

# **GTA Reporting Suite VERSION 1.1**

## **Product Guide**

## **Copyright**

© 1996-2004, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

## **GTA Reporting Suite Product Guide**

**May 2004**

### **Technical Support**

GTA includes 30 days "up and running" installation support from the date of purchase. See GTA's website for more information. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local GTA authorized channel partner.

**Tel:** +1.407.482.6925    **Email:** [support@gta.com](mailto:support@gta.com)

### **Disclaimer**

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

### **Trademarks & Copyrights**

GNAT Box and Surf Sentinel are registered trademarks of Global Technology Associates, Incorporated. RoBoX, GB-Commander and GB-Ware are trademarks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. WELF and WebTrends are trademarks of NetIQ. Sun, Sun Microsystems and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. The Java product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>. SurfControl is a registered trademark of SurfControl plc.

All other products are trademarks of their respective companies.

## **Global Technology Associates, Inc.**

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: <http://www.gta.com> • Email: [info@gta.com](mailto:info@gta.com)

**Lead Development Team:** Larry Baird, Richard Briley, Jim Silas, Brad Plank, Chris Williamson.

**Technical Consulting:** David Brooks. **Documentation:** Mary Swanson.

# Contents

<b>1 INTRODUCTION</b>	<b>1</b>
<b>About GTA Reporting Suite</b>	<b>1</b>
Features	1
Requirements	1
GTAsyslog Requirements	1
<b>Registration and Activation</b>	<b>2</b>
Licensing and Activation	2
<b>Installation Support</b>	<b>2</b>
Support Options	2
<b>Documentation</b>	<b>3</b>
Additional Documentation	3
<b>2 INSTALLATION</b>	<b>5</b>
<b>Database Selection</b>	<b>5</b>
<b>Network Configuration</b>	<b>5</b>
Database Layout	6
Default Installation	7
Private Service Network (PSN) Server	7
<b>Preinstallation</b>	<b>8</b>
Database Setup	8
ODBC Driver	8
DSNs (Data Sources)	8
<b>Installation</b>	<b>9</b>
Download Installer	9
GTAsyslog Installation	10
Database Conversion	11
Activation	11
Activation Information	12
Manual Activation	12
<b>Remote Logging on a GTA Firewall</b>	<b>13</b>
<b>Uninstall</b>	<b>14</b>
<b>3 USING REPORTS &amp; CHARTS</b>	<b>15</b>
<b>Overview</b>	<b>15</b>
File	15
Reports	15
Window	15
Help	15
<b>Select Firewall Group Parameters</b>	<b>16</b>
<b>Export</b>	<b>17</b>
<b>Print</b>	<b>17</b>
<b>Charts &amp; Reports</b>	<b>17</b>
Query Parameters	17
IP Address	18
Date/Time Range	18
<b>Charts</b>	<b>18</b>
Change Chart Title	19
Choose Different Chart Type (Chart Parameters)	19

---

Display Report Text .....	20
Charts, Reports .....	20
<b>Reports .....</b>	<b>21</b>
Change Report Title .....	21
Chart Current Report .....	21
Editing Functions .....	21
Charts, Reports .....	21
<b>4 STANDARD CHARTS &amp; REPORTS .....</b>	<b>23</b>
<b>Overview .....</b>	<b>23</b>
<b>Standard Charts .....</b>	<b>23</b>
Usage Summary .....	23
Firewall Filter Blocks .....	24
Internet Access Management .....	25
User Name .....	26
<b>Standard Reports .....</b>	<b>27</b>
Usage Summary .....	27
Firewall Filter Blocks .....	28
Internet Access Management .....	29
<b>5 DATABASE MANAGEMENT .....</b>	<b>31</b>
<b>Overview .....</b>	<b>31</b>
<b>DBmanager .....</b>	<b>31</b>
Database .....	32
Back Up and Restore Data .....	32
Purge and Restore Data .....	32
Convert to New Format .....	33
Reinitialize .....	33
Repair .....	33
Unlock .....	33
Utilities .....	34
GTAsyslog Utility Configuration .....	34
Circular File .....	34
Licensed Firewalls .....	35
Import Logs Utility .....	36
Help .....	36
Verify Installation .....	36
<b>Creating DSNs .....</b>	<b>38</b>
MySQL DSNs .....	38
PostgreSQL DSNs .....	39
Microsoft SQL Server DSNs .....	40
<b>6 TROUBLESHOOTING .....</b>	<b>43</b>
<b>Q&amp;A .....</b>	<b>43</b>
<b>INDEX .....</b>	<b>45</b>

# 1 Introduction

---

## About GTA Reporting Suite

GTA Reporting Suite utilizes the information contained in GTA Firewall logs to provide clear, concise, top-level reports and enable administrators to manage network usage. This easy-to-use tool can be used to generate intuitive reports from log data that has been parsed by the GTAsyslog server and sent to a supported ODBC-compliant database.\* A modified version of GTA Reporting Suite also functions as part of the GB-Commander application.

### Features

- Historical reports.
- Intuitive and easy-to-use.
- Supports ODBC-compliant databases, including the provided Microsoft SQL Server Desktop Engine (:) for small-scale use.
- Uses GTAsyslog and GTA's DBmanager utility to manage the database and import logs.
- Usage Summary, Filter Blocks and Internet Access Reports.

### Requirements

- Windows 2000 (SP 4)[, Windows XP (SP 1), or Windows 2003 Server.
- DSNs for ODBC-compliant database and driver.\*
- 500 MHz Pentium III (minimum),
- 256 MB RAM (minimum).
- GTAsyslog server must be installed as service and running locally or remotely. See GTAsyslog Requirements, below.

### GTAsyslog Requirements

- Windows 2000 (SP 4), Windows XP (SP 1), or Windows 2003 Server.
- Supported ODBC-compliant database and associated driver.\*
- Firewalls using GNAT Box System Software version 3.4 or higher.

\* See [www.gta.com](http://www.gta.com) for the most current listing of supported database products.

## Registration and Activation

Make sure to register your GTA Reporting Suite product. You can do this at GTA's online support center: <http://www.gta.com/support/logon.php>.

### Licensing and Activation

GTA Reporting Suite activation requires a serial number and verification code located on product packaging and available from your account home page in the GTA Support Center after product registration.

After installing GTA Reporting Suite from the Installation CD, you will be prompted to install GTAsyslog and license the product. Once GTAsyslog is installed, DBmanager will open and the license screen will appear.

Click **RETRIEVE ACTIVATION CODE**. In the Activation Information form, enter the serial number, verification code and other information, then submit the form to GTA Support. Once GTA licensing responds with an activation code, the **ACTIVATION CODE** field will populate automatically. Click **APPLY ACTIVATION CODE** to activate GTA Reporting Suite.

To activate GTA Reporting Suite when installing GTAsyslog separately (as when using the download installer or installing GTAsyslog alone), and for more detailed activation instructions, see page 13.

---

## Installation Support

Installation ("up and running") support is available to registered users. See GTA's website for more information. If you need installation assistance during the first 30 days after purchase, register your product and then contact the GTA Support team by email at [support@gta.com](mailto:support@gta.com). Include your product name and serial number.

Installation support covers only the aspects of configuration related to installation and default setup of GTA Reporting Suite and does not include installation or set-up of ODBC databases. For further assistance, contact GTA Sales staff for information about support offerings.

### Support Options

If you need support for GTA products, a variety of support contracts are available. Contact GTA Sales staff for more information. Contracts range from support by the incident, to full coverage for a year. Other assistance is available through the GNAT Box Mailing List or through an authorized GTA Channel Partner.

---

## Documentation

This guide demonstrates how to install, set up and use the GTA Reporting Suite, a program designed to create reports, charts and graphs. A few conventions are used in this guide to help you recognize specific elements of the text.

---

### Documentation Conventions

---

SMALL CAPS	FIELD NAMES IN BODY TEXT.
BOLD SMALL CAPS	NAMES OF PUBLICATIONS.
<b>Bold</b>	<b>Chapters.</b>
<b><i>Bold Italics</i></b>	<b><i>Emphasis.</i></b>
Courier	Screen text.
<b>ALL CAPS</b>	<b>ON SCREEN BUTTONS.</b>
<b>&lt;BRACKETS&gt;</b>	<b>WITH ALL CAPS, KEYBOARD BUTTONS.</b>
<b>Condensed Bold</b>	<b>Menus, menu items, menu selections.</b>
<b>Slash "/"</b>	<b>In menu items, indicates menu structure.</b>

---

### Additional Documentation

For instructions on installation, registration and setup of a GTA Firewall, see your GTA Firewall's product guide; for optional features, see the appropriate Feature Guide. User's Guides, Product Guides and Feature Guides are delivered with new GTA products; these manuals and other documentation for registered products can also be found on the GTA website, [www.gta.com](http://www.gta.com).

Documents on the website are either in plain text (\*.txt) or Portable Document Format (PDF) which requires Adobe Acrobat Reader version 5.0. A free copy of the reader can be obtained at [www.adobe.com](http://www.adobe.com). Documents received from GTA Support may also be in email or Microsoft Word format (\*.doc).

