GenWatch3®
GW_SAM
Software Version 2.23.5
Module Book

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

Trademarks

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

The Genesis Group Trademark Information

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

Copyright

Copyright © 2006-2023; Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks. All rights are reserved. No part of this publication or the associated program may be reproduced, transmitted, transcribed, in whole or in part, in any form or by any means, whether it is mechanical, magnetic, optical, electronic, manual or otherwise, without the prior written consent of Burks GenCore Co., Inc. D.B.A:
The Genesis Group and Phil Burks
5800 Eagles Nest Blvd
Tyler, Texas 75703.

Includes technology licensed from Motorola.

Disclaimer

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

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

License

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

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

Support

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

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

Document History

Revision	Description	Author
2.0.2	Initial Release	
2.0.3	Updated Screenshots	CBH
2.0.3	Revision before Release	CBH
2.0.4	Added Exempt Control Detail	KIH
2.0.5	Revision before Release	TDW
2.0.6	Updated screenshots	REB
2.0.6	Updated screenshots	CLB
2.0.6	Added note to Radio Search section	WRK
2.0.6.6	Revision before Release	TDW
2.2	Update settings screenshot	WRK
2.2	Document Reviewed	WRK
2.3	Revisions Before Release	CWF
2.4	Revisions Before Release	CWF
2.5	Revisions Before Release	CWF
2.5	Corrected Schedule Deletion	KIH
2.6	Revisions Before Release	CWF
2.7	Revisions Before Release	JAW
2.8	Revisions Before Release	CWF
2.9	Revisions Before Release	CWF
2.10	Revisions Before Release	CWF
2.11	Conversion to docx	BCY
2.12	Revisions Before Release	JAW
2.13	Revisions Before Release	ATG
2.14	Revisions Before Release	JAW
2.15	Revisions Before Release	REB
2.16	Revisions Before Release	JPS
2.17	Added CSV exports of SAM lists Updated description of overlapping calls	DW
2.17.16	Added Purging to Settings window.	REB
2.23.4	Added Reject Watch to Settings window.	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 OVERVIEW ... 9

WHAT IS GW_SAM? ... 9
WHAT IS A SUSPECT? ... 10

CHAPTER 2 SETTING UP GW_SAM ... 11

RESOURCES AND ID RANGES TREE ... 11
Managing Schedules ... *12*
Managing Schedules ... 12
Adding a Schedule ... 13
Editing a Schedule ... 13
Deleting a Schedule ... 13
Copying a Schedule ... 14
Managing Resource ID Ranges ... *14*
Resource ID Range Rules ... 14
Adding Talkgroup ID Ranges ... 15
Adding Radio ID Ranges ... 16
Radio Search ... 18
Editing an ID Range ... 19
Deleting an ID Range ... 20

CHAPTER 3 USING GW_SAM ... 21

USING THE SUSPECT LIST ... 21
Suspect List Options ... *22*
New ... 22
Delete ... 23
Exempt ... 23
Add to Suspect Hotlist ... 23
History ... 24
Export ... 25
Print ... 25
USING THE SUSPECT HOTLIST ... 26
Suspect Hotlist Options ... *27*
Remove ... 27
History ... 27
Export ... 27
Print ... 27
USING THE SUSPECT EXEMPTION LIST ... 28
Suspect Exemption List Options ... *29*
Delete ... 29

Restore 29
History 29
Export 29
Print 30
CHANGING GW_SAM SETTINGS 30
Overlap *30*
Impossible Driving Distance (IDD) Threshold *31*
Assumed Driving Speed 32
Ignored IDD Suspect Threshold 32
Ignore Site Change Threshold 32
Average Broadcast Radius 32
The IDD Formula 32
IDD Formula Conclusion 33
View Site Map 34
Affiliation Watch *35*
Talkgroup Watch *36*
Reject Watch *38*
Recommended 38
Other Rejects 38
Clear 38
Notifications *39*
Purging *40*
SUSPECT NOTIFICATIONS 41

About this Manual

Goals

This manual describes the role and function of the GW_SAM module in the GenWatch3 solution.

Who Should Read This Manual?

This manual is written for the intended audience of novice to mid-level trunked radio system users and novice to mid-level PC users.

How This Manual Is Organized

This manual is organized as follows:

- **Overview:** Describes the GW_SAM module and provides a brief overview of its function.
- **Setting up GW_SAM:** Describes how to set up GW_SAM resource ID ranges and schedules.
- **Using GW_SAM:** This chapter describes how to use GW_SAM to monitor suspect activities.

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.

Chapter 1 Overview

This chapter describes the GW_SAM module and provides a brief overview of its function.

This chapter contains the following sections:

- **What is GW_SAM?:** Defines the GW_SAM module and GUI (Graphical User Interface).
- **What is a Suspect?:** Describes how GW_SAM identifies suspects.

What is GW_SAM?

The GW_SAM module monitors resources (groups and radios) for suspicious activity. Suspect resources are added to a list where the suspect's activities are then displayed and recorded in detail.

When an activity (push-to-talk, affiliation, etc.) is received on a group or radio ID (also known as resources), this activity is validated against the resource ranges defined within the GW_SAM GUI. If the activity of the resource violates the expected activity definitions, the resource is added to the *Suspect List*. Once in the *Suspect List*, the resource's activity is closely monitored and detailed in the GW_SAM database.

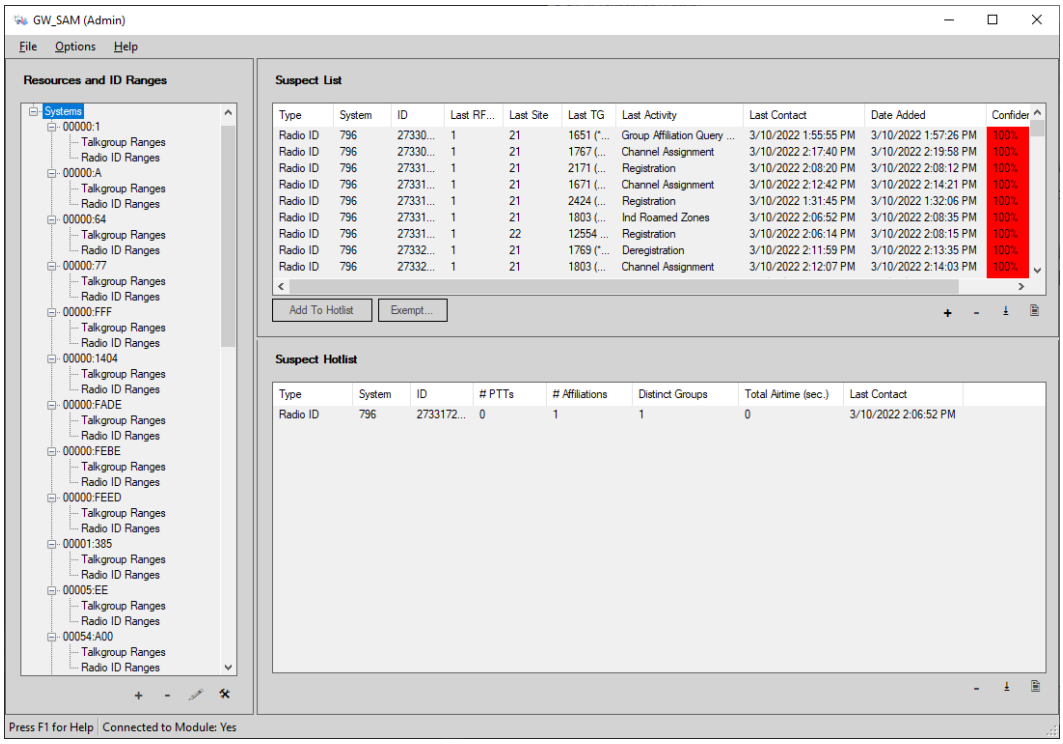


Figure 1.1 – GW_SAM GUI

The Options menu contains the **Exempt Suspects…** button. This will display the *Suspect Exemption List*.

What is a Suspect?

A suspect is a resource (radio ID or group) that breaks a predefined rule of expected behavior. The following rules are enforced within GW_SAM:

- **Usage outside of the predefined schedule of usage:** This rule is applied when you set up a GW_SAM schedule (described in *Chapter 2 – Setting Up GW_SAM*) and assign that schedule to a radio ID. If usage is detected outside of the schedule, GW_SAM adds the radio ID to the *Suspect List* with a confidence level of 100%.
- **Usage of a resource that is in an unassigned or unallocated resource range:** This rule is applied when you assign a validity level of Unassigned or Unallocated to a resource range (described in *Chapter 2 – Setting Up GW_SAM*). If usage is detected on one of these resources, GW_SAM adds the resource to the **Suspect List** with a confidence level of 100%.
- **Usage of a service that is not selected when services are restricted:** This rule is applied to radio ID resource ranges when you select the **Allow Only the Following Services** option (described in *Chapter 2 – Setting Up GW_SAM*). Services are radio features such as dispatch, private, status, message, etc. GW_SAM validates each activity that is detected for radio IDs in this range against the selected services. If a radio ID in the range uses a service outside of the selected services, then GW_SAM adds this radio ID to the *Suspect List* with a confidence level of 100%.
- **Overlapping calls:** This rule is applied to conversations that occur on radio IDs. If a conversation for a radio ID on a given group overlaps with a conversation for the same radio ID on a different group or private call, GW_SAM adds the radio ID to the suspect list. If there is a partial overlap, the confidence level is 75%. If there is a full overlap, the confidence level is 100%. This rule ignores patch, multiselect, and multigroup calls. Private calls will have a group ID of 0.
- **Impossible Driving Distance (IDD) activity:** This rule is applied only to multisite data and requires latitudinal and longitudinal coordinates set up in the GW_Alias module for each site on the system(s) monitored by GenWatch3. Each time the source site for a radio ID changes, this rule looks at the current activity time and the last activity time. If the speed required to travel between the coverage areas of the two sites within that time frame exceeds the defined IDD threshold, GW_SAM adds the radio ID involved in the activity to the *Suspect List*.
- **Rapid Affiliation:** This rule is applied when a radio issues an affiliation activity (usually when a radio is turned on), switches groups or responds to a dispatcher issuing a radio check. Each system has an expected number of affiliations received from a radio for these events. If more than that number of affiliations is received, there may be two radios with the same ID.

