgrade to correctly set the database and app configurations.
- Click “Create SSL Self Signed Certificates”
- Click Deploy Tileserver to set up the Genesis tile server for Open Map usage.

Update Genwatch3 Webserver Connection

Log into iVista and navigate to the Configuration page (Management → Configuration). Select the General tab if it is not already selected.
If the machine name is what is used in the GenWatch3 Server property (https://[[Machine Name]:13001) then update it to the new machine name. Click on the Test Connection button to verify and then click the Update button to save your changes.
If the IP Address is what is used in the GenWatch3 Server property then simply verify by clicking on the Test Connection button.