---

## Documentation Map

---

### Products and Options

GNAT Box System Software .....	GNAT Box System Software User's Guide
GTA Firewall Installation.....	Product Guides
GB-Commander for Firewalls.....	GB-Commander Product Guide
Reporting.....	GTA Reporting Suite Product Guide
Content Filtering .....	Surf Sentinel Content Filtering Feature Guide
High Availability .....	H <sub>2</sub> A High Availability Feature Guide
Virtual Private Networking .....	GNAT Box VPN Feature Guide
VPN Examples .....	GNAT Box VPN to VPN Tech Docs

### Utilities & Information

Logging Utilities .....	GNAT Box System Software User's Guide & Addendum
Troubleshooting .....	Product and Feature Guides
Ports & Services.....	Product CDs
Drivers & NICs .....	www.gta.com
Frequently Asked Questions .....	FAQs on www.gta.com
Web Interface, GBAAdmin.....	GNAT Box System Software User's Guide
Console interface .....	Console Interface User's Guide

---

### Note

Only initial product purchases are eligible to receive free printed manuals. Upgrade products include PDF documentation. Check our website for the latest documentation.



## 2 Installation

### Database Selection

GTA recommends using the supplied MSDE database only for evaluation or for small networks with low logging activity. The MSDE installation creates the database, as well as the required GTA Firewall DSNs. For more information about MSDE, see <http://www.microsoft.com/sql/msde/>.

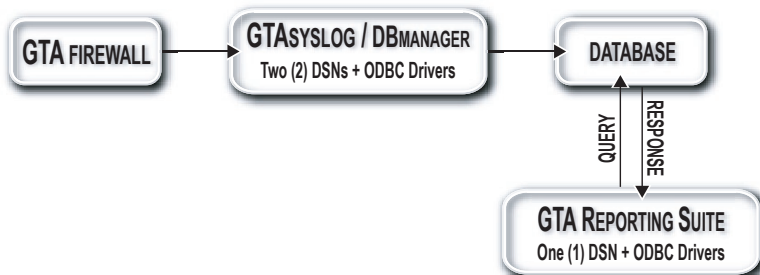
For larger networks and for use with high logging activity, install one of GTA's other supported databases.

#### Note

For the most recent list of GTA's supported ODBC-compliant databases, see [www.gta.com](http://www.gta.com).

### Network Configuration

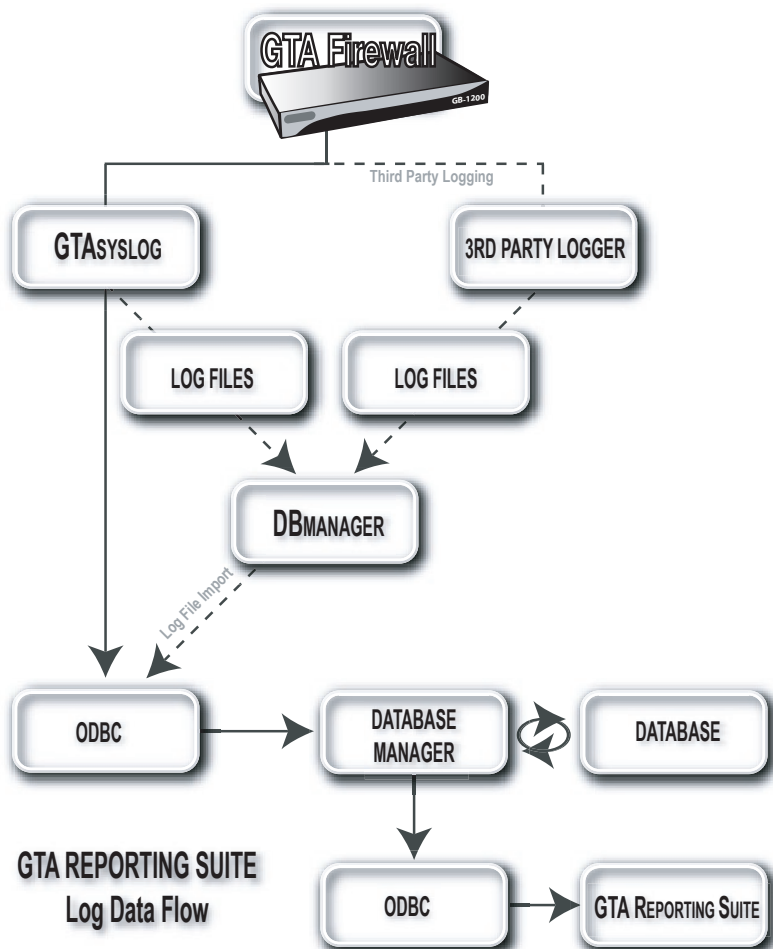
The diagram below illustrates GTA Reporting Suites's basic data flow. A firewall sends logs to GTAsyslog, which parses the data and sends it to the database. GTA Reporting Suite can then query the database and build charts and reports based on the data.



*Data Flow*

## Database Layout

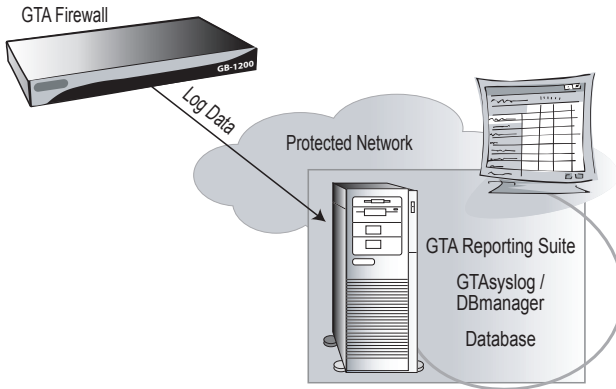
Log file data flows through the GTA Firewall and GTA Reporting Suite system to create a versatile database setup. The database can be placed separately, either on a different machine or a different network; multiple copies of GTA Reporting Suite can monitor the same data. In addition, using GTA Reporting Suite with a multiple license, any number of firewalls can be monitored, even over a distributed network.



*GTA Reporting Suite Log Data Flow*

## Default Installation

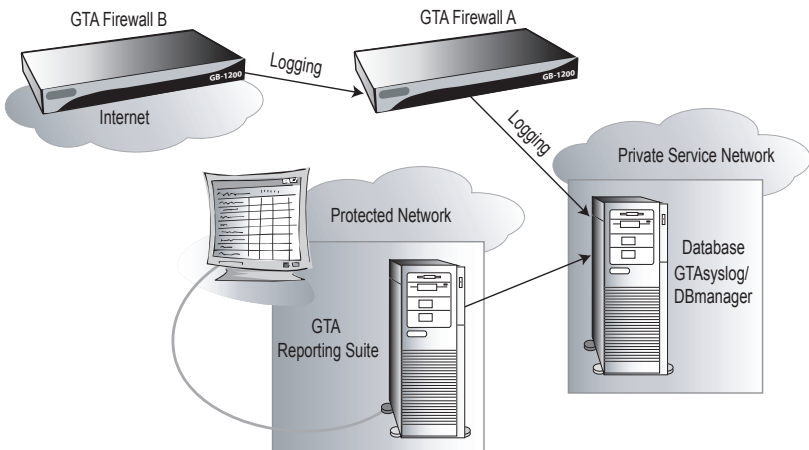
GTA Reporting Suite can monitor data on a network in a variety of configurations. The single-system database/network installation illustrated below simplifies installation.



*Single System Installation*

## Private Service Network (PSN) Server

In another common layout, typically used when multiple firewalls will be logging to GTAsyslog, the database server is housed on the PSN, with GTA Reporting Suite installed on the Protected Network. This places the database on a secure, isolated network. In the illustration below, Inbound tunnels will need to be added to GTA Firewall A to allow access through the External Network interface on UDP port 514 for GTA Firewall B.



*Database on PSN*

## Preinstallation

For installing the supplied MSDE database, skip these preliminary database steps and go to the Installation section on page 9. Use the steps below for installing one of GTA's other supported ODBC-compliant databases. Explanations of the steps follow.

1. Download your preferred database package and ODBC driver.
2. Install and configure the database on a server machine according to the instructions provided with the database package.
3. Install the ODBC driver on machines where GTAsyslog and/or GTA Reporting Suite will be installed.
4. Create two (2) DSNs, `GTA Firewall` and `GTA Firewall Admin`, on the machine where GTAsyslog will be installed.
5. Create one (1) DSN, `GTA Firewall`, on any machine where GTA Reporting Suite will be installed without GTAsyslog.
6. Insert the Installation CD or download GTA Reporting Suite. A license is required to download and activate GTA Reporting Suite.

## Database Setup

Select and install one of the supported ODBC-compliant databases. The database can be installed anywhere on the network accessible to GTA Reporting Suite and GTAsyslog; if GTAsyslog or GTA Reporting Suite are set up on a remote machine, the database server must be configured to accept connections from that location. Supported databases are noted in the Creating DSNs section of Chapter 5 – Database Management; for the most up-to-date list of supported databases, go to [www.gta.com](http://www.gta.com).

## ODBC Driver

The database will require an associated ODBC driver on the GTAsyslog and GTA Reporting Suite machines. Follow the driver installation instructions for your selected database.