Chapter 2 Setting Up GW_SAM

This chapter describes how to set up GW_SAM resource ID ranges and schedules.

This chapter contains the following sections:

- **Resources & ID Ranges Tree**: Describes the *Resources and ID Ranges* tree.
- **Managing Schedules**: Describes how to create and manage schedules.
- **Managing Resource ID Ranges**: Describes how to manage resource ID ranges.

Resources and ID Ranges Tree

The *Resources and ID Ranges* tree contains each schedule and resource ID range that you define within the GW_SAM GUI. The ID ranges are organized by system and even further by resource ID range type (radio ID or talkgroup). Using the *Resources and ID Ranges* tree, you can easily add, edit, delete or view schedules and resource ID ranges.

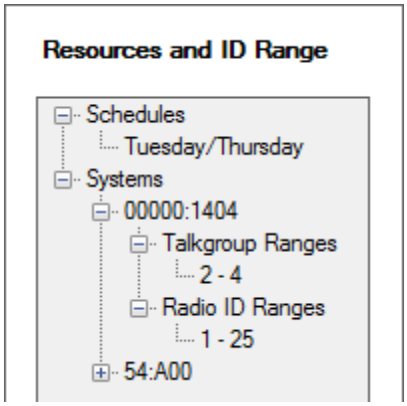


Figure 2.1 – Resources and ID Ranges tree

Resource ID Range: A range of groups or radio IDs, such as radio IDs 1 through 4.

Managing Schedules

GW_SAM schedules are weekly plans of expected (allowed) usage for a radio ID on the system. Once you create a schedule, you can apply it to any radio ID range that you wish to restrict to this schedule. Any radio ID that violates its schedule is reported as a suspect within the *Suspect List*.

Some common examples of schedules are day shift and night shift, where day shift is from 6:00 AM to 6:00 PM and night shift is from 6:00 PM to 6:00 AM.

Managing Schedules

You can add, update, delete and copy schedules using the buttons below the *Resources and ID Ranges* tree or by right-clicking on the root schedules node or a schedule node below the root schedules node. Schedules are displayed and edited within the *Add/Edit Schedule* window (Figure 2.2).

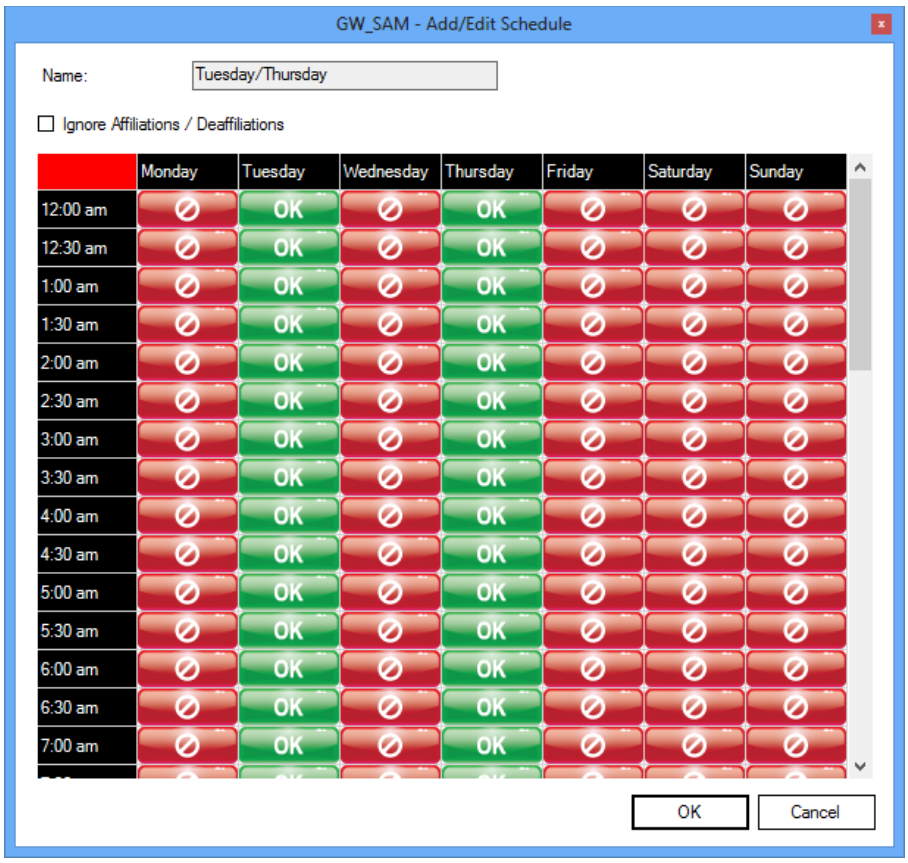


Figure 2.2 – *Add/Edit Schedule* Window

Adding a Schedule

To add a new schedule, take the following steps:

1. Click the root schedules node in the *Resources and ID Ranges* tree. This will enable the **Add** button below the *Resources and ID Ranges* tree if it is not already enabled.

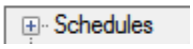
   

   Figure 2.3 – Root Schedules Node

2. Click the **Add** button below the *Resources and ID Ranges* tree or right-click the **Schedules** node and choose **Add a New Schedule…** from the menu. Either of these actions will load the *Add/Edit Schedule* window.
3. Type a name in the **Name** text box to describe the schedule. This name should describe the schedule, such as "Night Shift," "Day Shift," etc.
4. Check the **Ignore Affiliations/Deaffiliations** checkbox to ignore affiliations and deaffiliations that occur outside of the scheduled times.
5. In the date and time grid, select each 30-minute period that the unit is allowed usage on. To select a 30-minute period, double-click on the period (cell). To select an entire day, double-click on the day (top of each column). To select a 30-minute period across all days, double-click the time (left-most column). To clear all selected periods, double-click on the upper-left cell of the grid.
6. When you are finished selecting time periods, click the **OK** button. This will close the *Add/Edit Schedule* window and return you to the GW_SAM main window. Notice that your new schedule now appears in the *Resources and ID Ranges* tree.

Editing a Schedule

To edit an existing schedule, take the following steps:

1. In the *Resources and ID Ranges* tree, select the schedule that you wish to edit. This will enable the **Edit** button if it is not already enabled.
2. Click the **Edit** button (Figure 1.1) or right-click on the schedule in the *Resources and ID Ranges* tree and choose **Edit…** from the resulting menu, or double-click the range in the tree. This will load the *Add/Edit Schedule* window.
3. Make the desired changes to the schedule.
4. Press the **OK** button to save your changes or press the **Cancel** button to abort the changes. Either of these actions will return you to the GW_SAM GUI.

Deleting a Schedule

To delete a schedule, take the following steps:

1. In the *Resources and ID Ranges* tree, select the schedule that you wish to delete. This will enable the **Delete** button if it is not already enabled.

2. Click the **Delete** button, or right-click on the schedule in the *Resources and ID Ranges* tree and choose **Delete…** from the resulting menu. This will result in a confirmation window.
3. Choose **Yes** to delete the selected schedule.

Copying a Schedule

Sometimes you may want to create a new schedule that is similar to an existing schedule. The **Copy** function is made to help save time in this process. To copy an existing schedule, take the following steps:

1. In the *Resources and ID Ranges* tree, select the schedule that you wish to copy.
2. Right-click on the selected schedule. This will open a context menu.
3. Click the **Copy** option from the menu. This will create a copy of the selected schedule. You will now see a schedule in the *Resources and ID Ranges* tree with the text "(1)." This schedule is the resulting copy of the selected schedule.
4. Edit the newly copied schedule. (See *Editing a Schedule* above).

Managing Resource ID Ranges

A resource ID range is a number range of IDs that share the same set of GW_SAM rules. A common example is even group IDs. Many systems only allow usage on odd-numbered group IDs. For these systems, when activity is detected on an even-numbered group, the activity is the result of a rogue user or incorrect programming. To monitor activity on even-numbered group IDs with GW_SAM, you need only set up one Resource ID Range for all even group IDs in the range 2-65534. This ID range will be 'Unallocated' (meaning that they are not provisioned on the system) or 'Unassigned' (meaning that they are provisioned on the system, but not for use).

Resource ID Range Rules

Below is a list of rules regarding resource ID ranges:

- ID values cannot overlap within a resource ID range type. For example, you cannot have a range of groups from 2 through 10 and a range of groups from 5 through 21. An exception to this is if the range from 2 through 10 contains even numbers only and the range from 5 to 21 contains odd numbers only. In this case the ranges do not truly overlap, because they do not share a number within the ranges. GW_SAM will not allow you to create overlapping resource ID ranges.
- Odd number ranges must begin and end with odd numbers, and even number ranges must begin and end with even numbers.

Adding Talkgroup ID Ranges

To add a talkgroup ID range, take the following steps:

1. In the *Resources and ID Ranges* tree, click on the **Talkgroup Ranges** entry that you wish to have as the parent of the new talkgroup ID range. This will enable the **Add** button if it is not already enabled.
2. Click the **Add** button under the *Resources and ID Ranges* tree, or right-click the **Talkgroup Ranges** node and choose **Add a New Talkgroup ID Range…** from the menu. This will load the *Add / Edit ID Range* window. (Figure 2.4). The WACN ID, system ID and type values are provided based on the *Resources and ID Ranges* tree entry that you had selected when you pressed the **Add** button. These values cannot be changed.
3. Enter the talkgroup ID range. Follow the rules in the *Resource ID Range Rules* section previously defined in this chapter. Remember to choose **Odd Only** or **Even Only** if either option applies. If neither is chosen, then all numbers in the range will be included.
4. Choose a **Validity Level**. Below is a definition for each option:
    - **Assigned:** IDs in this range are assigned to users and activity on these IDs is expected.
    - **Unassigned:** IDs in this range are provisioned on the Central Controller. However, these IDs are not assigned to anyone and should not receive activity.
    - **Unallocated:** IDs in this range are not provisioned on the Central Controller and should not receive activity.

