



GW3-TRBO®
SAM
Software Version 2.16.4
Module Book

GW3-TRBO®

600-2.16.4-J.1
4/5/2019

Trademarks

The following are trademarks of Motorola: MOTOTRBO™.

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

The Genesis Group Trademark Information

GW3-TRBO® is a registered trademark of GenCore Candeco, LTD., a subsidiary of Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks.

Copyright

Copyright © 2006-2019; Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks. All rights are reserved. No part of this publication or the associated program may be reproduced, transmitted, transcribed, in whole or in part, in any form or by any means, whether it is mechanical, magnetic, optical, electronic, manual or otherwise, without the prior written consent of Burks GenCore Co., Inc. D.B.A:

The Genesis Group and Phil Burks
5800 Eagles Nest Blvd
Tyler, Texas 75703.

Includes technology licensed from Motorola.

Disclaimer

The GW3-TRBO Users Manual is printed in the U.S.A. Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks believe that the information included in this manual is correct; however, Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks reserves the right to alter, revise and make periodic changes to the manual and its contents. Burks GenCore Co., Inc. D.B.A. The Genesis Group does not assume responsibility to notify any person of such revisions or changes. While we have taken strides to carefully examine our software and documentation and believe that it is reliable, the Genesis Group and Phil Burks assume no responsibility for the use of the manual, or GW3-TRBO software, nor for any patent infringements or other rights of third parties who may use the manual or the GW3-TRBO software. Burks GenCore Co., Inc. D.B.A. The Genesis Group and Phil Burks make no representations or warranties with respect to the contents or fitness for a particular purpose beyond the cost of the software paid by the end-user.

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

License

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

Refer to the GW3-TRBO Manual Overview for your full license. All license information contained on pages 4-7 (Book 600-2.16.4-AA.1) are to be considered as contained herein.

Support

Customer satisfaction is our number one priority at Genesis. We are here to provide you with the best software possible, and we want to know when you have any questions, concerns or problems with GW3-TRBO so that we can make it a better product for everyone.

Refer to the *Troubleshooting & Support* section of the GW3-TRBO Manual Shell (Book 600-2.16.4-AA.1) for complete support and contact information.

Document History

Revision	Description	Author
2.0.5	Initial Release	JAW
2.0.5	Replaced GW3-TRBO trademark with registered trademark.	JAW
2.0.6	Updated screenshots with F1 Help	REB
2.0.6	Updated screenshots	CLB
2.0.6	Added note to Radio Search section	WRK
2.0.6.6	Revisions for release	TDW
2.1	Added IP Console Inhibit and Slot Disable information	REB
2.1	Revisions for release	WRK
2.1	Updates of Screenshots and Descriptions	CWF
2.2	Initial Version Updates	CWF
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	Updated screenshot of Notification Options	WRK
2.8	Revisions Before Release	ATG
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

Table of Contents

<i>Trademarks</i>	3
<i>The Genesis Group Trademark Information</i>	3
<i>Copyright</i>	3
<i>Disclaimer</i>	3
<i>License</i>	3
<i>Support</i>	3
DOCUMENT HISTORY	4
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 SAM?	9
WHAT IS A SUSPECT?	11
CHAPTER 2 SETTING UP SAM	13
RESOURCES & ID RANGES TREE	13
<i>Managing Schedules</i>	14
Managing Schedules	14
Adding a Schedule	15
Editing a Schedule	15
Deleting a Schedule	16
Copying a Schedule	16
<i>Managing Resource ID Ranges</i>	17
Resource ID Range Rules	17
Adding Talkgroup ID Ranges	18
Adding Radio ID Ranges	19
Radio Search	21
Editing an ID Range.....	23
Deleting an ID Range.....	23
CHAPTER 3 USING SAM	25
USING THE QUARANTINE LIST.....	26
<i>Quarantine List Options</i>	27
New	27
Delete	27
Exempt	28
Selective Inhibit	28
Cancel Selective Inhibit	28
IP Console Inhibit	28
Cancel IP Console Inhibit	28
Radio Check.....	29
Slot Disable.....	29
Add to Hotlist.....	30
History	30
Print.....	32
USING THE HOTLIST	33
<i>Hotlist Options</i>	34
Remove	34

History	34
Print.....	34
USING THE SUSPECT EXEMPTION LIST	35
<i>Suspect Exemption List Options</i>	36
Delete	36
Restore	36
History	36
Print.....	37
CHANGING SAM SETTINGS	38
<i>Overlap Threshold</i>	38
<i>Automatic Inhibit</i>	39
<i>Talkgroup Watch</i>	41
<i>Notification Options</i>	43
<i>Suspect Notifications</i>	44

Goals

This manual describes the role and function of the SAM module in the GW3-TRBO solution.

Who Should Read This Manual?



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

How This Manual Is Organized

This manual is organized as follows:

- **Overview:** Describes the SAM module and provides a brief overview of its function.
- **Setting up SAM:** Describes how to set up SAM Resource ID Ranges and Schedules.
- **Using SAM:** This chapter describes how to use 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.

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

This chapter contains the following sections:

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

What is SAM?

SAM will greatly help the MOTOTRBO owner manage who can and cannot use the MOTOTRBO system. The SAM module accomplishes this by monitoring 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, data call, etc.) is received on a group or radio ID (also known as resources), this activity is validated against the Resource Ranges defined within the SAM GUI. If the activity of the resource violates the expected activity definitions, the resource is added to the **Quarantine List**. Once in the **Quarantine List**, the resource's activity is closely monitored and detailed in the SAM database.

The Halcyon module provides a workflow for radio commands, such as Selective Inhibit, Cancel Selective Inhibit and Radio Check. If you are licensed for the Halcyon module and the *Selective Inhibit*, *Radio Check*, *IP Console Inhibit*, and *Slot Disable* features within Halcyon, you can request these commands on any radio in the **Quarantine List**. Please refer to Halcyon help for more information on the Halcyon module.