## DSNs (Data Sources)

After installing the database and the ODBC driver, create the two DSNs required for communication between GTAsyslog, GTA Reporting Suite, and the database. GTA Reporting Suite requires the `GTA Firewall` DSN to communicate with the database server. GTAsyslog requires both the `GTA Firewall` DSN and a `GTA Firewall Admin` DSN to communicate with GTA Reporting Suite and the database server. See Chapter 5 – Database Management for help creating the required DSNs for your preferred database.

---

## Installation

GTA Reporting Suite may be installed in multiple locations, including the server machine on which GTAsyslog is installed; only one installation of GTAsyslog can be used with GTA Reporting Suite. If installing from the Installation CD, the wizard should start automatically; if not, locate and run the GTA Reporting Suite installer. The GTA Reporting Suite CD installer includes these steps:

1. Read the license agreement; if you accept the terms, click **YES**.
2. Select an installation destination. (**C:\Program Files\GTA**)
3. Choose the typical (default) setup to install Documentation, GTA Reporting Suite, System Files and Help.
4. Review installation, then allow the installer to continue.
5. Select whether to install program icons, install GTAsyslog and its associated utilities, request a product license or view product notes.
6. The license screen will appear; activate GTA Reporting Suite by entering your serial number and verification code. If the license screen does not appear automatically, open DBmanager after installation, then go to Activation Code under the Utilities tab.
7. Allow installation of GTAsyslog and GTA Reporting Suite to complete. (See GTAsyslog installation, below.)
8. Configure remote logging on the GTA Firewalls.

## Download Installer

If downloading the installer from GTA's website, first install GTAsyslog, using the instructions in the GTAsyslog Installation section, below, then follow these GTA Reporting Suite download installer instructions:

1. Read the license agreement; if you accept the terms, click **YES**.
2. Select an installation destination. (**C:\Program Files\GTA**)
3. Choose the typical (default) setup to install Documentation, GTA Reporting Suite, System Files and Help.
4. Review, then allow installation to complete.
5. To activate, open DBmanager, then go to Activation Code under the Utilities tab. Enter your serial number and verification code.
6. Configure remote logging on the GTA Firewalls.

## GTAsyslog Installation

GTAsyslog is required to activate GTA Reporting Suite and must be running as a service before GTA Reporting Suite can access the database. Only one GTAsyslog can be used with GTA Reporting Suite.

When using the Installation CD, you will be prompted to install GTAsyslog after completing the GTA Reporting Suite installation process.

When downloading software from GTA's website or using the separate GTAsyslog installer on the Installation CD, GTA recommends downloading and installing GTAsyslog first.

GTAsyslog is configured through the DBmanager interface; DBmanager and LogView are installed with GTAsyslog. See installation notes at the prompt for installation information about all three utilities.

### **Note**

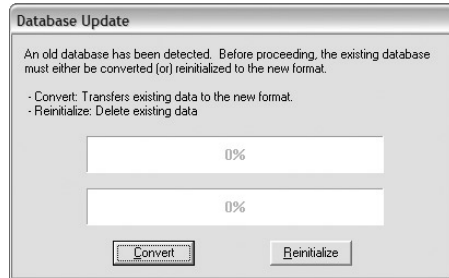
LogView 1.0 requires Java runtime environment (JRE) 1.4 or higher. Go to [www.java.com](http://www.java.com) to download Sun's latest JRE or install the Java version available on the Installation CD.

If you would like to change GTAsyslog's configuration or substitute other firewalls for those that are added automatically, see the GTAsyslog configuration section in Chapter 5 – Database Management.

1. Read the license agreement; if you accept the terms, click **YES**.
2. Select an installation destination for the utilities (**C:\Program Files\GTA**) and for the log files. (**C:\Program Files\GTA\GTAsyslog\Logs**)
3. Choose the typical (default) setup to install the utilities – GTAsyslog, DBmanager, LogView and Documentation.
4. Review installation, then allow the installer to continue.
5. In the Select Service Owner window, enter the user name and password for an administrator-level local account. The account will be set up if it does not already exist. (GTAsyslog will be run in the context of the Service Owner user identity. For instructions on changing GTAsyslog's identity, see Chapter 6 – Troubleshooting.)
6. Select whether to install MSDE (Microsoft SQL Server Desktop Engine) as your database. (The MSDE installer is also available separately on the Installation CD.)
7. If you have a previously installed database, the installer will prompt to convert it.
8. Select whether to install program icons and the Java Runtime Environment (JRE).
9. Complete the installation of the JRE, if selected, and GTAsyslog.

## Database Conversion

If a database already exists on your system, and the GTAsyslog installation detects it, a database conversion dialog will appear. These functions can also be performed from the Database menu in DBmanager.



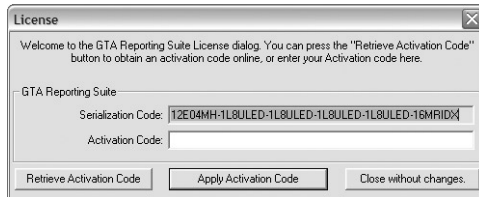
*Database Conversion Dialog*

## Activation

GTA Reporting Suite activation requires a serial number and verification code located on product packaging and available from your account home page in the GTA Support Center after product registration.

A license screen will appear automatically when GTAsyslog is installed with GTA Reporting Suite from the Installation CD; to open the license screen and activate the program when GTAsyslog is installed separately, open DBmanager and go to Activation Code under the Utilities tab.

After installing GTA Reporting Suite from the Installation CD, you will be prompted to install GTAsyslog and license your product. Once GTAsyslog is installed, DBmanager will open and the license screen will appear. Click **RETRIEVE ACTIVATION CODE**. The Activation Information form will appear.



*License Screen*

## Activation Information

Enter the serial number and verification code in the appropriate fields. Next, enter contact information for the program owner in the **OWNER** fields; fill out the **SYSTEM ADMINISTRATION** contact fields if this information is different, or click **COPY FROM OWNER** to apply the Owner information to these fields. Print the form for your records.

### *Activation Form*

Click **RETRIEVE ACTIVATION CODE**. Once GTA licensing responds with an activation code, the license screen will reappear, and the **ACTIVATION CODE** field will populate automatically. Click **APPLY ACTIVATION CODE** to license GTA Reporting Suite.

## Manual Activation

If you do not have Internet access from the GTA Reporting Suite workstation, send the Activation Information page to GTA Technical Support by fax to 1(407) 380-6080 or by mail to 3505 Lake Lynda Drive, Suite 109, Orlando, Florida, 32817, Attention: Technical Support - GTA Reporting Suite Activation. When you receive the activation code, enter the number in the **ACTIVATION CODE** field and click **APPLY ACTIVATION CODE** to license GTA Reporting Suite. Activation code entry is *not* case-sensitive.

## **Caution**

Entering an invalid activation code will un-license your product. See Chapter 6 – Troubleshooting if your product becomes unlicensed.



# Remote Logging on a GTA Firewall

To receive log data automatically for GTA Reporting Suite, remote logging must be enabled on the GTA Firewall and configured in GTAsyslog. GTAsyslog’s default configuration should be sufficient for most uses; see Chapter 5 – Database Maintenance for configuration instructions. For more information about configuring remote logging on GTA Firewalls, see the **GNAT BOX SYSTEM SOFTWARE USER’S GUIDE**.

The Remote Logging section on the GTA Firewall (under the Services menu) provides a means to configure how log information on the GTA Firewall is stored and where it is sent. To enable Remote Logging on a firewall, select the source IP address object from the BINDING INTERFACE dropdown list, then enter the server IP address/port number in the SYSLOG SERVER field .

## Remote Logging Fields

Enable	Enable remote logging. Disabled by default.
Binding interface	Address from which logging is sourced, “Auto” by default.
Syslog server	IP address or host name of a system that will accept the remote logging data (GTAsyslog). The port is 514 by default. To enter a different port number, use the standard format, e.g., 192.168.71.2:514 or example.gta.com:514.

## Facilities

Filter Facility	Logs information associated with any filter that has logging enabled. Any attempts at unauthorized access will be logged to the Filter Facility log stream.
NAT Facility	Logs information associated with Network Address Translation: essentially, outbound packets.
WWW Facility	Logs all URLs accessed through the GTA Firewall.

For more information about the syslog protocol, see RFC 3164.

GNAT-Box Remote Logging

Enable: ☐

Binding interface: <AUTO>

Syslog server: 192.168.101.2:514

Facilities

Filter facility: local1

NAT facility: local0

WWW facility: local2

Default Save Reset

## Remote Logging

## Uninstall

Select the installer used to install GTA Reporting Suite and follow the removal instructions given by the installation wizard.

Optionally:

1. Go to **Start/Settings/Control Panel/Add/Remove Programs** and select GTA Reporting Suite.
2. Select **Change/Add/Remove Programs** and follow the removal instructions.

## 3 Using Reports & Charts

---

### Overview

The GTA Reporting Suite main window will display four main dropdown menus—**File**, **Reports**, **Window** and **Help**.