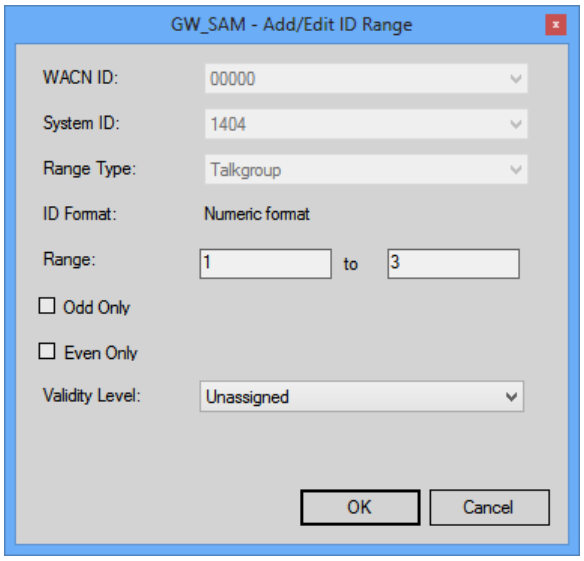


Figure 2.4 – Add / Edit Talkgroup ID Range Window

5. Once you are satisfied with the options for this ID Range, click the **OK** button. This will close the *Add / Edit ID Range* window and return you to the GW_SAM GUI. Notice that your new talkgroup ID range is now in the *Resources and ID Ranges* tree.

Adding Radio ID Ranges

To add a radio ID range, take the following steps:

1. In the *Resources and ID Ranges* tree, click on the **ID Ranges** entry that you wish to have as the parent of the new radio ID range. This will enable the **Add** button if it is not already enabled.
2. Click the **Add** button under the *Resources and ID Ranges* tree, or right-click the **Talkgroup Ranges** node and choose **Add a New Radio ID Range…** from the menu. This will load the *Add / Edit ID Range* window. (Figure 2.5). The system ID and type values are provided based on the *Resources and ID Ranges* tree entry that you had selected when you pressed the **Add** button. These values cannot be changed.

NOTE: If your radio ID ranges will use schedules, you must create these schedules before you can assign them to the radio ID ranges. See the *Managing Schedules* section above for instructions on creating schedules.

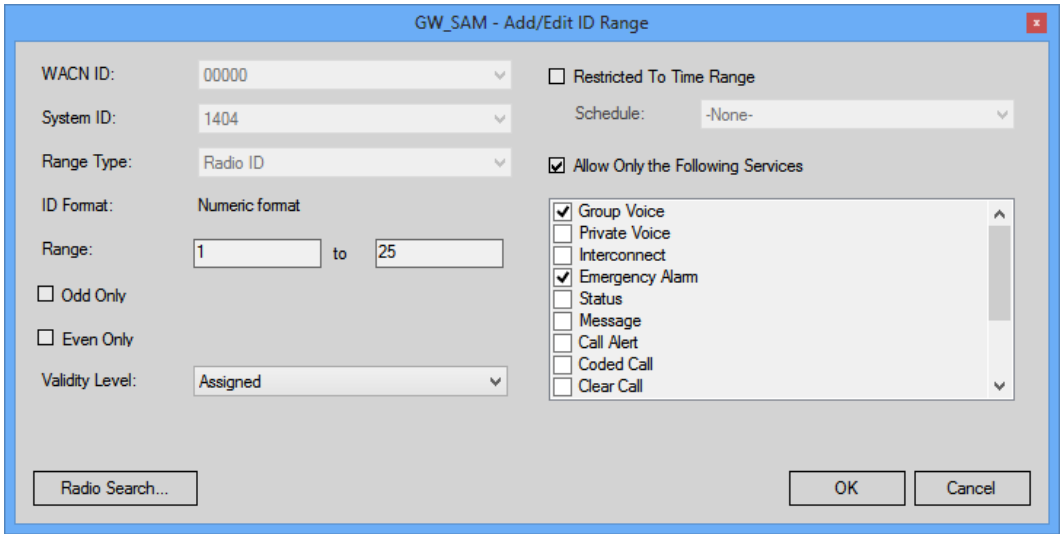


Figure 2.5 – Add / Edit ID Range Window

3. Enter the ID range. Follow the rules in the *Resource ID Range Rules* section previously defined in this chapter. Remember to choose **Odd Only** or **Even Only** if either option applies. If neither is chosen, then all numbers in the range will be included.
4. Choose a **Validity Level**. Below is a definition for each option:
   - **Assigned:** IDs in this range are assigned to users and activity on these IDs is expected.
   - **Unassigned:** IDs in this range are provisioned on the Central Controller. However, these IDs are not assigned to anyone and should not receive activity.
   - **Unallocated:** IDs in this range are not provisioned on the Central Controller and should not receive activity.
5. Optionally restrict the ID range to a specific time range by checking the **Restricted to Time Range** option. This option is only available if the ID

range has a **Validity Level** of *Assigned* selected. Checking the **Restricted to Time Range** option enables the **Schedule** combo box. Choose a schedule from the combo box.

6. Optionally restrict the services for this radio ID range by checking the **Allow Only the Following Services** option. This option is available only if the ID range has a **Validity Level** of *Assigned* selected. Checking the **Allow Only the Following Services** option enables the **Services** list box (below the checkbox). Select (double-click) the services that the radio ID range is expected to use. GW_SAM will consider a radio ID in this range suspect if it uses a service that is not selected in this list.
7. If you wish to set up Radio Search on this radio ID range, click the **Radio Search…** button. (See the *Radio Search* section for more information.)
8. Once you are satisfied with the options for this ID range, click the **OK** button. This will close the *Add / Edit ID Range* window and return you to the GW_SAM GUI. Notice that your new radio ID range is now in the *Resources and ID Ranges* tree.

The Dispatch service includes the following radio activities:

- **Affiliations:** If the radio affiliates to a group.
- **Busies:** If the radio receives a busy on a group.
- **Channel Assignments:** If the radio issues a group-based call.

Radio Search

On each radio ID range, you can enable the Radio Search option. Radio Search slowly sends a Radio Check command over your control channel for each radio ID in the radio ID range.

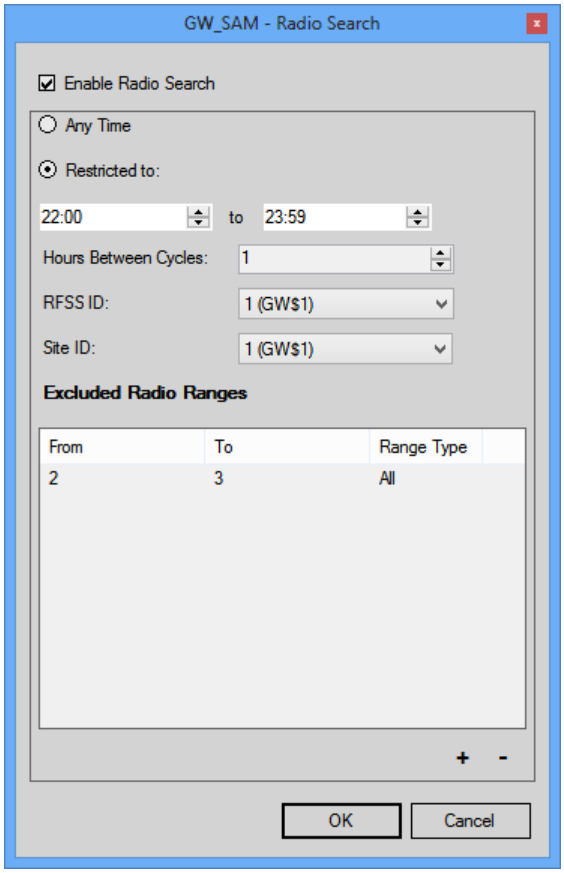


Figure 2.6 – Radio Search Window

In order to use Radio Search, you must be licensed for *RadioSearch* under the GW_SAM module and *RadioCheck* under the GW_Halcyon module.

You can monitor the progress of these Radio Search commands via the RCM Command window if you are logged in as the Admin user. The commands are archived in the Halcyon database and are available for reporting.

By specifying unallocated or unassigned radio ID ranges, you may use this feature to detect suspect radios operating on your system.

The following options are available on the *Radio Search* options window:

- **Enable Radio Search:** Enables radio search on this radio ID range.
- **Time of day restriction:** Allows you to restrict when radio searching occurs. This allows you to prevent radio search during peak hours.
    - **Any Time:** Perform radio search any time of day.
    - **Restricted to:** Restrict radio search to a time between the two specified times of day.
- **Hours Between Cycles:** Provides a minimum rest time between when the last radio search is performed on this radio ID range and when radio search for this radio ID range restarts.
- **RFSS ID:** RFSS ID targeted in this search.
- **Site ID:** Site ID targeted in this search.
- **Excluded Radio ID Ranges:** Ranges within the radio ID range that are excluded from the search.
    - **Add:** Add range to exclude from the radio search. This button loads the *Add Excluded Radio Search Range* window.
    - **Remove:** Remove all selected ranges from the *Excluded Radio Ranges* list.
- **OK:** Close the *Radio Search* window and save changes.
- **Cancel:** Close the *Radio Search* window and cancel changes.

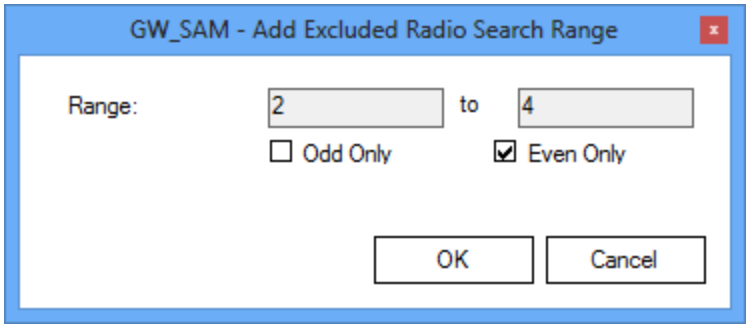


Figure 2.7 – Add Excluded Radio Search Range Window

Editing an ID Range

To edit a talkgroup or radio ID range, take the following steps:

1. In the *Resources and ID Ranges* tree, select the ID range that you wish to edit. This will enable the **Edit** button if it is not already enabled.
2. Click the **Edit** button or right-click the node and choose **Edit…** from the menu. This will load the *Add / Edit ID Range* window.
3. Change the options that you wish to change.
4. Once you are satisfied with the changes, click the **OK** button. This will save the changes, close the *Add / Edit ID Range* window and return to the GW_SAM GUI.