To successfully send a command, your input connection must be capable of issuing that command type. See the Trbo or Connect module documentation for more information about sending commands on your connection type.

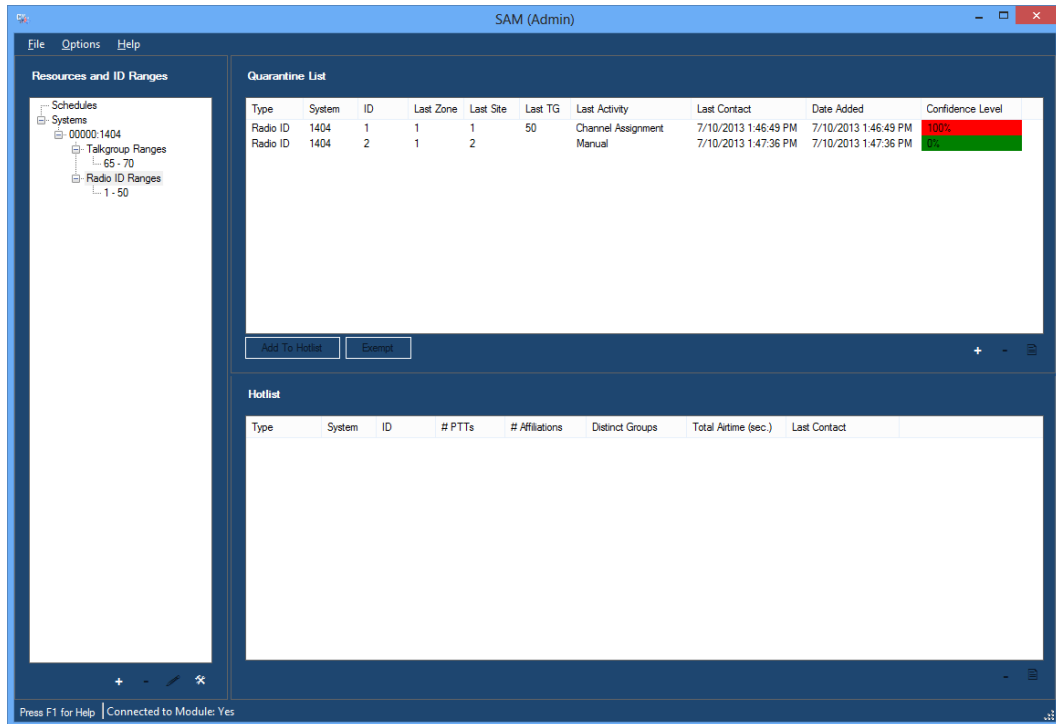


Figure 1.1 – SAM GUI

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 SAM:

- **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 resource range (described in *Chapter 2*). If usage is detected on one of these resources, then SAM adds the resource to the **Quarantine List** with a confidence level of 100%.
- **Usage outside of the predefined schedule of usage:** This rule is applied when you set up a SAM schedule (described in *Chapter 2*) and assign that schedule to a radio ID. If usage is detected outside of the schedule, then SAM adds the radio ID to the **Quarantine 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*). Services are radio features such as private calls, call alerts, etc. 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 SAM adds this radio ID to the **Quarantine 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, then SAM adds the radio ID to the **Quarantine List**. If there is a partial overlap, the confidence level is 75%. If there is a full overlap, the confidence level is 100%.
- **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.



NOTE: SAM will consider Multiple Group Affiliation packets when processing the Rapid Affiliation rule for Capacity Max systems.

This chapter describes how to set up SAM Resource ID Ranges and Schedules.

This chapter contains the following sections:

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

Resources & ID Ranges Tree

The **Resources & ID Ranges** tree contains each Schedule and Resource ID Range that you define within the SAM GUI. The ID ranges are organized by System and even further by Resource ID Range Type (radio ID or group). Using the **Resources & ID Ranges** tree, you can easily add, edit, delete or view Schedules and Resource ID Ranges.

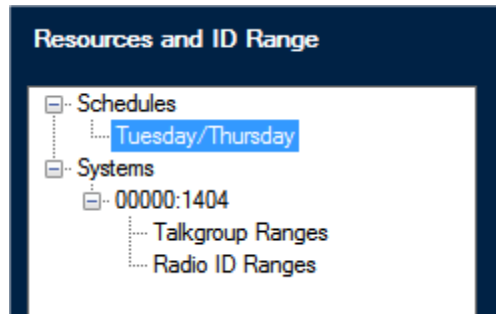



Figure 2.1 – Resource ID Ranges Tree

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

Managing Schedules

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 SAM **Quarantine 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 & 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 show below.