#### **Note**

On first opening GTA Reporting Suite, a welcome message will appear with brief instructions for using the application. Click the “Don’t show this message in the future” checkbox, if desired.

GTA Reporting Suite is consistent with a standard Windows interface, providing column sorting, column sizing and right-click menus. The main menu contains general options available throughout the application. Select options are also available using dropdown menus (at the top of each window) and right-click menus.

### File

The **File** menu contains the functions **Select Firewall Routers**; **Export**; **Print...**; and **Exit**. The Exit command closes the application.

### Reports

The type and content of reports and charts is selected using the items under the **Reports** menu. Each report or chart run creates a new window, up to nine concurrent windows. The active window is indicated by a colored title bar and a check mark next to the item in the menu.

### Window

The **Window** menu on the main menubar allows the administrator to arrange the current display windows in Vertical, Horizontal, Tile or Cascade format. Use **Refresh** to renew the contents of the current windows.

### Help

Find the version number and date of last build in the **Help/About** dialog. To utilize online help for GTA Reporting Suite, see the **Help/Using GTA Reporting Suite** item.

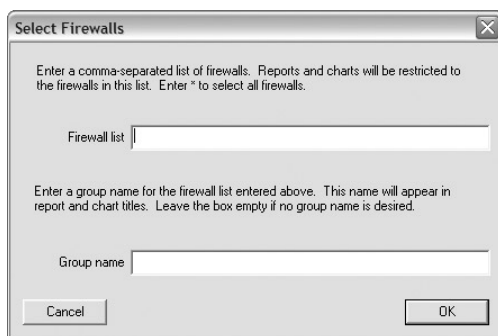
## Select Firewall Group Parameters

**Select Firewall Routers** under the **File** menu allows the administrator to select and name the firewall group for which to run successive reports.

If you would like to select a specific group of firewalls and/or name the firewall group in successive charts and reports, choose **Select Firewall Routers** before running a chart or report. All monitored firewalls are chosen by default.

In the Firewall Group Parameters dialog that appears, enter the serial number of each firewall desired in a comma-separated format, e.g., 1234 5678,23456789,34567890 in the FIREWALL LIST field. Choose all monitored firewalls using the asterisk "\*" wildcard symbol. Choose a series of firewall serial numbers using the asterisk "\*" wildcard symbol, e.g., 1234567\*, to select 12345678, 9, 10, 11 and 12. In the GROUP NAME field, enter a name for the selected firewalls to appear in successive charts and reports.

The firewall group is selected until **Select Firewall Routers** is chosen again, and either the firewall list or group name is changed.



Select Firewalls

Enter a comma-separated list of firewalls. Reports and charts will be restricted to the firewalls in this list. Enter \* to select all firewalls.

Firewall list

Enter a group name for the firewall list entered above. This name will appear in report and chart titles. Leave the box empty if no group name is desired.

Group name

Cancel OK

*Firewall Group Parameters*

## Export

Export to a file format by selecting **File/Export** from the main menu or the window menu. Note that only the currently selected report or chart exports to a file. Choose one of the file output formats below:

---

### Export File Formats

---

CSV	Comma-separated variable. View the fields in CSV format using a spreadsheet program.
DOC	Tab-separated fields. A text editor or word processor that can set tab stops can view the DOC format.
TXT	Plain text file. TXT format requires a fixed-pitch character font to display correctly.
HTML	Basic markup language for web pages. Use a web browser to view HTML as a formatted page.
JPG	Chart Only. Compressed graphic file. Ideal for use in presentations and PDF documents.

---

## Print

Print the highlighted chart or report by selecting **Print** from the report window or main menu. Most charts and many reports are designed to display and print in landscape mode. Only the currently selected window will print. You can also select print from window menus and right-click menus.

---

## Charts & Reports

Open window menus in charts and reports by clicking the **Report** or **Chart** icon on the left side of the title bar or by right-clicking the window and selecting from the right-click menu. Chart and report window menus display options available for the type of report or chart.



*Chart Icon*



*Report Icon*

## Query Parameters

After choosing and naming the Firewall Group (or using the defaults), select a chart or report to run. The Query Parameters dialog will appear. Query Parameters will vary by the type of chart or report run.

Select the desired range of information by completing the Date/Time and/or IP address fields required to run the query. Click **OK**.

*Query Parameters Example*

## IP Address

If prompted for an IP address, enter an asterisk “\*” or wildcard symbol to select all IP addresses; a complete IP address to restrict the selection to that address; or a partial IP address terminated by an asterisk, e.g., 192.168.1.\* , 192.168.\* or 192.\* to restrict the selection to addresses whose values match the partial address.

## Date/Time Range

Use **STARTING DATE/TIME** and **ENDING DATE/TIME** dropdown and selection fields to select the period for which you wish to run this chart or report.

## Charts

Select a chart from the **Reports/Charts** menu. Enter parameters in the Query Parameters dialog. The chart will display in a new window using the selected (or default) firewall list and group name parameters, the chosen Query Parameters and default chart parameters. The default chart name appears in the title bar and as a title in the chart window. Legends for each chart are displayed by default.

### Note

Default chart parameters are chosen to display the maximum amount of information in a readable and meaningful format.

In addition to the functions listed below, the user can select these options: window resizing (Minimize, Maximize, Restore), Close window (also, <ALT+F4>) and Print.

The Chart right-click menu includes: Chose Chart Title, Choose Different Chart Type and Display Report Text.

## Change Chart Title

Use **Change Chart/Report Title** under the windows menus to change the title displayed in the top-center of a chart or report. The user may also use the **Chart Parameters** dialog to change the title. This option is also selectable from the right-click menu.

## Choose Different Chart Type (Chart Parameters)

From a chart or report, the user can select Chart Parameters; select, copy and paste text in a highlighted report window; and select Chart Parameters or display a chart as a report in a highlighted chart window. This option is also selectable from the right-click menu.

To display the current chart using other parameters, select **Choose Chart Type** from the chart window menu; to display the current report as a chart, select **Chart Current Report** from the report window menu. This will bring up the **Chart Parameters** dialog, allowing the user to select the type of chart to display. You may then select a chart type or select specific fields to display and change chart labels and positions.

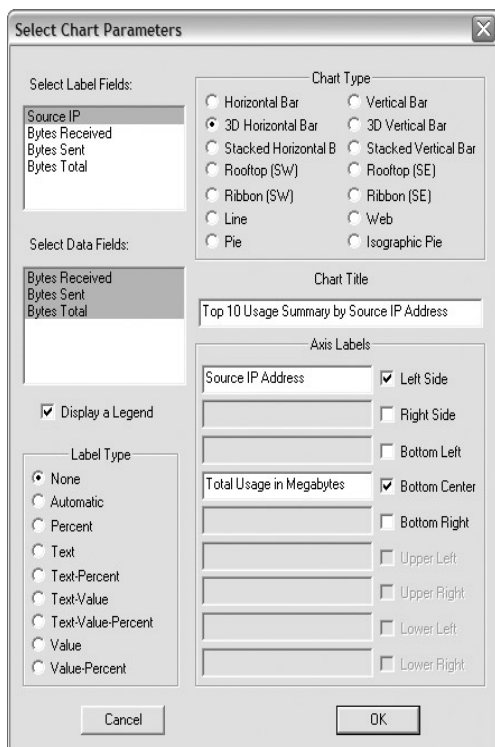
---

### Chart Parameter Fields

---

Label Fields	Label fields to display.
Data Fields	Data fields to display, depending on the data.
Display Legend	Display legend on the chart.
Label Type	Data item labels. None; Automatic; Percent: in pie charts, expresses the percentage of the value represented; Text: uses Axis Label text; Value: expresses exact numeric value of the labelled data; Text-Percent; Text-Value; Text-Value-Percent; Value-Percent.
Chart Type	Chart layout: Horizontal Bar, 3D Horizontal Bar, Stacked Horizontal Bar, Vertical Bar, 3D Vertical Bar, Stacked Vertical Bar, Rooftop SW and SE, Ribbon SW and SE, Line, Web, Pie, and Isographic Pie Chart.
Title	A chart title is required. Use to modify the chart title.
Axis Label	Optional. Label position must be specified.
Label Position	Identify the label location. Required to use labels.

---



The dialog box is titled "Select Chart Parameters". It contains several sections for configuring a chart:

- Select Label Fields:** A list box containing "Source IP", "Bytes Received", "Bytes Sent", and "Bytes Total". "Source IP" is selected.
- Select Data Fields:** A list box containing "Bytes Received", "Bytes Sent", and "Bytes Total". "Bytes Received" is selected.
- Display a Legend:** A checked checkbox.
- Label Type:** A group box containing radio buttons for "None", "Automatic", "Percent", "Text", "Text-Percent", "Text-Value", "Text-Value-Percent", "Value", and "Value-Percent". "None" is selected.
- Chart Type:** A group box containing radio buttons for "Horizontal Bar", "Vertical Bar", "3D Horizontal Bar", "3D Vertical Bar", "Stacked Horizontal B", "Stacked Vertical Bar", "Rooftop (SW)", "Rooftop (SE)", "Ribbon (SW)", "Ribbon (SE)", "Line", "Web", "Pie", and "Isographic Pie". "3D Horizontal Bar" is selected.
- Chart Title:** A text box containing "Top 10 Usage Summary by Source IP Address".
- Axis Labels:** A group box containing a list of labels and checkboxes for their positions:
  - "Source IP Address" with checkboxes for "Left Side" (checked) and "Right Side".
  - "Total Usage in Megabytes" with checkboxes for "Bottom Left", "Bottom Center" (checked), and "Bottom Right".
  - Three empty text boxes with checkboxes for "Upper Left", "Upper Right", "Lower Left", and "Lower Right".