Deleting an ID Range

To delete a talkgroup or radio ID range, take the following steps:

1. In the *Resources and ID Ranges* tree, select the ID range that you wish to delete. This will enable the **Delete** button if it is not already enabled.
2. Click the **Delete** button or right-click the node and choose **Delete…** from the menu. This will result in a confirmation dialog box.
3. Click the **Yes** button to delete the selected ID range. This will remove the ID range from the *Resources and ID Ranges* tree.

Chapter 3 Using GW_SAM

This chapter describes how to use GW_SAM to monitor suspect activities.

This chapter contains the following sections:

- **Using the Suspect List**: Describes how to view and manipulate the *Suspect List*.
- **Using the Suspect Hotlist**: Describes how to view and manipulate the *Suspect Hotlist*.
- **Using the Suspect Exemption List**: Describes how to view and manipulate the *Suspect Exemption List*.
- **Changing GW_SAM Settings**: Describes the GW_SAM settings.
- **Suspect Notifications**: Describes user notifications of suspect activity.

GW_SAM contains many lists, like the one in Figure 3.1 below. Eliminate list columns that you do not wish to see by decreasing the column size to a 0 width. To decrease a column size:

1. Move the mouse over the right-most edge of the column's header. This will show the I-bar icon.
2. Click the left mouse button and move the mouse to the left until the column is invisible.

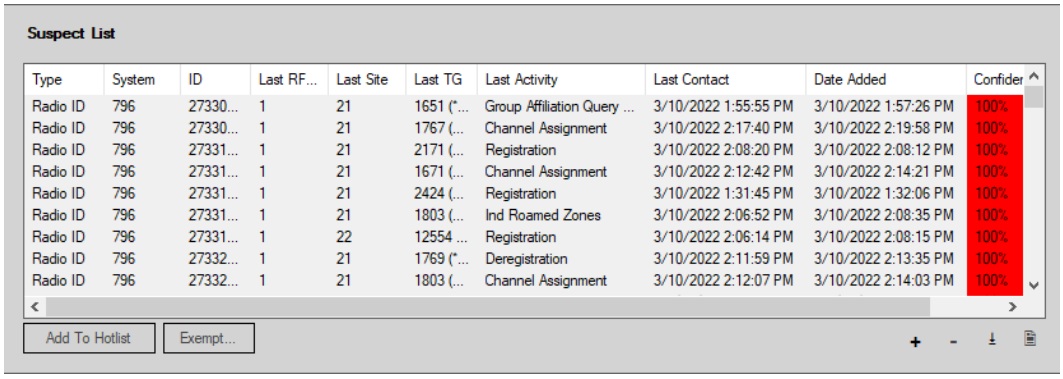
GW_SAM saves the current column widths for all lists whenever it is closed and restores the column widths whenever it is opened.

Using the Suspect List

The *Suspect List* contains each suspect that has been added due to suspicious activity and suspects that you have added manually. The *Suspect List* contains the following information about each suspect in the list:

- **Type:** The type of suspect ID. This will either be **Talkgroup** or **Radio ID**.
- **System:** The system ID of the suspect
- **ID:** The ID of the suspect. Its alias is shown in parentheses if it is not the default GW$ alias.
- **Last RFSS:** The last RFSS on which the suspect reported activity.
- **Last Site:** The last site on which the suspect reported activity.
- **Last TG:** The last talkgroup on which the suspect reported activity. Its alias is shown in parentheses if it is not the default GW$ alias.
- **Last Activity:** The last activity reported for the suspect.
- **Last Contact:** The last date and time the suspect reported activity.
- **Date Added:** The date and time the suspect was added to the *Suspect List*.

- **Confidence Level:** Number indicating how sure GW_SAM is that this is a suspect. The higher this number is, the more confident GW_SAM is that this is a suspicious ID.



Type	System	ID	Last RF...	Last Site	Last TG	Last Activity	Last Contact	Date Added	Confider
Radio ID	796	27330...	1	21	1651 (*...	Group Affiliation Query ...	3/10/2022 1:55:55 PM	3/10/2022 1:57:26 PM	100%
Radio ID	796	27330...	1	21	1767 (...	Channel Assignment	3/10/2022 2:17:40 PM	3/10/2022 2:19:58 PM	100%
Radio ID	796	27331...	1	21	2171 (...	Registration	3/10/2022 2:08:20 PM	3/10/2022 2:08:12 PM	100%
Radio ID	796	27331...	1	21	1671 (...	Channel Assignment	3/10/2022 2:12:42 PM	3/10/2022 2:14:21 PM	100%
Radio ID	796	27331...	1	21	2424 (...	Registration	3/10/2022 1:31:45 PM	3/10/2022 1:32:06 PM	100%
Radio ID	796	27331...	1	21	1803 (...	Ind Roamed Zones	3/10/2022 2:06:52 PM	3/10/2022 2:08:35 PM	100%
Radio ID	796	27331...	1	22	12554 ...	Registration	3/10/2022 2:06:14 PM	3/10/2022 2:08:15 PM	100%
Radio ID	796	27332...	1	21	1769 (*...	Deregistration	3/10/2022 2:11:59 PM	3/10/2022 2:13:35 PM	100%
Radio ID	796	27332...	1	21	1803 (...	Channel Assignment	3/10/2022 2:12:07 PM	3/10/2022 2:14:03 PM	100%

Figure 3.1 – GW_SAM Suspect List

It is possible to receive suspect activity on a radio ID or a group that does not exist in your GW_Alias database. You may see a value in the **ID** or **Last TG** columns with a (*NOT FOUND*) next to the radio ID or group. This means that the radio ID or group does not exist in the GW_Alias database.

Suspect List Options

New

The **New** button allows you to manually add a suspect to the *Suspect List*. You may want to add a suspect if you know a radio ID or group ID is being abused, but you have not yet seen activity on it. Once the suspect has been added, GW_SAM will begin to keep a detailed history of the activity reported on the suspect ID. To manually add a suspect, take the following steps:

1. Click the **New** button below the *Suspect List***.** This will load the *Add Suspect* window (Figure 3.2).

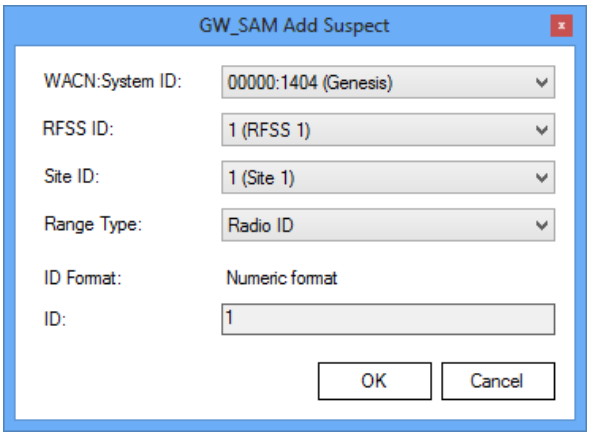


Figure 3.2 – Add Suspect Window

2. Choose the **WACN:System ID**.

3. Choose an **RFSS ID**.
4. Choose a **Site ID**.
5. Choose the **Range Type**. These values include:
    - **Radio ID**
    - **Talkgroup**
6. Type the **ID**.
7. Click the **OK** button to add the suspect. This will close the *Add Suspect* window and return you to the GW_SAM GUI.

Delete

The **Delete** button allows you to delete a suspect from the *Suspect List*. You may wish to delete a suspect that was manually added or a suspect that has not received activity in a while. To delete a suspect from the *Suspect List*, take the following steps:

1. Select the suspect that you wish to delete from the *Suspect List*. This will enable the **Delete** button if it is not already enabled.
2. Click the **Delete** button or right-click the suspect and choose **Delete…** from the menu. This will result in a confirmation dialog box.
3. Click the **Yes** button to delete the suspect. This will remove the suspect from the *Suspect List* and delete any history related to the suspect.

Exempt

The **Exempt** button allows you to move a suspect from the *Suspect List* to the *Suspect Exemption List*. You may want to mark a suspect as 'exempt' if the suspect exhibits behaviors that result in false suspicious activity. To exempt a suspect from the **Suspect List**, take the following steps:

1. Select the suspect that you wish to exempt from the *Suspect List*. This will enable the **Exempt** button if it is not already enabled.
2. Click the **Exempt** button or right-click the suspect and choose **Exempt…** from the menu. A confirmation dialog will be displayed for each selected suspect.
3. Click **Yes** to exempt the suspect, **No** to skip to the next suspect, (if multiple suspects were selected), or **Cancel** to abort all remaining exemptions.

Add to Suspect Hotlist

The *Suspect Hotlist* is a list of suspects, taken from the *Suspect List*, which you would like to monitor more closely. The *Suspect Hotlist*, described in the *Using the Suspect Hotlist* section, provides additional tracking information for suspects. To add a suspect to the *Suspect Hotlist*, take the following steps:

1. Select the suspect you wish to add to the *Suspect Hotlist***.** This will enable the **Add to Hotlist** button if it is not already enabled.
2. Click the **Add to Hotlist** button or right-click the suspect and choose **Add to Hotlist** from the menu. This will add the suspect to the *Suspect Hotlist*.

History

GW_SAM keeps detailed activity information for each suspect in the *Suspect List*. This information is called History. To view the history for a suspect in the *Suspect List*, take the following steps:

1. Click on the suspect for which you wish to view history. This will enable the **History** button if it is not already enabled.
2. Click the **History** button, right-click the suspect and choose **History…** from the menu, or double-click the suspect. This will load the *Suspect History* window (Figure 3.3).