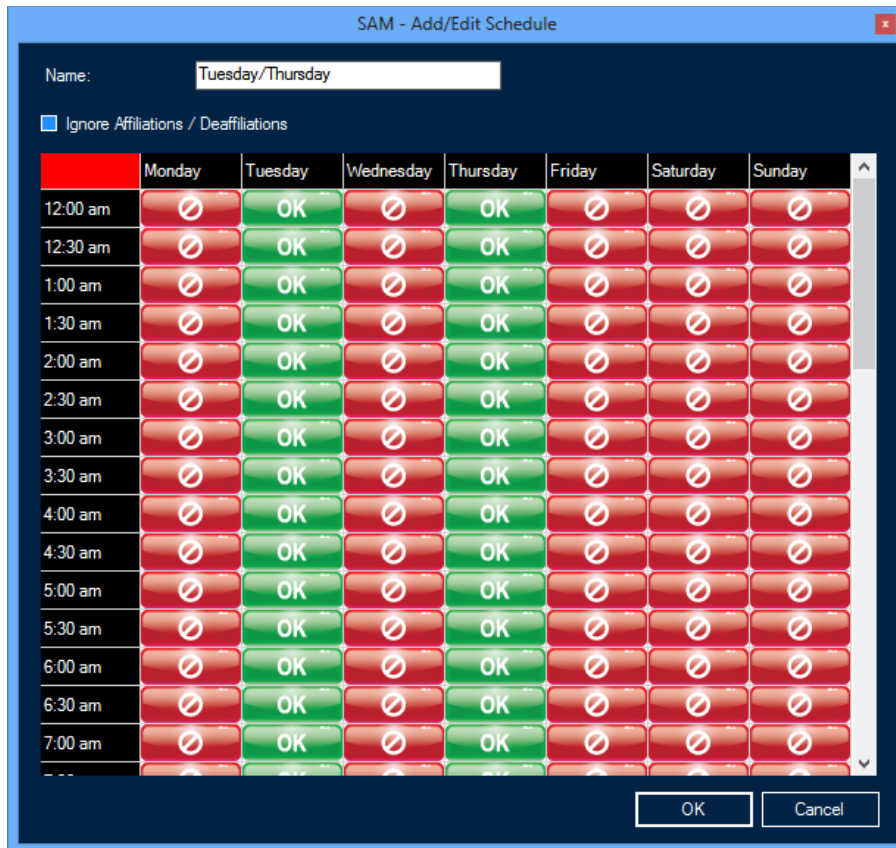


Figure 2.2 – Add/Edit Schedule window

Adding a Schedule

To add a new Schedule, take the following steps:

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



Figure 2.3 – Root Schedules Node

2. Click the **Add** button below the **Resources & ID Ranges** tree (Figure 1.1, item 2), 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/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 Schedules* window and return you to the SAM GUI. Notice that your new Schedule now appears in the **Resources & ID Ranges** tree.

Editing a Schedule

To edit an existing Schedule, take the following steps:

1. In the **Resources & 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, item 4) or right-click on the Schedule in the **Resources & 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 SAM GUI.

Deleting a Schedule

To delete a Schedule, take the following steps:

1. In the **Resources & 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 & 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 & ID Ranges** tree, select the Schedule that you wish to copy.
2. Right-click on the selected Schedule. This will result in a menu of options.
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 & 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 SAM rules. An ID range can be created for group IDs or radio IDs and basically allows the IDs in that range to be allowed or prohibited on the system. Using multiple ranges for both radio and group IDs, activity that utilizes any radio or group on a MOTOTRBO system can be “verified” by SAM.

If, for example a MOTOTRBO Capacity Plus system has talkgroup 1 through 25 and all-call group 255 in use for paying customers, a group ID range could be set up in SAM to monitor activity on all other groups, since they should not be in use. This unallocated group ID range in SAM would then serve to notify you of any radio activity detected on groups 26 through 254.

The group ID range in that example is an exclusive range because the range was defined as unallocated. It serves as a virtual gate through which users of any talkgroup in that range cannot pass through undetected. On the other hand, an inclusive range can be set up and the acceptable activity on the groups in that range limited to a customizable subset of what GW3-TRBO can detect.

These same tactics of guarding a MOTOTRBO system can also be used for setting up ID ranges in order to catch rogue or incorrectly programmed radio IDs. Additionally, even though the example above was for a Capacity Plus system, these principles can be used on an IP Site Connect system as well, keeping in mind the difference in radio and group ID limitations of IP Site Connect.

Resource ID Range Rules

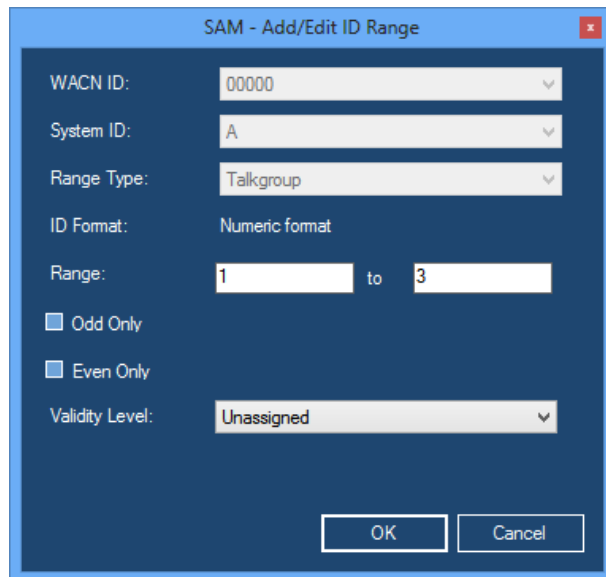
Below is a list of rules regarding Resource ID ranges:

- 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. 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 & ID Ranges** tree, click on the **Talkgroup Ranges** entry that you wish 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 & 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. (Shown in Figure 2.4). The WACN ID, System ID and Type values are provided based on the **Resources & 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. However, these IDs are not assigned to anyone and should not receive activity.
 - **Unallocated:** IDs in this range are not provisioned and should not receive activity.



The screenshot shows a dialog box titled "SAM - Add/Edit ID Range". It contains the following fields and options:

- WACN ID: 00000
- System ID: A
- Range Type: Talkgroup
- ID Format: Numeric format
- Range: 1 to 3
- Odd Only
- Even Only
- Validity Level: Unassigned
- Buttons: OK, Cancel

Figure 2.4 – Add / Edit Talkgroup ID Range


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 SAM GUI. Notice that your new Talkgroup ID Range is now in the **Resources & ID Ranges** tree.