At the bottom are "Cancel" and "OK" buttons.

*Chart Parameters*

## Display Report Text

Use Display Report Text to change the display in a highlighted chart window to a text report with the same information. The resulting report can be manipulated using the Reports functions described below. This option is also selectable from the right-click menu.

## Charts, Reports

From these chart window menu items, select new charts or reports based on the Firewall Group parameters chosen for the current window.



## Reports

Select a report from the **Reports/Reports** menu. Enter parameters in the Query Parameters dialog. The report will display in a new window using the selected (or default) firewall group parameters and the chosen query parameters. The default report name appears in the title bar and as a title in the report window.

In addition to the functions listed below, the user can select these options: window resizing (Minimize, Maximize, Restore), Close window (also, **<ALT+F4>**) and Print.

The Report right-click menu includes: Copy, Find, Find Again, and Select All; Change Report Title and Chart Current Report.

### Change Report Title

Use **Change Report Title** under the window menu to change the title displayed in the top-center of a report. This option is also selectable from the right-click menu.

### Chart Current Report

From a report, select Chart Current Report to change the display in a highlighted report window to a chart with the same information. The resulting chart can be manipulated using the Charts functions described above. This option is also selectable from the right-click menu.

## Editing Functions

The editing functions, Copy, Find, Find Again, and Select All are available from the report windows menu. Editing applies to the current window. This option is also selectable from the right-click menu.

## Charts, Reports

From these report window menu items, select new charts or reports based on the Firewall Group parameters chosen for the current window.



## 4 Standard Charts & Reports

### Overview

Data from logs can be used in both charts and reports. Information from a chart can be used to create a report and vice versa, therefore any of the standard charts listed below can be used to create a report of the same information using the contextual menu item **Display Report Text**.

### Standard Charts

Select a chart from the **Reports/Charts** menu.

#### Usage Summary

Usage Summary Charts refer to the number of bytes transferred between two endpoints, or the total number of connections made to a URL.

##### Top 10 by Source IP Address

Charts the total data transferred for the source IP addresses with the top 10 highest rates of use.

Input prompt	Date/time range.
Description	Horizontal bar chart with usage (horizontal) for each source IP address (vertical).

##### Top 10 by Destination IP Address

Charts the total data transferred for the destination IP addresses with the top 10 highest rates of use.

Input prompt	Date/time range.
Description	Horizontal bar chart with usage (horizontal) for each destination IP address (vertical).

##### Top 10 by Both Source and Destination IP Address

Charts the total data transferred for the source IP address/destination IP address pairs with the top 10 highest rates of use.

Input prompt	Date/time range.
Description	Horizontal bar chart with usage (horizontal) for each source/destination pair (vertical).

**Top 10 by Protocol**

Charts the total data transferred for the protocol and source IP address pairs with the top 10 highest rates of use.

Input prompt	Source IP address and date/time range.
Description	Horizontal bar chart with usage (horizontal) for each protocol/source pair (vertical).

**Sum by Time of Day and Source IP Address**

Charts the total data transferred for selected source IP addresses by time.

Input prompt	Source IP address and date/time range.
Description	Ribbon chart with usage (right ) by hour (left).

**Sum by Time of Day and Destination IP Address**

Charts the total data transferred for selected destination IP addresses by time and day.

Input prompt	Destination IP address and date/time range.
Description	Ribbon chart with usage (right ) by hour (left vertical).

**Sum by Time of Day, Day of Week and Source IP Address**

Charts the total data transferred for selected source IP addresses by time and day. It provides the best visibility of all data automatically; consequently, days may not appear in sequence.

Input prompt	Source IP address and date/time range.
Description	Ribbon chart with usage (right) by hour (left) and day of week (horizontal).

**Sum by Time of Day, Day of Week and Destination IP Address**

Charts the total data transferred for selected destination IP addresses by time and day. It provides the best visibility of all data; consequently, days may not appear in sequence.

Input prompt	Destination IP address and date/time range.
Description	Ribbon chart with usage (right) by hour (left) and day of week (horizontal).

**Firewall Filter Blocks**

Filter Blocks Charts summarize the number of packets blocked by a filter.

**Top 10 Rules Triggered**

Charts the Top 10 filter blocks triggered for filter rules. Zero indicates blocks that resulted from an implicit rule violation, such as “possible spoof.”

Input prompt	Date/time range.
Description	Vertical bar chart with total filter blocks triggered (vertical) for each filter rule (horizontal).

**Top 10 by Source IP Address**

Charts the top 10 filter blocks triggered for selected filter rules by source IP address.

Input prompt	Date/time range.
Description	Horizontal bar chart with total filter blocks triggered (horizontal) for the top 10 source IP addresses (vertical).

**Top 10 by Destination Port**

Charts the top 10 filter blocks triggered for selected filter rules by destination port.

Input prompt	Date/time range.
Description	Horizontal bar chart with total filter blocks triggered (horizontal) for the top 10 port pairs (vertical).

**Top 10 Rules Triggered by Source IP Address**

Charts the top 10 filter blocks triggered for selected source IP address/rule pairs. Zero indicates blocks that resulted from an implicit rule violation.

Input prompt	Source IP address and date/time range.
Description	Horizontal bar chart with total filter blocks triggered (horizontal) for the top 10 source addresses (vertical).

**By Day of Week**

Charts the filter blocks triggered for selected source IP addresses by the day of the week.

Input prompt	Source IP address and date/time range.
Description	Horizontal bar chart with the total number of blocks (horizontal) for each day of week (vertical).

**By Time of Day and Day of Week**

Charts the filter blocks triggered for selected source IP addresses by the day of the week and time of day. It provides the best visibility of all data automatically; consequently, days may not appear in sequence.

Input prompt	Source IP address and date/time range.
Description	Ribbon chart with the total number of blocks (right) for each hour (left ) and day of week (horizontal).

**Internet Access Management**

Internet Access Management Charts display information gathered by content filtering, available to those with Surf Sentinel 2.0 subscription. Request an evaluation of Surf Sentinel 2.0 from GTA's website at [www.gta.com](http://www.gta.com), or obtain a subscription by contacting a GTA Channel Partner or the GTA sales staff at [sales@gta.com](mailto:sales@gta.com).

## User Name

The user name reflects the name logged by the firewall when GBAuth is used for authentication. If you are not using authentication log data, run these reports by entering the wildcard symbol (\*) in the user name field, and use the source IP address for user identification. Where user name is applicable, the source IP address is referred to as the user IP address.

### Top 10 Web Categories by Connection

Charts the total connections made to the top 10 web categories.

Input prompt	Date/time range.
Description	Horizontal bar chart with total connections (horizontal) to the top 10 web categories (vertical).

### Top 10 Web Categories by Bandwidth

Charts the total bandwidth used for the top 10 web categories.

Input prompt	Date/time range.
Description	Horizontal bar chart with total bytes transferred (horizontal) for each of the top 10 web categories (vertical).

### Top 10 Web Users by Connection

Charts the total connections made by the top 10 web users.

Input prompt	Date/time range.
Description	Horizontal bar chart with total number of connections (horizontal) for the top 10 user IP addresses (vertical).

### Total Connections by Time of Day, Day of Week and User IP Address

Charts the total number of connections for the selected users by time and day.

Input prompt	User IP address and date/time range.
Description	Ribbon chart with total number of connections (right) by time (left) and day (horizontal).

### Total Blocked Web Access Attempts by Time of Day and Day of Week

Charts the total number of blocked web access attempts for a user by time of day and day of week.

Input prompt	User IP address and date/time range.
Description	Ribbon chart with number of blocked web access attempts (right) by time (left) and day (horizontal).

### Top 10 URLs by Bandwidth

Charts the total usage for the top 10 URLs.

Input prompt	Date/time range.
Description	Horizontal bar chart with bandwidth (horizontal) by URL (vertical).

**Top 10 URLs by Bandwidth and User IP Address**

Charts the total usage for the top 10 URL/user IP address pairs.

Input prompt	User IP address and date/time range.
Description	Horizontal bar chart with top 10 URLs/user IP address pairs (vertical) by total bandwidth (horizontal).

---

## Standard Reports

Select a report from the **Reports/Reports** menu.

### Usage Summary

Usage Summary Reports refer to the number of bytes transferred between two endpoints, or the total number of connections made to a URL.

#### By Source IP Address

Reports the total data transferred for the selected source IP addresses.

Input prompt	Source IP address and date/time range.
Columns	Source IP, Bytes Received, Bytes Sent, Bytes Total

#### Top 10 by Source IP Address

Same as above, limited to the top 10 users.