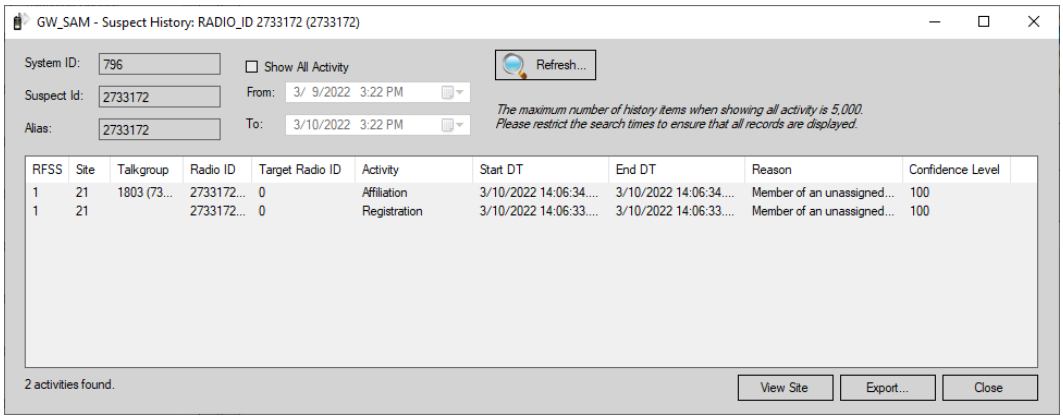


Figure 3.3 – Suspect History window

3. Press the **Close** button on the *Suspect History* window to return to the GW_SAM GUI.

The *Suspect History List* contains the following columns:

- **RFSS:** The RFSS on which the activity was reported.
- **Site:** The site on which the activity was reported.
- **Source:** The source site on which the activity was reported (ATIA only).
- **Talkgroup:** The group on which the activity was reported. Its alias is shown in parentheses if it is not the default GW$ alias.
- **Radio ID:** The radio ID on which the activity was reported. Its alias is shown in parentheses if it is not the default GW$ alias.
- **Target Radio ID:** The target radio ID involved in the activity (if any). Its alias is shown in parentheses if it is not the default GW$ alias.
- **Activity:** Description of the activity.
- **Start DT:** Date and time the activity started.
- **End DT:** Date and time the activity ended.

- **Reason:** The reasons this activity was deemed as suspect (if any).
- **Confidence Level:** The percent confidence that GW_SAM has that this is suspect activity (if a reason is provided).

GenWatch3 stores the last 30 days of suspect activity for each suspect. Suspect history is purged via the centralized GenWatch3 purging operation. This length of time can be adjusted with the help of GenWatch3 support personnel.

It is possible to receive suspect activity on a radio ID or a talkgroup that does not exist in your GW_Alias database. You may see a value in the **Talkgroup**, **Radio ID** or **Target Radio ID** columns with a (*NOT FOUND*) next to the talkgroup, radio ID or target radio ID. This means that the talkgroup, radio ID or target radio does not exist in the GW_Alias database.

The **View Site** button shows a graphical representation of the site activity included in the history results. This requires settings for **Latitude**, **Longitude** and **Coverage Radius** for each site to be in place in GW_Alias.

By default, the *Suspect History* window will show only suspect activities with suspect reasons (i.e. activities that would result in the resource to be added to the *Suspect List*). From the *Suspect History* window, you can also view detailed activity. To view the detailed activity for a suspect, take the following steps:

1. Load the *Suspect History* window. This will show the suspect activities for the selected suspect.
2. Click the **Show All Activity** checkbox.
3. Choose your **From** date/time and **To** date/time. These will default to:
    a. 24 hours ago for the **From** value
    b. Now for the **To** value
4. Press the **Enter** key or click on the **Refresh** button. This will query the database for all activities for this suspect within the given **From** and **To** date/time values.

Export

SAM allows you to export the activity in its *Suspect List*. To export the *Suspect List*, click the **Export** button. Alternatively, you can right-click the list and choose **Export…**. You will be prompted to specify the name of file in which to save the records.

Print

GW_SAM allows you to print the activity in its *Suspect List*. To print the *Suspect List*, take the following steps:

1. Select the activity in the *Suspect List* that you wish to print. Select a range by clicking on the first activity and holding **Shift** while clicking on the last activity in the desired range. If you wish to print all the activity in the *Suspect List*, skip this step.

2. Right-click on the *Suspect List* and choose **Print …** from the menu. This will show the printer options window specific to your default printer.
3. Select the options for your printer. It is usually best to choose to print in landscape mode (not portrait).
4. Click **OK** once you are satisfied with your printer options. This will result in a dialog asking if you want to print the selected items or all items.
5. Click **OK** to print.

You can also access these options by right-clicking an item in the *Suspect List*.

Using the Suspect Hotlist

The *Suspect Hotlist* contains each suspect that has been manually added from the *Suspect List*. This list holds the suspect resources that we wish to watch more closely. The *Suspect Hotlist* contains the following information about each suspect in its list:

- **Type:** The type of suspect ID. This will either be **Talkgroup** or **Radio ID**.
- **System:** The system ID of the suspect.
- **ID:** The ID of the suspect. Its alias is shown in parentheses if it is not the default GW$ alias.
- **# PTTs:** The number of push-to-talks that have been received by the ID (or on IDs in the group, in the case of suspect groups) since the suspect was added to the *Suspect List***.**
- **# Affiliations:** The number of affiliations that have been received by the ID (or by IDs in the group, in the case of suspect groups) since the suspect was added to the *Suspect List*.
- **Distinct Groups:** The total number of groups that the suspect has issued or received activity on (always 1 in the case of suspect groups).
- **Total Airtime (sec.):** The total airtime (in seconds) that the suspect has issued activity for. For suspect groups, this will include all radio IDs on the group.
- **Last Contact:** The last date and time the suspect reported activity.

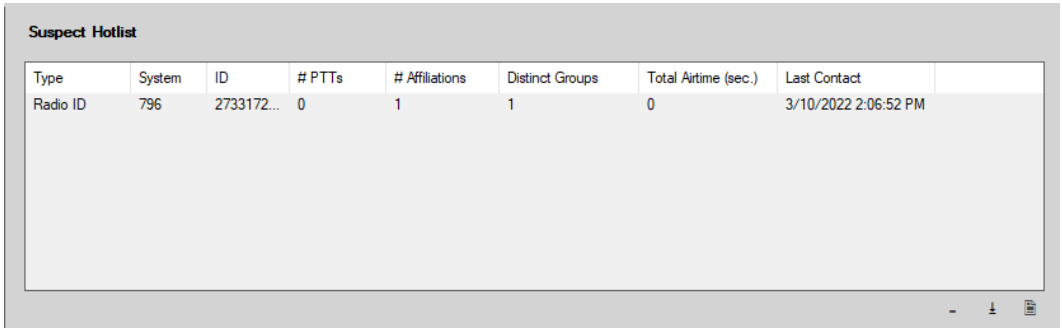


Figure 3.4 – GW_SAM Suspect Hotlist

Suspect Hotlist Options

Remove

The **Remove** button allows you to remove a suspect from the *Suspect Hotlist*. The suspect will not be removed from the *Suspect List*. To remove a suspect from the *Suspect Hotlist*, take the following steps:

1. Select the suspect that you wish to remove from the *Suspect Hotlist*. This will enable the **Remove** button if it is not already enabled.
2. Click the **Remove** button or right-click the suspect and choose **Remove…** from the menu. This will result in a confirmation dialog message box.
3. Click the **Yes** button. This will remove the suspect from the *Suspect Hotlist*.

Once you remove a suspect from the *Suspect Hotlist*, you may need to unselect the removed suspect in the *Suspect List* before the **Add to Hotlist** option is available for the removed suspect.

History

GW_SAM keeps detailed activity information for each suspect in the *Suspect List*, including all suspects in the *Suspect Hotlist*. This information is called History. To view the history for a suspect in the *Suspect Hotlist*, take the following steps:

1. Select the suspect for which you wish to view history. This will enable the **History** button if it is not already enabled.
2. Click the **History** button, right-click the suspect and choose **History…** from the menu or double-click the suspect. This will load the *Suspect History* window (Figure 3.3).
3. Click the **Close** button on the *Suspect History* window to return to the GW_SAM GUI.

Export

SAM allows you to export the activity in its *Suspect Hotlist*. To export the *Suspect Hotlist*, click the **Export** button. Alternatively, you can right-click the list and choose **Export…**. You will be prompted to specify the name of file in which to save the records.

Print

1. Select the activity in the history list that you wish to print. Select a range by clicking on the first activity and holding **Shift** while clicking on the last activity in the desired range. If you wish to print all the activity in the history list, skip this step.
2. Right-click on the *Suspect Hotlist* and choose **Print …** from the menu. This will show the printer options window specific to your default printer.
3. Select the options for your printer. It is usually best to choose to print in landscape mode (not portrait).
4. Click **OK** once you are satisfied with your printer options. This will result in a dialog asking if you want to print the selected items or all items.

5. Click **OK** to print.

You can also access these options by right-clicking an item in the *Suspect Hotlist*.

Using the Suspect Exemption List

The *Suspect Exemption List* contains each suspect that has been marked as exempt.

You may want to mark a suspect as "exempt" if the suspect exhibits behaviors that result in false suspicious activity. The *Suspect Exemption List* is accessed using the **Exempt Suspects…** menu option on the **Options** menu. The *Suspect Exemption List* contains the following information about each exempt suspect in the list:

- **Type:** The type of suspect ID. This will either be **Talkgroup** or **Radio ID**.
- **ID:** The ID of the suspect. Its alias is shown in parentheses if it is not the default GW$ alias.
- **Last RFSS:** The last RFSS on which the suspect reported activity.
- **Last Site:** The last site on which the suspect reported activity.
- **Last TG:** The last talkgroup on which the suspect reported activity. Its alias is shown in parentheses if it is not the default GW$ alias.
- **Last Activity:** The last activity reported for the suspect.
- **Last Contact:** The last date and time the suspect reported activity.
- **Confidence Level:** Number indicating how sure GW_SAM is that this is a suspect. The higher this number is, the more confident GW_SAM is that this is a suspicious ID.