Adding Radio ID Ranges

To add a Radio ID Range, take the following steps:

1. In the **Resources & ID Ranges** tree, click on the **ID Ranges** entry that you wish 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 & 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. (Shown in Figure 2.5 below). The System ID and Type values are provided based on the **Resources & 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.

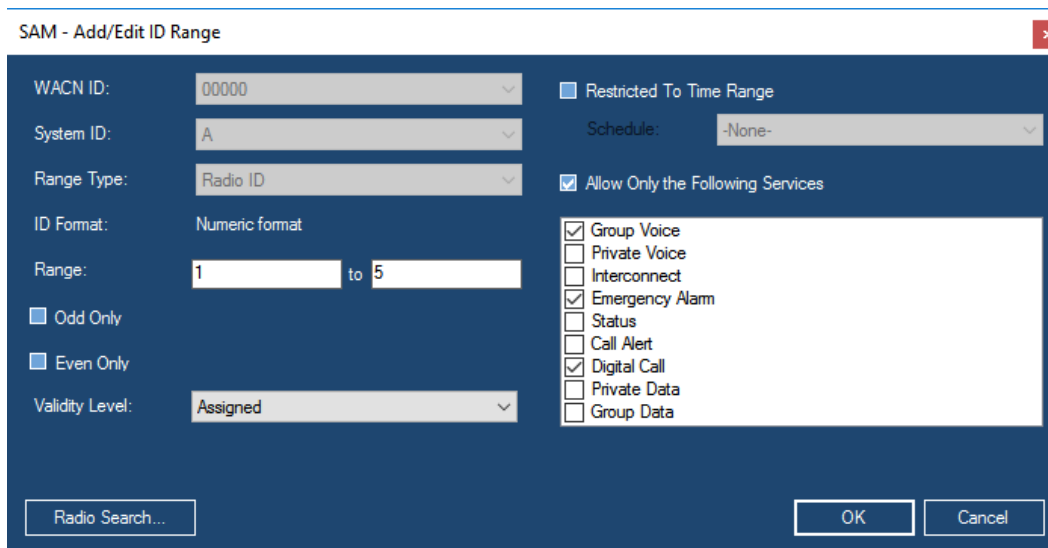


Figure 2.5 – Add / Edit ID Range Window

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. However, these IDs are not assigned to anyone and should not receive activity.
 - **Unallocated:** IDs in this range are not provisioned and should not receive activity.
5. Optionally restrict the ID range to a specific time range by checking the **Restrict 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 only available 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 check box). Select (double-click) the services that the Radio ID Range is expected to use. 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 setup Radio Search on this Radio ID Range, click the **Radio Search...** button. . (See *Radio Search* section below)
 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 SAM GUI. Notice that your new Radio ID Range is now in the **Resources & ID Ranges** tree.


Radio Search


On each Radio ID Range, you can enable the Radio Search option. Radio Search slowly sends a Radio Check command for each radio ID in the Radio ID Range.

From	To	Range Type
1	3	All

Figure 2.6 – Radio Search Options Window

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

 You can monitor the progress of these Radio Search commands via the RC Command window. 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.
- **Zone ID:** Zone 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.

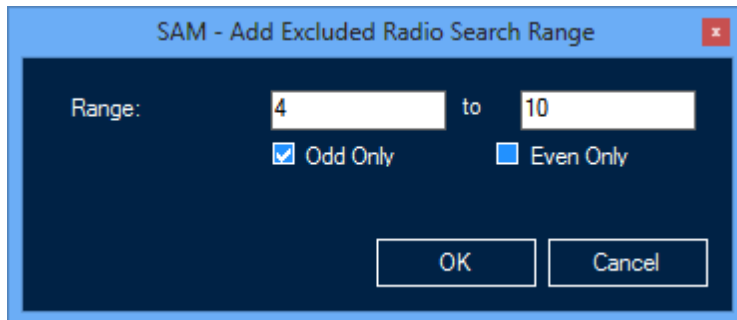


Figure 2.7 – Add Excluded Radio Search Range Window

Editing an ID Range

To edit a Talkgroup or Radio ID Range, take the following steps:

1. In the **Resources & 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 SAM GUI.

Deleting an ID Range

To delete a Talkgroup or Radio ID Range, take the following steps:

1. In the **Resources & 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 & ID Ranges** tree.

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

This chapter contains the following sections:

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



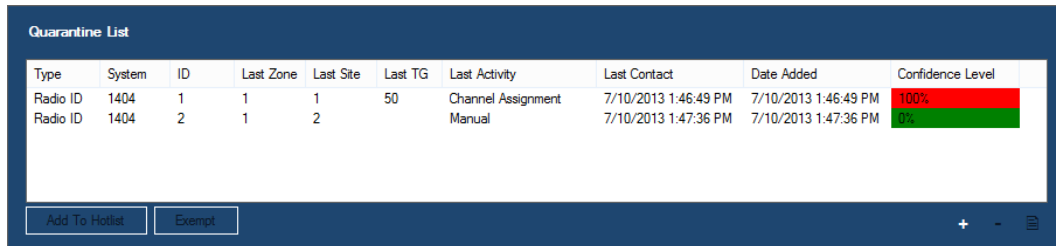
SAM contains many lists, like the one in Figure 3.1 below. Eliminate list columns that you do not wish to see by decreasing the column size to a 0 width. To decrease a column size:

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

Using the Quarantine List

The **Quarantine List** contains each suspect that has been added due to suspicious activity and suspects that you have added manually. The **Quarantine 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 Zone:** The last zone 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 **Quarantine List**.
- **Confidence Level:** Number indicating how sure SAM is that this is a suspect. The higher this number is, the more confident SAM is that this is a suspicious ID.