#### By Destination IP Address

Reports the total data transferred for the selected destination IP addresses.

Input prompt	Destination IP address and date/time range.
Columns	Dest IP, Bytes Received, Bytes Sent, Bytes Total

#### Top 10 by Destination IP Address

Same as above, limited to the 10 users identified by destination IP address.

#### By Both Source and Destination IP Address

Reports the total data transferred for the selected source/destination IP address pairs.

Input prompt	Source IP address, destination IP address and date/time range.
Columns	Source IP, Dest IP, Bytes Received, Bytes Sent, Bytes Total

#### Top 10 by Both Source and Destination IP Address

Same as above, limited to the top 10 source/destination IP address pairs.

#### By Protocol

Reports the total data transferred for each protocol and destination port for the selected source IP addresses.

Input prompt	Source IP address and date/time range.
--------------	--

Columns	Protocol, Dest Port, Source IP, Bytes Received, Bytes Sent, Bytes Total
---------	---

**Top 10 by Protocol**

Same as above, limited to the top 10 protocol and destination port pairs.

**Firewall Filter Blocks**

Filter Blocks Reports summarize the number of packets blocked by a filter.

**By Source IP Address**

Reports the total number of filter blocks for the specified source IP address or addresses.

Input prompt	Source IP address and date/time range.
Columns	Source IP, Blocks

**Top 10 by Source IP Address**

Same as above, limited to the top 10 source IP addresses.

**By Destination Port**

Reports the total number of filter blocks for the source IP addresses and associated destination IP addresses, ports and protocols.

Input prompt	Source IP address and date/time range.
Columns	Source IP and Port, Dest IP and Port, Protocol, Blocks

**Top 10 by Destination Port**

Same as above, limited to the top 10 destination IP addresses.

**Total Rules Triggered**

Reports the total number of filter blocks for each rule violated. Zero indicates blocks that resulted from an implicit rule violation.

Input prompt	Date/time range.
Columns	Rule, Blocks

**Rules Triggered by Source IP Address**

Reports the total number of filter blocks by the selected source IP addresses for each rule violated. Zero indicates blocks that resulted from an implicit rule violation.

Input prompt	Source IP address and date/time range.
Columns	Rule, Source IP, Blocks

**Top 10 Rules Triggered by Source IP Address**

Same as above, limited to the top 10 destination IP addresses.



## Internet Access Management

Internet Access Management Reports: see information under Internet Access Management Charts, page 27.

### Blocks by Time/Date and User IP Address

Reports the web site and category by time/date and user IP address.

Input prompt	User IP address and date/time range.
Columns	Time, User IP Address, Web Site and Category

### Blocks by Time/Date and User Name

Reports the user name, source IP address, web site and category by time of day.

Input prompt	User name and date/time range.
Columns	Time, User, User IP Address, Web Site, Category

### Total Blocks by User IP Address

Reports the web site, category and total attempts by user IP address.

Input prompt	User IP address and date/time range.
Columns	User IP Address, Web Site, Category and Total Attempts

### Total Blocks by User Name

Reports the user, source IP address, web site, category and total attempts by user name.

Input prompt	User name and date/time range.
Columns	User, User IP Address, Web Site, Category, Total Attempts

### Total Blocks by Category

Reports the total number of blocks by category.

Input prompt	Date/time range.
Columns	Category and Blocks

### Total Access Attempts by User

Reports the total attempts by a user by web site and category.

Input prompt	User name and date/time range.
Columns	User, Web Site, Category, Total Attempts

### Total Blocked Web Access Attempts by Time of Day and Day of Week

Reports the number of blocks by hour for each day of the week.

Input prompt	User IP address and date/time range.
Columns	Hour, Days of Week (Sunday through Saturday)

### Categories by Connection

Reports the total bytes for each category.

Input prompt	Date/time range.
--------------	------------------

Columns	Category, Total
---------	-----------------

**Usage Summary by Category**

Reports the connections and data transferred for each category.

Input prompt	Date/time range.
--------------	------------------

Columns	Category, Connections, Bytes Received, Bytes Sent, Bytes Total
---------	--

**Usage Summary by Category and URL**

Reports the connections, data transferred and URL for each category.

Input prompt	Date/time range.
--------------	------------------

Columns	Category, Connections, Bytes Received, Bytes Sent, Bytes Total, URL
---------	---

**Usage Summary by Category and Destination IP Address**

Reports the connections, bytes sent, bytes received, total bytes and destination for each category.

Input prompt	Date/time range.
--------------	------------------

Columns	Category, Connections, Bytes Received, Bytes Sent, Bytes Total, Destination IP
---------	--

**Usage by URL**

Reports the connections, bytes sent, bytes received, total bytes and URL for each source IP address.

Input prompt	Source IP address and date/time range
--------------	---------------------------------------

Columns	Source IP, Connections, Bytes Received, Bytes Sent, Bytes Total, URL
---------	--

**Top 10 Usage by URL**

Same as above, limited to the top 10 URLs.

**Most-Visited URLs**

Reports the URLs to which the selected source IP addresses connected and the total number of connections made.

Input prompt	Source IP address and date/time range.
--------------	--

Columns	Source IP, Connections, URL
---------	-----------------------------

**Top 10 Most-Visited URLs**

Same as above, limited to the top 10 URLs.

**Web Access by User and URL**

Reports the time of day for each URL by user name/source IP address.

Input prompt	Source IP Address, user name, web site URL and date/time range.
--------------	---

Columns	User Name, Source IP Address, Time of Day, Web Site
---------	---

## 5 Database Management

---

### Overview

The Database Management chapter covers the utilities provided by GTA to manage GTA Reporting Suite's database, GTAsyslog and DBmanager; the flow of data through the system, and how to set up standard DSNs for each of GTA Reporting Suite's supported databases.

---

### DBmanager

DBmanager provides a licensing interface, verifies installation success and maintains your selected database by performing backups, data purges, data restores, log imports, format conversions, re-initializations, unlocking and repairs. DBmanager also contains a configuration interface for GTAsyslog and LogView. Functions in DBmanager used by GTA Reporting Suite and GTAsyslog are covered in this guide; functions specific to other products are covered in that product's guide.

Once DBmanager is installed, select DBmanager from the **GTA** sub-menu of the **Windows Start Menu**.



*DBmanager – Database Tab*

## Database

The **Database** menu includes facilities for purge and backup, database conversion, re-initialization and repair, and a facility to unlock the database.

### Back Up and Restore Data

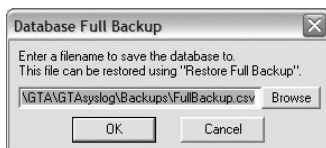
Backups and purges of old records can be done daily, weekly or monthly, depending on corporate requirements. Restore functions are used in case of a system failure or to search for evidence in a previously unrealized attack.

#### Note

GTA recommends storing full and incremental backups on a separate machine in a secure location. When using the same machine for backups, if the system fails, the backup files will be inaccessible.

#### Full Backup

Using Full Backup allows the user to create a backup file of the current database (FullBackup.csv). The database remains unchanged. A full backup does not remove any information.



*Full Backup*

#### Full Restore

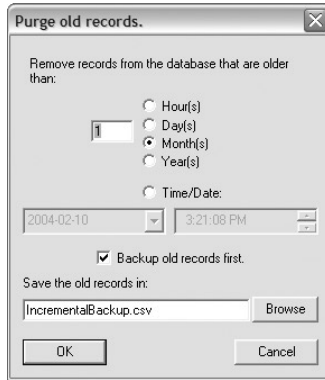
A Full Restore of the database allows the user to select a file that copied the contents of the database at a specific time and return the entire backup to the database (e.g., FullBackup.csv). The utility restores information exactly as it was at the selected Full Backup.

### Purge and Restore Data

Files backed up by Full Backup and Purge Old Records are named FullBackup.csv and IncrementalBackup.csv by default. Establish a file naming convention and select a backup location other than the one where the server database is housed.

#### Purge Old Records

Purge Old Records is a utility for deleting selected database records from the database and create an incremental backup in the Comma Separated Values format (IncrementalBackup.csv). The user enters either the number of hours, days, months or years before which records should be purged, or the date before which records should be purged.



*Purge Old Records*

### Restore Purge Records

Restore Purge Records allows the user to restore records deleted from the database and stored in an incremental backup (IncrementalBackup.csv).

### Convert to New Format

Convert a stored database to the current database format.

### Reinitialize

Reinitialize by removing the current database and replacing it with a new, blank database.

### Repair

The Repair function checks for missing or damaged tables in the database and if the database has become corrupted, restores them.

### Note

Always back up your database before re-initialization or repair.

### Unlock

Unlock clears the GTA options table, unlocking the connection between a client and its server. This allows another syslog the opportunity to connect and write to the database. The first syslog to write to the database has control of it, and the database is again locked.

## Utilities

The **Utilities** menu in DBmanager contains the GTA Reporting Suite Activation Code interface; an interface for configuring the GTAsyslog for GNAT Box System Software and GTA Reporting Suite; and the Import Logs function to import old logs into the GTA Reporting Suite. Instructions for activating GTA Reporting Suite are in Chapter 2 – Installation.