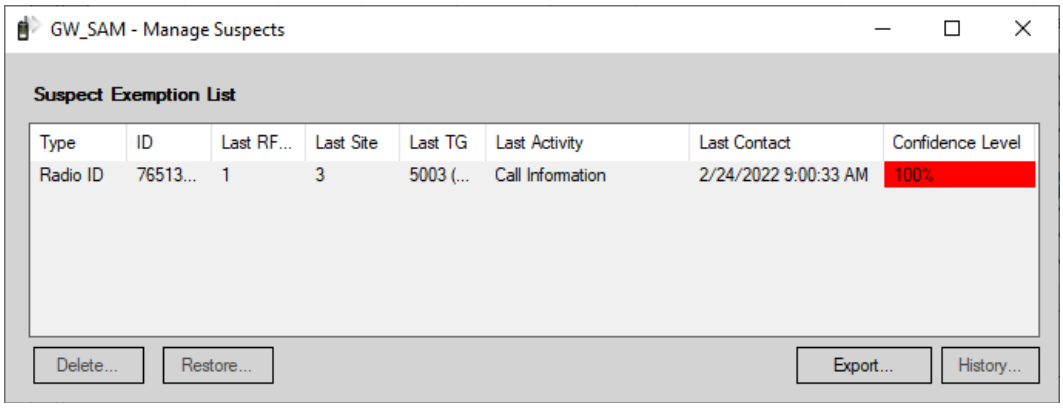


Figure 3.5 – Manage Suspects Window

Once a suspect is exempted, GW_SAM will stop storing detailed activity for the suspect.

When the *Manage Suspects* window is opened, the user will have exclusive access to it for 10 minutes or until the window is closed. During this time, other clients will not be able to access the window.

Suspect Exemption List Options

Delete

The **Delete…** button allows you to delete a suspect from the *Suspect Exemption List*. You may wish to delete an exempt suspect that was manually added or a suspect that has not received activity in a while. To delete a suspect from the *Suspect Exemption List*, take the following steps:

1. Select the suspect that you wish to delete from the *Suspect Exemption List*. This will enable the **Delete…** button if it is not already enabled.
2. Click the **Delete…** button or right-click the suspect and choose **Delete…** from the menu. This will result in a confirmation dialog box.
3. Click the **Yes** button to delete the suspect. This will remove the suspect from the *Suspect Exemption List* and delete any history related to the suspect.

Restore

The **Restore…** button moves a suspect out of the *Suspect Exemption List* and back into the main *Suspect List*. To restore a suspect to the *Suspect List*, take the following steps:

1. Select the suspect that you wish to restore to the *Suspect List*. This will enable the **Restore…** button if it is not already enabled.
2. Click the **Restore…** button or right-click the suspect and choose **Restore…** from the menu. This will result in a confirmation dialog.
3. Confirm the move, by clicking the **Yes** button. This will move the suspect from the *Suspect Exemption List* back into the *Suspect List*.

History

Once a suspect is added to the *Suspect Exemption List*, existing radio activity information is retained, but additional activity will not be recorded. This information is called History. To view the history for a suspect in the *Suspect Exemption List***,** take the following steps:

1. Select the suspect for which you wish to view history. This will enable the **History…** button if it is not already enabled.
2. Click the **History…** button, right-click the suspect and choose **History…** from the menu, or double-click the suspect. This will load the *Suspect History* window (Figure 3.3).
3. Click the **Close** button on the *Suspect History* window to return to the GW_SAM GUI.

Export

SAM allows you to export the activity in its *Suspect Exemption List*. To export the *Suspect Exemption List*, click the **Export** button. Alternatively, you can right-click the list and choose **Export…**. You will be prompted to specify the name of file in which to save the records.

Print

1. Select the activity in the history list that you wish to print. Select a range by clicking on the first activity and holding **Shift** while clicking on the last activity in the desired range. If you wish to print all the activity in the history list, skip this step.
2. Right-click on the *Suspect Exemption List* and choose **Print …** from the menu. This will show the printer options window specific to your default printer.
3. Select the options for your printer. It is usually best to choose to print in landscape mode (not portrait).
4. Click **OK** once you are satisfied with your printer options. This will result in a dialog asking if you want to print selected items or all items.
5. Click **OK** to print.

You can also access these options by right-clicking an item in the *Suspect Exemption List*.

Changing GW_SAM Settings

The *Settings* window allows you to customize the settings for GW_SAM.

Overlap

This tab contains two settings, the second of which is explained in detail on the window.

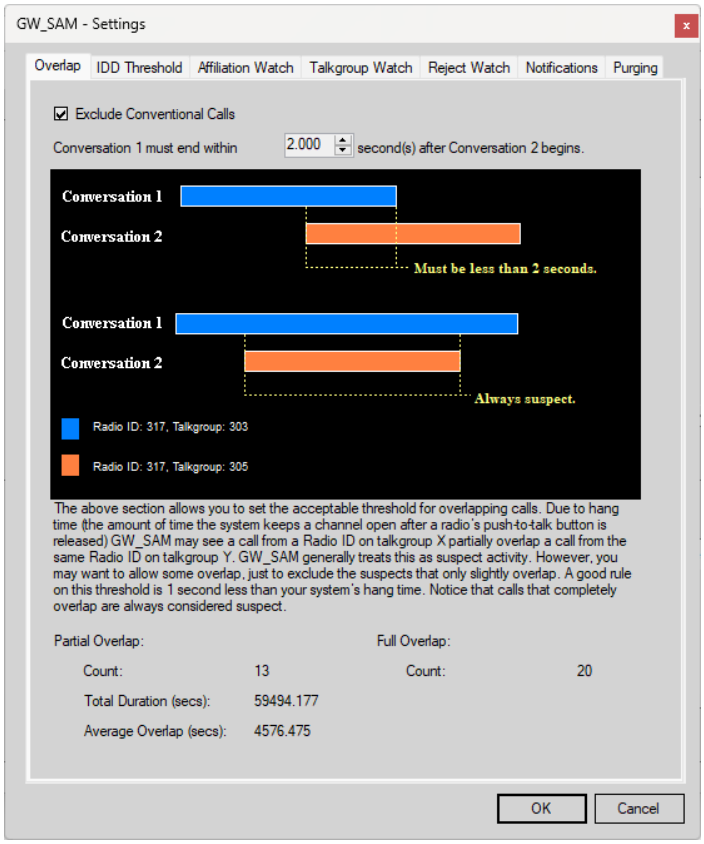


Figure 3.6 – GW_SAM Settings – Overlap Tab

The Exclude Conventional Calls setting does just that, exclude conventional calls when checking for overlapping calls.

The overlap statistics section is provided to better help you gauge the ideal overlap threshold setting.

Multisite data may not report overlapping calls in the same way as control channel data. If your GenWatch3 is receiving data from a multisite data source, set your Overlap Threshold to 0.000 seconds. This will allow GW_SAM to detect calls that begin and end at the same time. For some multisite configurations, this is the only way to detect partially overlapping calls.

Impossible Driving Distance (IDD) Threshold

This tab contains three values:

- Assumed driving speed (adjustable)
- Ignored IDD Suspect Threshold (adjustable)
- Average Broadcast Radius

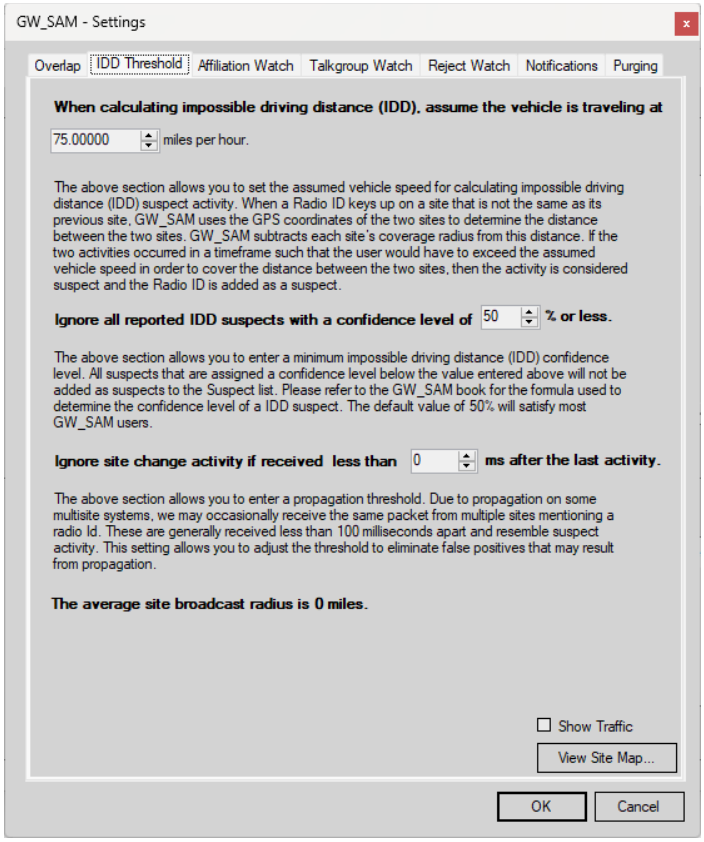


Figure 3.7 – GW_SAM Settings – IDD Threshold Tab

Assumed Driving Speed

When GW_SAM calculates an IDD, it uses this value as the maximum speed with which a radio ID could travel from point A to point B. If a radio ID keys up in such a way that it moved from point A to point B faster than the Assumed Driving Speed, the radio ID is considered a suspect.

Ignored IDD Suspect Threshold

This value allows you to ignore IDD suspects that are added with a low confidence level. You may wish to increase this value based on the quality of IDD suspects being reported by GW_SAM. The logic used to derive IDD suspects is not exact, because GW_SAM is not provided with the exact broadcast limitations of each site and because terrain is variable.

Ignore Site Change Threshold

This value indicates the amount of time in milliseconds to wait before processing data from a source site ID that differs from a radio ID's previous source site ID. Adjust this threshold to prevent false positives when propagation results in activity from the radio's nearby sites presented as if they were the radio's source site.

Average Broadcast Radius

This value indicates the average broadcast radius among all sites in all systems. This value is used in the IDD formula described below.

The IDD Formula

The IDD formula consists of two separate calculations:

- SMPH: Miles per hour required to cover the distance between two sites (minus the broadcast radiuses of the two sites) in the given amount of time.
- SMID: Miles in the distance between two sites (minus the broadcast radiuses of the two sites).