Type	System	ID	Last Zone	Last Site	Last TG	Last Activity	Last Contact	Date Added	Confidence Level
Radio ID	1404	1	1	1	50	Channel Assignment	7/10/2013 1:46:49 PM	7/10/2013 1:46:49 PM	100%
Radio ID	1404	2	1	2		Manual	7/10/2013 1:47:36 PM	7/10/2013 1:47:36 PM	95%

Figure 3.1 – SAM Quarantine List



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

Quarantine List Options

New

The **New** button allows you to manually add a suspect to the **Quarantine 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, 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 **Quarantine List**. This will load the *Add Suspect* window (shown in figure 3.2, below).

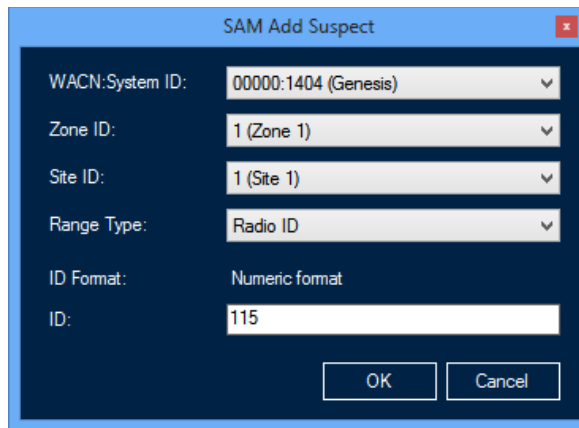


Figure 3.2 – Add Suspect Window

2. Choose the **WACN: System ID**.
3. Choose a **Zone 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 SAM GUI.

Delete

The **Delete** button allows you to delete a suspect from the **Quarantine 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 **Quarantine List**, take the following steps:

1. Select the suspect that you wish to delete from the **Quarantine 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 **Quarantine List** and delete any history related to the suspect.

Exempt

The **Exempt** button allows you to move a suspect from the **Quarantine 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 **Quarantine List**, take the following steps:

1. Select the suspect that you wish to exempt from the **Quarantine 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.

Selective Inhibit

Sends a Selective Inhibit command via Halcyon to the selected radio. This will disable the radio until the Selective Inhibit command is canceled, either in SAM or the RC tool. SAM will receive notification of a simple success or failure. To monitor the progress of the command, load the RC tool and check the *Command Monitor* window.

Cancel Selective Inhibit

Sends a Cancel Selective Inhibit command via Halcyon to the selected radio. This will enable the radio if it is currently inhibited. SAM will receive notification of a simple success or failure. To monitor the progress of the command, load the RC tool and check the *Command Monitor* window.

You will only have access to the Selective Inhibit options if your user’s role has the *SelectiveInhibit* privilege and if you are licensed for *RadioInhibit* under Halcyon.

IP Console Inhibit

Sends an IP Console Inhibit command via Halcyon to the selected radio. This will prevent the radio from transmitting on its current channel until the IP Console Inhibit command is canceled, either in SAM or the RC tool. SAM will receive notification of a simple success or failure. To monitor the progress of the command, load the RC tool and check the *Command Monitor* window.

Cancel IP Console Inhibit

Sends a Cancel IP Console Inhibit command via Halcyon to the selected radio. This will enable the radio if it is currently inhibited. SAM will receive notification

of a simple success or failure. To monitor the progress of the command, load the RC tool and check the *Command Monitor* window.

You will only have access to the IP Console Inhibit options if your user's role has the *IPConsoleInhibit* privilege and if you are licensed for *IPConsoleInhibit* under Halcyon.

Radio Check

Sends a Request Radio Affiliation command via Halcyon to the selected radio. SAM will receive notification of a simple success or failure. To monitor the progress of the command, load the RC tool and check the *Command Monitor* window.

You will only have access to this option if your user's role has the *RadioCheck* privilege and if you are licensed for *RadioCheck* under Halcyon.

Slot Disable

Sends a Slot Disable command via Halcyon to the selected radio. If the radio is keyed up when the command is sent, the repeater slot on which the call is transmitting will disable its over-the-air repeating functions until the radio ends the call. After the radio de-keys, the repeater will re-enable the slot and may attempt to disable the unallocated radio with an IP Console Inhibit. SAM will receive notification of a simple success or failure. To monitor the progress of the command, load the RC tool and check the *Command Monitor* window.

You will only have access to this option if your user's role has the *SlotDisable* privilege and if you are licensed for *SlotDisable* under Halcyon.

Add to Hotlist

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

1. Select the suspect you wish to add to the **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 **Hotlist**.

History

SAM keeps detailed activity information for each radio in the **Quarantine List**. This information is called History. To view the history for a suspect in the **Quarantine 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 (shown below in Figure 3.3).

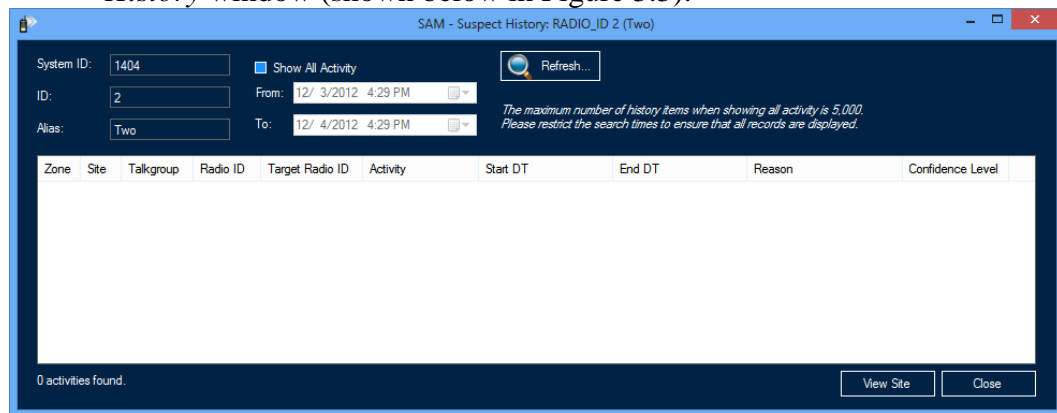


Figure 3.3 – Suspect History Window

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

The *Suspect History* List contains the following columns:

- **Zone:** The zone on which the activity was reported.
- **Site:** The site on which the activity was reported.
- **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 SAM has that this is suspect activity (if a reason is provided).