*DBmanager – Utilities Tab*

## GTAsyslog Utility Configuration

The GTAsyslog configuration dialog allows the administrator to select how GTAsyslog operates, where log files are kept, and which ports will be used by GTAsyslog and LogView. GTAsyslog writes data both to a circular file and to the database configured for GTA Reporting Suite and allows desired firewalls to be substituted for those that are currently monitored.

### Circular File

GTAsyslog automatically writes log data to a circular file in the standard WebTrends Enhanced Log Format (WELF). The file buffer size is dependent on the system and memory configuration. When the buffer is filled, GTAsyslog begins writing over older data. For instance, if the maximum number of files is five, and the maximum size of each log is 400 kilobytes, then when five log files each have been written, the first log file will be overwritten by the next consecutive log file. Circular file data can be viewed as it is written using LogView. Logs can be opened as text in a text editor.



## Licensed Firewalls

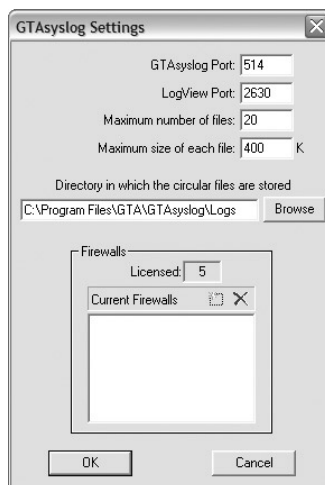
Once GTA Reporting Suite has been licensed, GTAsyslog begins logging the data of firewalls that report. All firewall information will go to the circular file, but if the number of firewalls logging exceeds the number of GTA Reporting Suite licenses, GTAsyslog will log the data of the first firewalls to report, up to the number of licenses, and no others will be able to log to the database.

## Current Firewalls (Add and Delete Monitored Firewalls)

GTAsyslog provides a way to substitute different firewalls for those currently monitored; this is mostly used in the case when the number of firewalls reporting to GTAsyslog exceeds the number of licenses, and other firewalls besides those that reported first are desired.

## GTAsyslog Fields

GTAsyslog Port	Default 514.
LogView Port	Default 2630.
Max number of files	Log entries retained before overwriting. Default 20.
Max size of each file	Maximum file size for each log. Default – 400 K.
File Directory	Circular log file name. Default C:\GTA\GTAsyslog\Logs.
Current Firewalls	Host names of firewalls monitored by GTAsyslog for GTA Reporting Suite.
New firewall 	Add a firewall to the monitored list manually.
Delete 	Stop monitoring a reporting firewall.



*GTAsyslog Configuration*

## Import Logs Utility

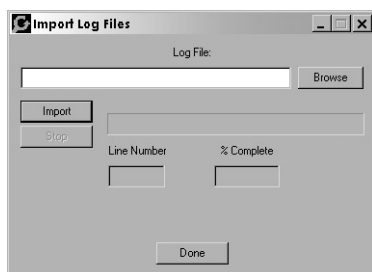
The Import Logs function imports GTA log files into the database or accesses log files from other sources.

To use the Import Logs function, click **BROWSE** and select one or more of log files in **C:\Program Files\GTA\GTAsyslog\Logs** or from any other location in which you have stored log files. Press the **<CTRL>** key while selecting file names to select more than one file.

When you have selected one or more log files, click **IMPORT**. Use the **STOP** button to stop the import process before it is complete. Click **IMPORT** again to restart the import. The **PROGRESS**, **LINE NUMBER** and **% COMPLETE** fields provide a calculation of the amount of data imported.

### Note

Compatible log files in WELF (WebTrends Enhanced Log Format) are required.



*Import Logs*

## Help

Verify Installation for GTAsyslog and GTA Reporting Suite and the About dialog box are found under DBmanager's **Help** menu.

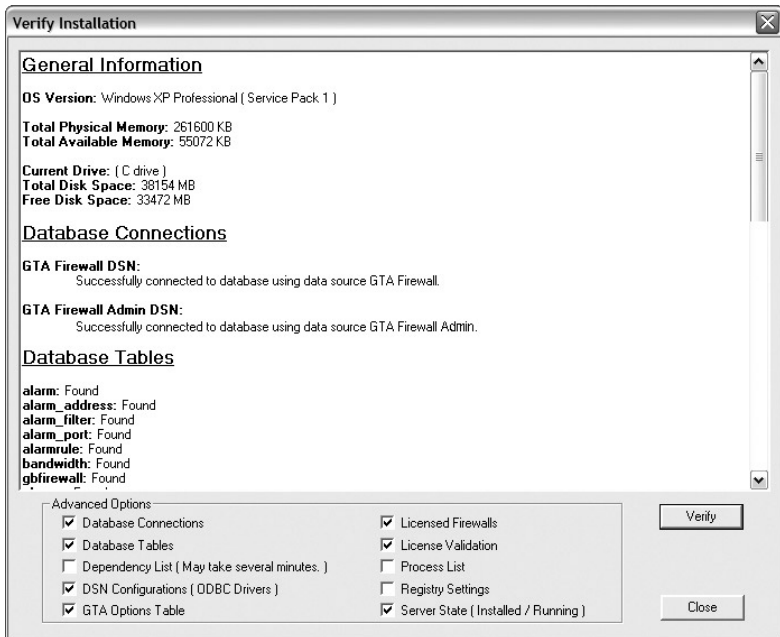
### Verify Installation

Verify Installation provides general information about your computer. It also provides a list of serial numbers; number of firewalls licensed; database information, including tables and DSNs; the status of GTAsyslog server; and associated registry settings.



The available verification options are:

- Database Connections
- Database Tables
- Dependency List
- DSN Configurations (ODBC drivers)
- GTA Options Table
- Licensed Firewalls & Validation
- Running Process List
- Registry Settings
- Server State (Installed/Running)



*Verify Installation*

## Creating DSNs

The required DSNs should be set up after the database has been installed and the ODBC drivers have been created, and before installation of GTA Reporting Suite and GTAsyslog. The configuration of DSNs will vary by database. See below for examples and suggested settings to apply to the DSNs of three supported databases.

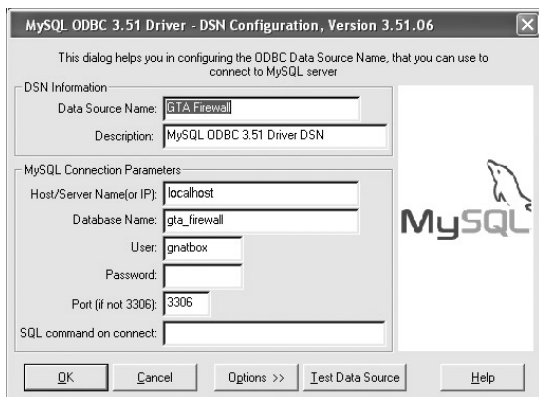
Two DSNs must be set up on the GTAsyslog server machine: *GTA Firewall* and *GTA Firewall Admin*. The *GTA Firewall* DSN must be created in any location where GTA Reporting Suite is installed alone. See Chapter 2 – Installation for more instructions on when and where to set up DSNs.

Use a standard Windows interface to create a DSN. On a Windows 2000 system, go to **Start/Control Panel/Administrative Tools** and select **Data Sources (ODBC)**. Click on the **System DSN** tab and choose **ADD** to open the **Create New Datasource** window. Scroll down and select the driver for your selected database. The DSN setup screen will appear.

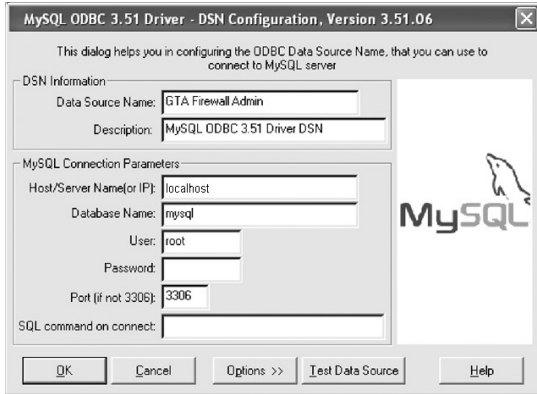
Enter the information and save to create each of the DSNs. Click **Save** and exit the Data Source Administrator. The DSN descriptions will be filled by the ODBC driver. When complete, the DSNs will appear in the System DSN list.