Given the two sites:

- Site ID: 1
    - Coverage Radius: 16 miles
    - Latitude: 13
    - Longitude: 14
- Site ID: 2
    - Coverage Radius: 14 miles
    - Latitude: 13
    - Longitude: 14.5

Kilometers are converted to miles before being used in the IDD Formula.

GPS values less than 1 positive or negative degree in both latitude and longitude will be ignored.

The distance between these two sites is approximately 33.66 miles. If radio ID 301 issues a push-to-talk with a reported source site of 1 and one minute later issues a push-to-talk with a reported source site of 2, the radio ID traveled 3.66 miles in 1 minute (distance between the two sites – (each site's coverage radius)) = (33.66 – (16 + 14)).

Covering 3.66 miles in 1 minute requires a speed of 219.6 mph. GW_SAM takes this speed and compares it with the assumed driving speed value above. In this example, we have 75 mph as the assumed driving speed. To determine the SMPH value, GW_SAM subtracts the assumed driving speed from the actual speed and caps the value off at 100.

SMPH = 219.6 mph – 75 mph = 144.6 mph (capped off at 100 mph = 100 mph)
So SMPH = 100

Next, GW_SAM calculates the SMID multiplier. This value decreases the confidence level, based on how small a distance was traveled. The SMID multiplier is derived by dividing the distance the radio ID traveled by the average broadcast radius (capped off at 100).

SMID = distance / average site broadcast radius = 3.66 / 15 = 0.244

The overall confidence level of this suspect activity = SMPH * SMID = 100 * 0.244 = 24.4%

IDD Formula Conclusion

As demonstrated, the above value is not a very high confidence level; and rightfully so. If a human were looking at these values they would, most likely, come to the same conclusion. This looks like a case where sites 1 and 2 are adjacent sites. The coverage radii provided for these two sites are either slightly off (as expected in estimated values) or the radio ID found site 2 after topping a hill, etc. If the Ignored IDD Suspect Threshold is 25 or more, this suspect will not be added to the GW_SAM Suspect List.

View Site Map

The **View Site Map** option shows a graphical representation of how your sites are geographically positioned, based on the **Longitude**, **Latitude** and **Broadcast Radius** values provided for each site in the GW_Alias window. To view the *Site Map* window, follow the steps below:

1. Load the *Settings* window by clicking on the **Settings** button.
2. Click on the *IDD Threshold* tab.
3. Click on the **View Site Map** button. This will load the *Site Map* window.

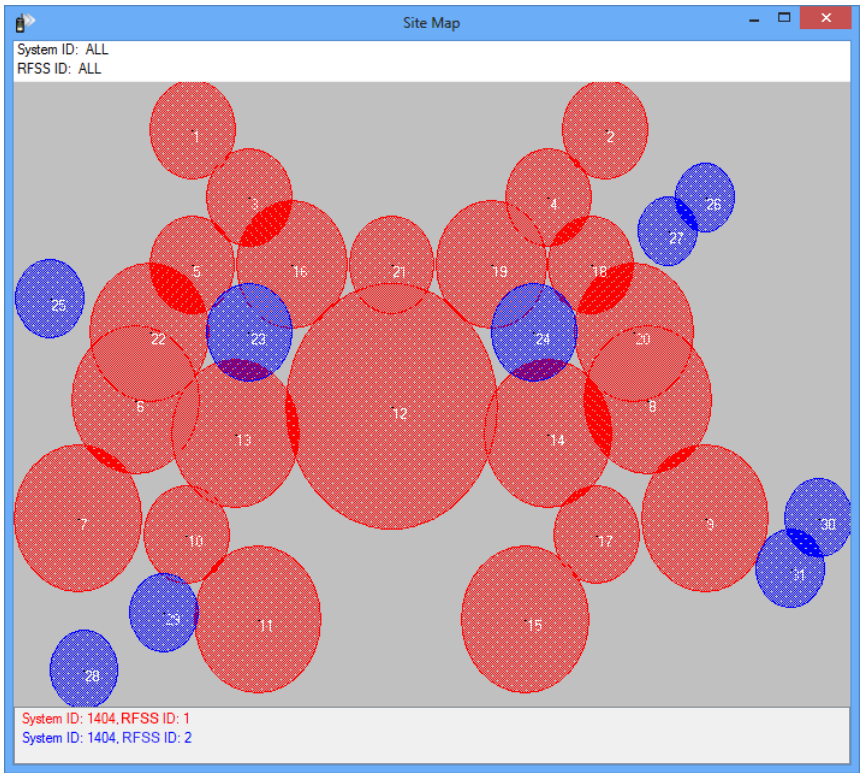


Figure 3.8 – Site Map Window

Affiliation Watch

This tab allows you to define how you expect radios to affiliate on your system. This tab also allows you to choose whether to automatically disable a radio with an ID in an unallocated ID range that generates activity. For more on how to create an unallocated ID range in GW_SAM, see *Chapter 2 – Setting Up GW_SAM*.

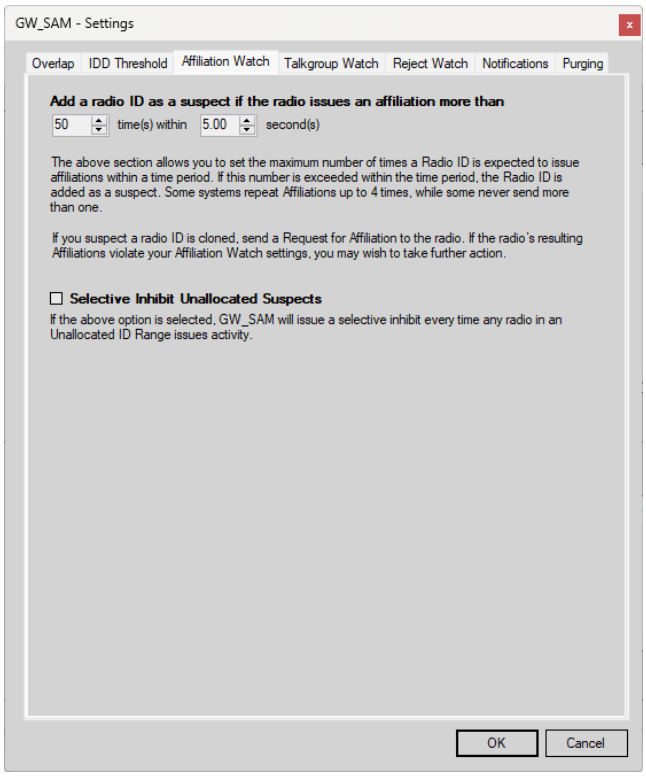


Figure 3.9 – GW_SAM Settings – Affiliation Watch Tab

If a single radio affiliates more often than the **time(s)** value within the **second(s)** value, the radio ID will be added as a suspect with 75% confidence. If you do not wish to use this feature, set the **time(s)** value to 99, the highest possible value.

When GenWatch3 receives activity from a system, GW_SAM checks it against all defined ID ranges. If the ID responsible for this activity falls within an unallocated range, GW_SAM will add it to the *Suspect List*. Lastly, if this checkbox is checked, GW_SAM will immediately issue an inhibit command, targeting the suspect radio. Subsequently, GW_SAM will issue an inhibit command every time the suspect radio generates activity, unless an automatic command is already pending to that ID. To prevent inhibits from unintentionally being sent repeatedly, after an automatic inhibit command is issued, new activity within 60 seconds will not trigger a new command.

This option is licensed separately and will only show up if licensed for *SelectiveInhibit*.

Talkgroup Watch

When you set up a talkgroup range in GW_SAM, you will get GUI notifications of any suspect activity on that range. That alert allows you to manually follow up to decide the appropriate actions to take.

In some circumstances, however, when a talkgroup is added to the *Suspect List*, you will also want to add any radio using that talkgroup to the *Suspect List*. Checking the box labeled **Add radio IDs on suspect talkgroups to Suspect List** will automatically add radio IDs to the *Suspect List* if they generate activity on a talkgroup that breaks the rules defined for that talkgroup.

Usage examples:

- **Cut off a specific talkgroup:** Imagine you have a customer on your system that uses 30 radios operating on talkgroup 16. If you wish to cut off the customer's access to your system without manually inhibiting every radio, create a talkgroup ID range of 16-16 and set its validity level to **Unallocated**. If the **Talkgroup Watch** and **Automatic Inhibit** options are checked, each radio will be inhibited automatically after it generates activity.
- **Prevent unauthorized talkgroups from using the system:** If authorized users on your system should be using talkgroups 1-10, create a talkgroup range from 11 to the maximum ID range on your system. If the **Talkgroup Watch** and **Automatic Inhibit** options are checked, any radio will be inhibited automatically after it generates activity on an invalid talkgroup.

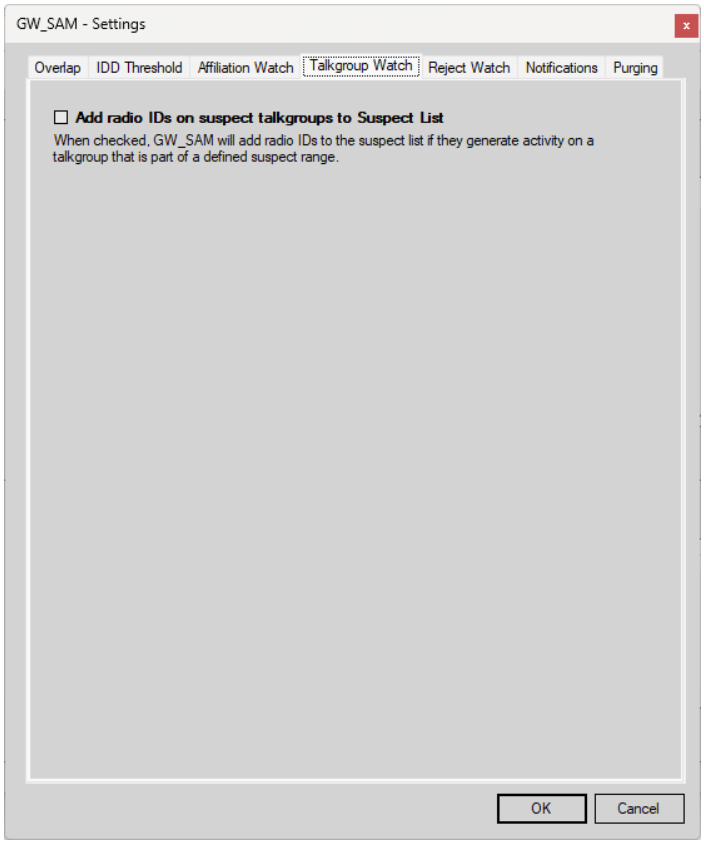


Figure 3.10 – GW_SAM Settings – Talkgroup Watch Tab

Reject Watch

This tab allows you to configure GW_SAM to respond to radio rejects on your system. If the reject matches the criteria configured on this tab, GW_SAM will add the ID responsible to the *Suspect List*.