GW3-TRBO stores the last 30 days of activity as a history for each quarantined radio. The history is purged via the centralized GW3-TRBO purging operation. This length of time can be adjusted with the help of GW3-TRBO support personnel.



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

Print

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

1. Select the activity in the **Quarantine 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 of the activity in the **Quarantine List**, skip this step.
2. Right-click in the **Quarantine List** and choose **Print ...** from the menu. This will show the printer options screen 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.

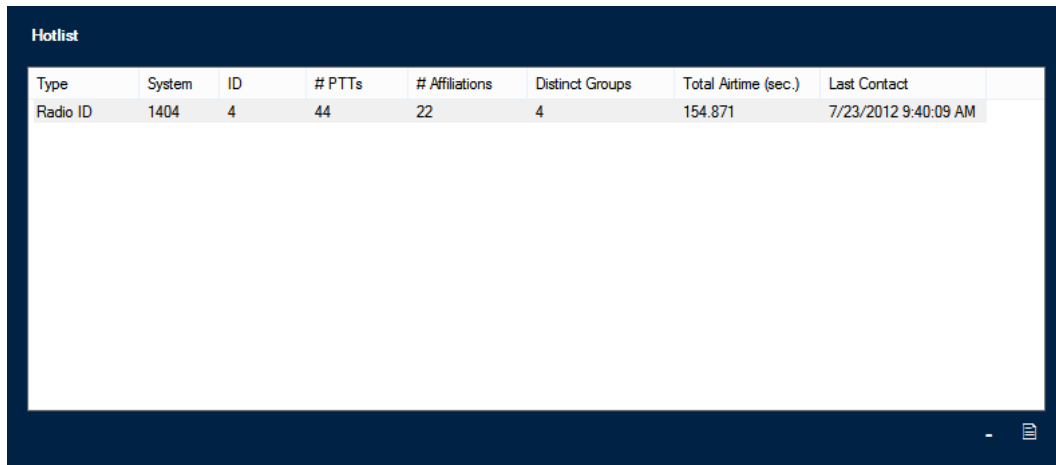


You can also access these options by right clicking an item in the Quarantine List.

Using the Hotlist

The *Hotlist* contains each suspect that has been manually added from the **Quarantine List**. This list holds the suspect resources that we wish to watch more closely. The **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 **Quarantine 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.



Type	System	ID	# PTTs	# Affiliations	Distinct Groups	Total Airtime (sec.)	Last Contact
Radio ID	1404	4	44	22	4	154.871	7/23/2012 9:40:09 AM

Figure 3.4 – SAM Hotlist

Hotlist Options

Remove

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

1. Select the suspect that you wish to remove from the **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 **Hotlist**.



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

History

SAM keeps detailed activity information for each suspect in the **Quarantine List**, and therefore all suspects in the **Hotlist**. This information is called History. To view the history for a suspect in the **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 (shown above in Figure 3.3)
3. Press the **Close** button on the *Suspect History* window to return to the SAM GUI.

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 of the activity in the history list, skip this step.
2. Right-click on the **Hotlist** and choose **Print ...** from the menu. This will show the printer options screen 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 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 Zone:** The last zone 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 SAM is that this is a suspect. The higher this number is, the more confident SAM is that this is a suspicious ID.

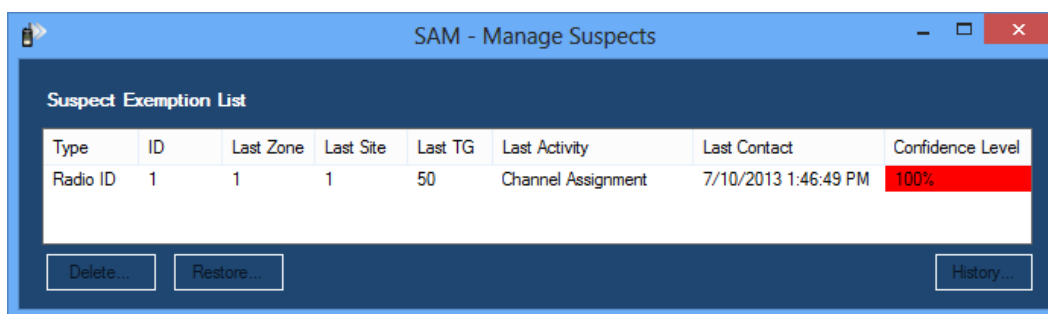


Figure 3.5 – Suspect Exemption List Window



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



When the *exemption list 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 *exemption list 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 **Quarantine List**. To restore a suspect to the **Quarantine List**, take the following steps:

1. Select the suspect that you wish to restore to the **Quarantine 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 **Quarantine 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 (shown in Figure 3.3).
3. Click the **Close** button on the *Suspect History* window to return to the SAM GUI.

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 of 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 screen 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 SAM Settings

The SAM settings allow you to customize the settings for call overlap and automatic inhibits.

Overlap Threshold

This tab contains a single setting which is explained in detail on the screen.