### MySQL DSNs

Data Source	GTA Firewall	GTA Firewall Admin
Database	gta_firewall	mysql
Host/Server	("localhost" or database IP address)	
User	gnatbox	root
Port	3306	3306



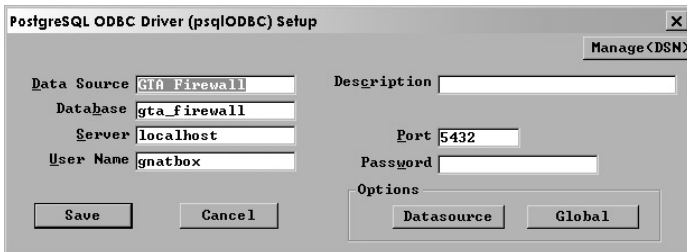
*GTA Firewall DSN Driver Setup*



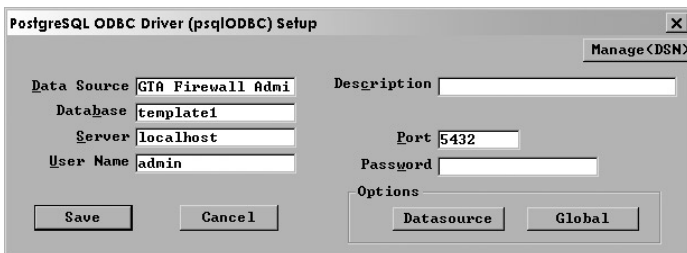
*GTA Firewall Admin DSN Driver Setup*

## PostgreSQL DSNs

Data Source	GTA Firewall	GTA Firewall Admin
Database	gta_firewall	template1
Host/Server	("localhost" or database IP address)	
User	gnatbox	admin
Port	5432	5432



*GTA Firewall DSN Driver Setup*

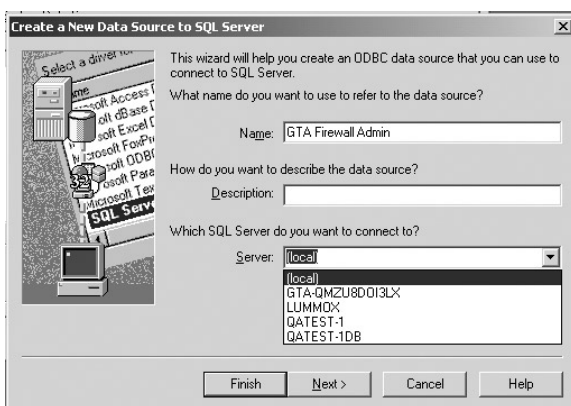


*GTA Firewall Admin DSN Driver Setup*

## Microsoft SQL Server DSNs

Use the DSN wizard to create the two required DSNs for SQL server. (These are the same DSNs created when MSDE is installed.)

Data Source	GTA Firewall	GTA Firewall Admin
Database	gta_firewall	master
Host/Server	("localhost" or database IP address)	
User	gnatbox	sa
Password	gnatbox	(None)
Port	1433	1433



*SQL Server DSN Wizard*

### GTA Firewall Admin DSN

1. Create a new DSN named `GTA Firewall Admin`, then select the appropriate SQL Server.
2. Check "with Windows SQL Server authentication..." and "Connect to SQL Server..." then enter `sa` (default) or another ID in the LOGIN ID field. Leave the PASSWORD field blank.
3. Select "Change the default database..." and enter `master`. Uncheck "Attach database filename." Check both "Ansi..." boxes.
4. Check "Perform translation for character data," and uncheck everything else on the screen.



*GTA Firewall Admin DSN Driver Setup*

#### **GTA Firewall DSN**

1. Create a new DSN named “GTA Firewall,” then select the appropriate SQL Server driver.
2. Check “with Windows SQL Server authentication...” and uncheck “Connect to SQL Server....” No ID or password is entered.
3. Select “Change the default database...” and enter `master`. Uncheck “Attach database filename.” Check both “Ansi...” boxes.
4. Check “Perform translation for character data,” and uncheck everything else on the screen.



*GTA Firewall DSN Driver Setup*



## 6 Troubleshooting

---

### Q&A

#### 1. Why can't I access any logs, OR, how do I start GTAsyslog?

This could mean that you have not entered a license activation code, or that GTAsyslog is no longer running. See Chapter 2 – Installation for more about entering your activation code to license your product. To verify that GTAsyslog is running, access the machine where you have set up GTAsyslog, e.g., from Windows 2000:

1. Select **Start/Settings/Control Panel/Administrative Tools/Services**.
2. In the Services applet, select the **GTAsyslog** Service.
3. If GTAsyslog has stopped, click the **Start Services** icon.

#### 2. How do I start my database manager?

Access the machine where you have set up the database manager, e.g., from Windows 2000:

1. Select **Start/Settings/Control Panel/Administrative Tools/Services**.
2. In the Services applet, select the database manager service.
3. If database manager has stopped, click the **Start Services** icon.

See your database documentation for more information.

#### 3. How do I retrieve a lost license activation code?

Saving an invalid activation code will "un-license" your product. Do not re-enter your license activation code (it is effective only once); send your product serial number, previous license activation code and contact information to the support email address, [support@gta.com](mailto:support@gta.com).

#### 4. I have installed GTA Reporting Suite, but I can't run reports.

This may indicate that your DSNs are pointing to the wrong location for your database. Using the information under "Creating DSNs" in Chapter 5, verify that your DSN has the correct location entered in the SERVER field. If your database is on your local machine, use "localhost." If your database is on another machine, enter the host name or IP address of that machine in the SERVER field.

## 5. How do I change the User Identity for GTAsyslog?

The GTAsyslog user can be changed in the Services applet:

1. Select **Start/Settings/Control Panel/Administrative Tools/Services** (in Windows NT/2000).
2. In the Services applet, select GTAsyslog.
3. Right-click and select **Properties** from the dropdown menu.
4. Select the **Logon** tab and enter the name and password for a valid user identity on the system.

## 6. After upgrade I get the following message: "The version of the database is not correct for this version of the GTA Reporting Suite."

First, perform a Full Backup of your old database. Then, open the DBmanager utility and click **CONVERT TO NEW FORMAT** under the Database tab to update/convert the database. This will transfer the compatible fields from the previous database to a new database.

## 7. After installing GTA Reporting Suite and GTAsyslog, I get a message similar to: "Error: unable to find the database gta\_firewall."

This message may indicate that your database manager (such as MySQL) has not started as a service, and the gta\_firewall database could not be created. From the Windows start menu, go to **Administrative Tools/Services**.

Locate MySQL, and start the service. Go back to Services and stop and restart the GTAsyslog service. This should create the gta\_firewall database.

If the service won't start, or the database manager is not in the services list, start the database manager as a service using the instructions in #8, below.

## 8. I installed the database package on a Windows XP, 2000 or NT platform, but it won't install as a service.

If, after downloading and installing your database package, you cannot find (or start) the database manager in Services, install it manually from a command prompt window, e.g.:

```
C:/ cd mysql
```

```
C:/mysql/>cd bin
```

```
C:/mysql/bin/> mysqld-max-nt --install
```



## Index

### Symbols

% 16  
 \*, wildcard 26  
 .csv, .doc, .html, .txt, .jpg 17

### A

asterisk. *See* wildcard symbol  
 attack 32

### B

back up  
     full 32  
     incremental 32  
 browsers  
     Internet Explorer ii

### C

cascade windows 15  
 case-sensitive 12  
 Change Chart/Report Title 19, 21  
 Chart Icon 17  
 column sizing 15  
 column sorting 15  
 Console interface 4  
 Content Filtering 4  
 conventions, documentation 3  
 CSV file format 17, 32

### D

database conversion 11, 32  
 database layout 7  
 database maintenance 31–33  
 data source. *See* DSNs  
 default setup 9  
 Documentation  
     additional 3  
     map 3  
 DOC file format 17  
 Driver Setup 38–41  
 DSNs 8, 31, 36, 38–41

### E

email address  
     support ii  
 error 44

export a file 17

### F

file format  
     csv 17  
     doc 17  
     html 17  
     jpg 17  
     txt 17  
 firewall group 16

### G

GB-Commander 1  
 GBAAdmin interface 4  
 GTAsyslog server utility 34–37  
     not running 43  
 GTA Firewall 38  
 GTA Firewall Admin 38, 39, 40  
 GTA Support ii

### H

help ii  
 High Availability 4  
 horizontal bar chart 23, 26  
 HTML file format 17

### I

Internet Explorer ii  
 Isographic pie chart 19

### J

Java 10, ii  
 JPG file format 17

### L

license 9, 10  
 Line Chart 19  
 log messages 34  
 lost license activation 43

### M

maintenance, database 31  
 Microsoft SQL Server 40  
 MSDE 1, 5, 8, 10, 40  
 MySQL 38, 44

### N

network layout 7  
 note 4, 17

## O

ODBC driver 1, 8, 37, 38

## P

PDF 3, 4

port

1433, Microsoft SQL Server 40

3306, MySQL 38

514, GTAsyslog 7

5432, PostgreSQL 39

PostgreSQL 39

Protected Network 7

PSN 7

purge/restore 32

## R

registration

GTA Firewall 3

reinitialize database 33

removal instructions 14

repair database 33

Report Icon 17

RFC 3164 13

right-click menus 15

Rooftop 19

## S

Serial Number 12

Services applet 43

sizing columns 15

sorting 15

SQL Server 40

Support ii

## T

Technical Support ii

tile windows 15

TXT file format 17

## U

unlock database 33

User Name

DSN 38, 39, 40

## V

Verification Code 12

Verify Installation in DBmanager 36

Vertical Bar 19

VPN 4

## W

Web chart 19

Web interface 4

WELF (WebTrends Enhanced Log  
Format) ii

wildcard symbol 16, 26

windows

nine concurrent 15

window menu 17, 19, 20