When GenWatch3 receives a reject from a system, GW_SAM checks it against the reasons selected. Check the reasons that you wish to consider suspect activity. Reasons in the Recommended category may represent suspect activity. Reasons in the Not Recommended category are unlikely to represent suspect activity.

Recommended

The **Recommended** button will select all reasons in the Recommended category.

Other Rejects

The **Other Rejects** button will select all reasons in the Other Rejects category.

Clear

The **Clear** button will unselect all reasons.

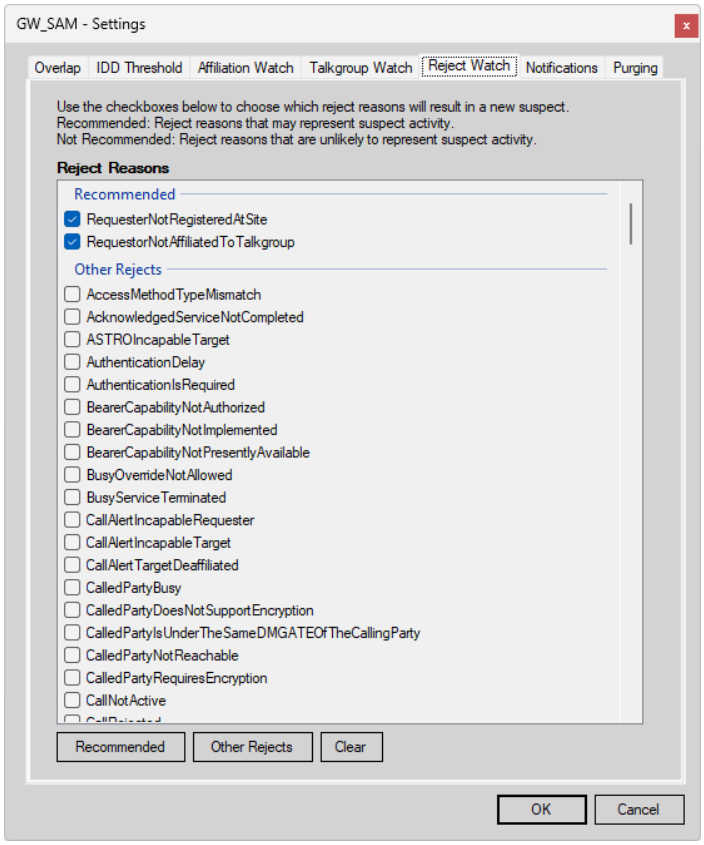


Figure 3.11 – GW_SAM Settings – Reject Watch Tab

Notifications

This window allows you to choose which suspect reasons result in a GUI notification (see the *Suspect Notifications* section) of a new suspect.

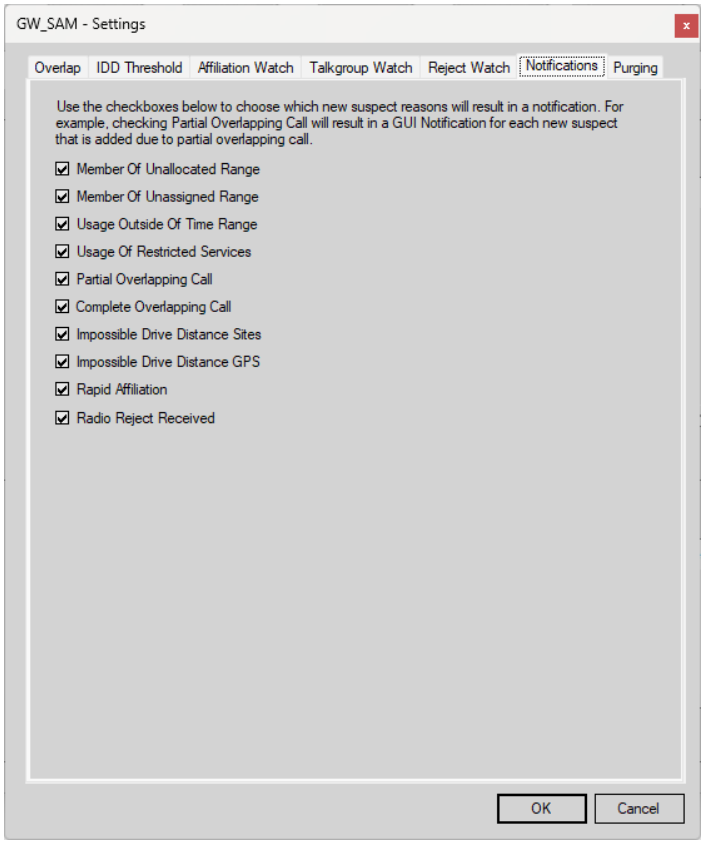


Figure 3.12 – GW_SAM Settings – Notifications Tab

Each checkbox on this window represents a reason why GW_SAM adds a suspect to the *Suspect List*. If you do not wish to receive a GUI notification when a suspect is added for a particular reason, uncheck that reason.

Purging

This window allows you to define how many suspects will be kept in the *Suspect List*. Limiting the size of the *Suspect List* will improve the performance of the GW_SAM module and make the list easier to view and maintain.

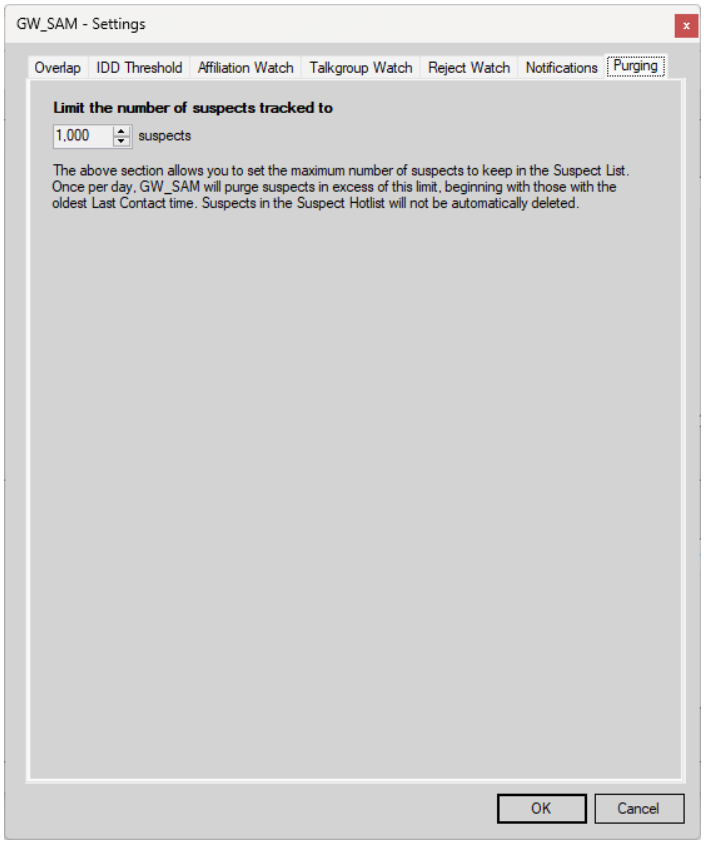


Figure 3.13 – GW_SAM Settings – Purging Tab

Once per day (around midnight local time), if the number of suspects exceeds the specified limit, GW_SAM will delete enough suspects to reduce the number down to the defined limit. Suspects will be deleted in ascending order by their Last Contact time, so the first suspects deleted are the ones that have not been seen on the radio system for the longest amount of time. Any suspects that have been placed in the *Suspect Hotlist* will never be automatically deleted.

Deleting a suspect also deletes the suspect history kept by the GW_SAM module. However, it will not delete any data from the archive tables used for reporting.

The number of suspects deleted by this process will be logged to the Windows event log.

Suspect Notifications

When GW_SAM adds a new suspect to the *Suspect List*, it also sends out a GenWatch3 GUI Notification. These are the same notifications discussed in *Chapter 10: GenWatch3 Notifications* of the *GenWatch3 Core Manual*.

For each new suspect, the GW_Alerts GUI shows a GenWatch3 GUI Notification window. This window's ***Desc.*** column shows:

- **Suspect Type:** Talkgroup or Radio ID.
- **Level:** Percent confidence level that this activity is unwanted activity.
- **Reason:** Why the activity is considered suspect.

These notifications are only shown to GenWatch3 users with the GW_Security *Administrator* privilege.

The GenWatch3 GUI Notification is accompanied by a sound of breaking glass (to denote breaking and entering). This sound file is named *NewSuspect.wav* and is located in the installation directory of GenWatch3 (by default *C:\Program Files\Genesis\GenWatch3*). GenWatch3 ships with two additional sound files:

- *NewSuspect2.wav*: Longer version of the breaking glass sound
- *NewSuspect3.wav*: Creaking door

To change the new suspect notification sound to one of the other sound files, follow the steps below:

1. Browse to the GenWatch3 installation directory.
2. Right-click on the *NewSuspect.wav* file. This will show the file options menu.
3. Choose **Rename** from the file options window.
4. Rename the file *NewSuspect.wav* to *NewSuspect1.wav*.
5. Right-click on the file that you wish to use as the new suspect sound file. This will show the file options menu.
6. Choose **Rename** from the file options window.
7. Rename the file to *NewSuspect.wav*.

You are not limited to replacing the *NewSuspect.wav* file with the ones provided in the GenWatch3 installation. If you have a .wav file you would prefer to hear for suspects, follow the steps above to rename your file to *NewSuspect.wav*.