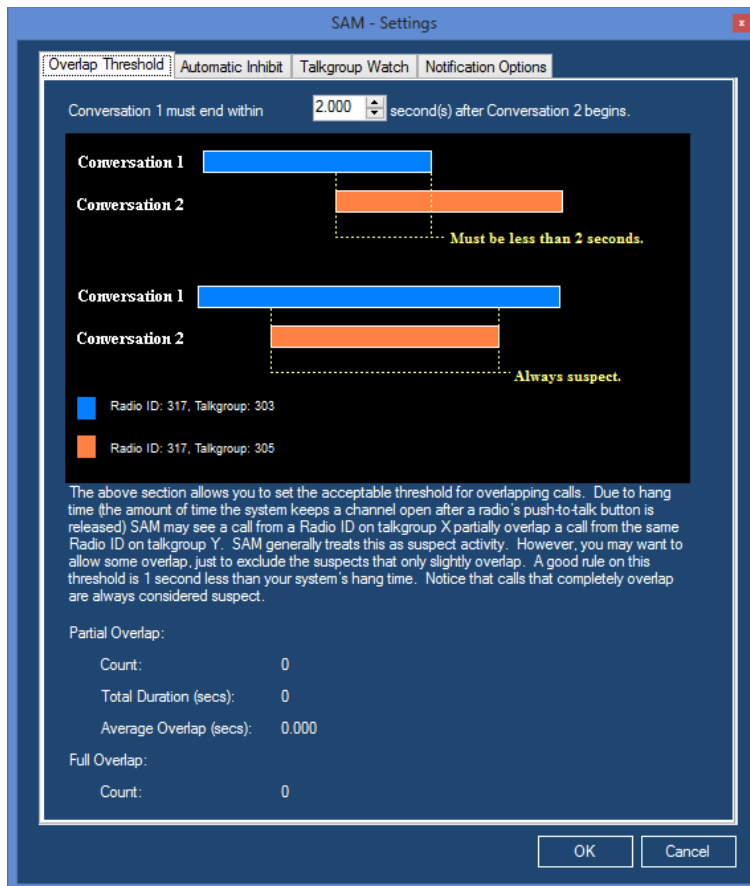


Figure 3.6 – SAM Settings – Overlap Threshold Tab

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

Automatic Inhibit

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 SAM, see Chapter 2.

At the top of this tab is an option to add a radio ID as a suspect if it issues affiliations more rapidly than the specified threshold. 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 75% confidence level suspect. If you do not wish to use this feature, set the **time(s)** value to 99, the highest possible value.

When GW3-TRBO receives activity from a MOTOTRBO system, SAM checks it against all defined ID ranges. If the ID responsible for this activity falls within an unallocated range, SAM will add it to the **Quarantine List**. Lastly, if this checkbox is checked, SAM will immediately issue an inhibit command, targeting the quarantined radio. Subsequently, SAM will issue an inhibit command every time the quarantined radio generates activity, unless an automatic command is already pending to that radio ID. To prevent inhibits from unintentionally being sent repeatedly, after an automatic Selective Inhibit or IP Console Inhibit command is issued, new activity within 60 seconds will not trigger a new command.

You may choose between the *Selective Inhibit*, *IP Console Inhibit* and *Slot Disable* commands to automatically disable suspect radios.

- *Selective Inhibits* may be disabled in a radio's programming. If a radio is programmed to ignore inhibits, this command will not disable the radio.
- *IP Console Inhibits*, which prevent the targeted radios from keying up on specific channels, were introduced in the R1.7 MOTOTRBO firmware. Radios using an earlier version of the firmware will not be affected by IP Console Inhibits.
- *Slot Disables* were introduced in the R1.7 MOTOTRBO repeater firmware. A Slot Disable will silence the repeater slot for the duration of every call by an unallocated suspect, preventing any radio from using that slot. Great care should be taken when using this feature, because SAM will potentially interrupt all calls from radios on an unallocated range.

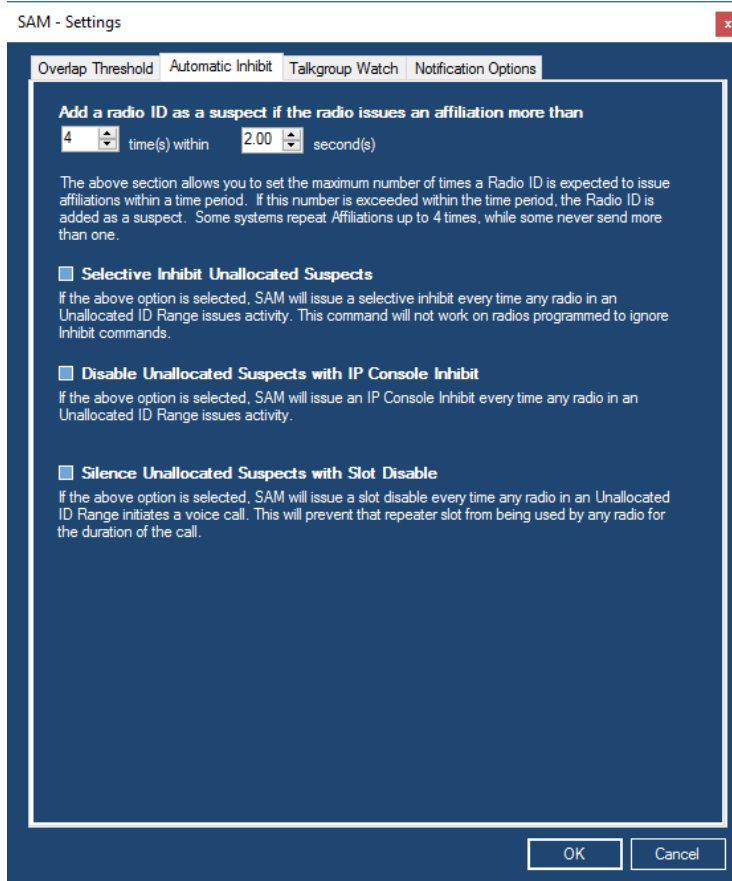



Figure 3.7 – SAM Settings – Automatic Inhibit Tab

 Each of these options is licensed separately, and will only show up if licensed for *SelectiveInhibit*, *IPConsoleInhibit* or *SlotDisable*.

Talkgroup Watch

When you set up a talkgroup range in 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 **Quarantine List**, you will also want to add any radio using that talkgroup to the **Quarantine List**. Checking the box labeled **Add radio IDs on suspect talkgroups to Quarantine List** will automatically add radio IDs to the quarantine 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.

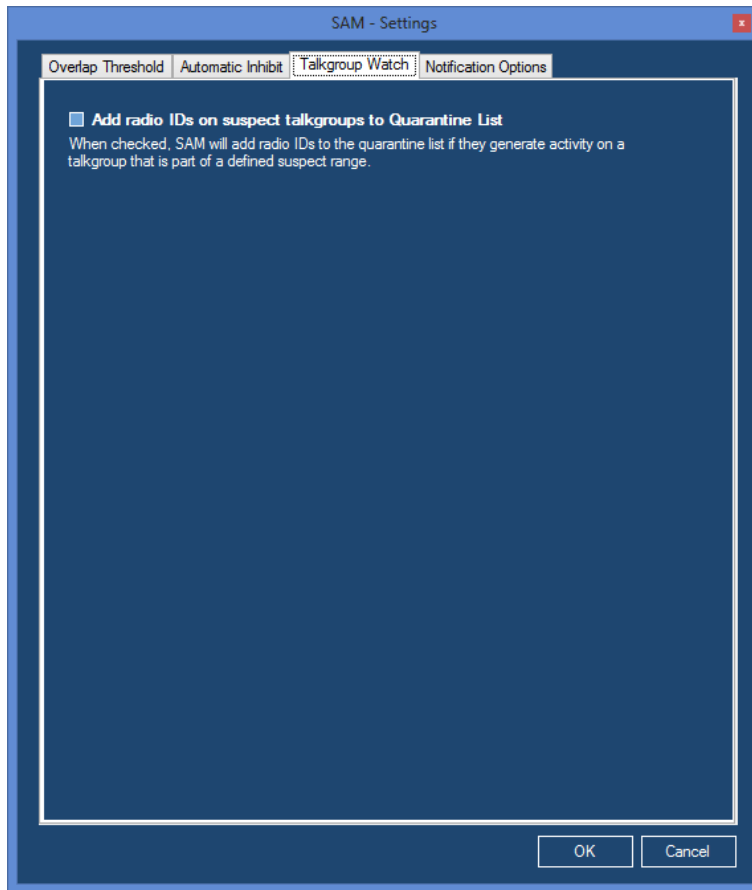


Figure 3.8 – SAM Settings – Talkgroup Watch Tab

Notification Options

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

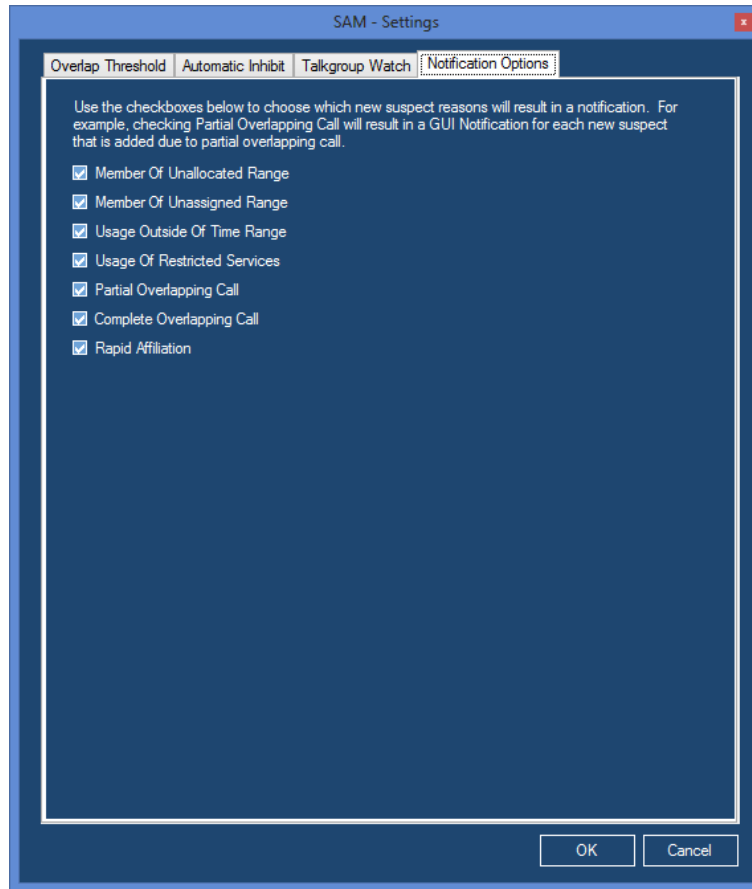


Figure 3.9 – SAM Settings – Notification Options Tab

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

Suspect Notifications

When SAM adds a new suspect to the **Quarantine List**, it also sends out a GW3-TRBO GUI Notification. These are the same notifications discussed in *Chapter 10: GW3-TRBO Notifications* of the *GW3-TRBO Core Manual*.

For each new suspect, the Alerts module shows a GW3-TRBO 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 GW3-TRBO users with the Security Administrator privilege.

The GW3-TRBO 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 GW3-TRBO (by default *C:\Program Files\Genesis\GenWatch3*). GW3-TRBO 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 GW3-TRBO 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 GW3-TRBO 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*.