

# **GB-Commander**

## **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.

## GB-Commander version 1.1 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 GB-Commander</b>	<b>1</b>
Features	1
Requirements	1
Knowledge	2
<b>Support &amp; Registration</b>	<b>2</b>
Installation Support	2
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>
Connection Initiation	6
Typical Installation	6
Single-System Installation	7
<b>Preinstallation</b>	<b>8</b>
Database Setup	8
ODBC Driver	8
DSNs (Data Sources)	8
<b>Installation</b>	<b>9</b>
Database Conversion/Re-initialization	10
User Identity	10
Configuring the Client	10
<b>Activation</b>	<b>11</b>
Activation Information	11
Manual Activation	12
<b>Client-Only Installation</b>	<b>12</b>
<b>Initial Logon</b>	<b>13</b>
<b>Uninstall</b>	<b>13</b>
<b>3 USING GB-COMMANDER</b>	<b>15</b>
<b>Overview</b>	<b>15</b>
GB-Commander Client Interface	15
Menus	16
Hierarchy & Alarm Icons	17
Status	18
Statistics & Alarms	19
<b>Top-Level Group Properties</b>	<b>21</b>
Connect to Server	21
Preshared Secrets	21
SMTP Email Settings	22
MAPI Email Account	22
<b>Administration</b>	<b>23</b>
Add Firewall	23
Add Firewall from GB-Commander Client	25
Firewall Groups	25
Firewalls	26

Not Monitored Group .....	27
Permission Groups .....	27
Users .....	28
Administrators Permission Group .....	28
Change Default Administrator Password .....	28
Delete GTA Firewall .....	28
<b>Monitoring</b> .....	29
Set Alarm Notification .....	29
Alarm Events .....	30
Acknowledge Alarm .....	31
Clear Alarm .....	31
Statistics .....	31
Graph Type .....	31
Run Reports .....	32
<b>4 USING GTA REPORTING SUITE</b> .....	33
<b>Overview</b> .....	33
<b>Chart and Report Functions</b> .....	33
Query Parameters .....	34
IP Address .....	34
Date/Time Range .....	34
Export .....	34
Print .....	35
Charts, Reports Menus .....	35
<b>Charts Window</b> .....	35
Change Chart Title .....	36
Choose Different Chart Type (Chart Parameters) .....	36
Display Report Text .....	37
<b>Reports Window</b> .....	38
Change Report Title .....	38
Chart Current Report .....	38
Editing Functions .....	38
<b>5 DATABASE MANAGEMENT</b> .....	39
<b>Overview</b> .....	39
<b>DBmanager</b> .....	39
Database .....	40
Back Up and Restore Data .....	40
Purge and Restore Data .....	40
Convert to New Format .....	41
Re-initialize .....	41
Repair .....	41
Unlock .....	41
Utilities .....	42
Import Logs Utility .....	42
Help .....	43
Verify Installation .....	43
<b>Creating DSNs</b> .....	44
MySQL DSNs .....	45
PostgreSQL DSNs .....	46
Microsoft SQL Server DSNs .....	46
GTA Firewall Admin DSN .....	47

GTA Firewall DSN .....	48
Password Registry Settings .....	48
<b>6 TROUBLESHOOTING</b> .....	51
<b>Q&amp;A</b> .....	51
<b>Event Viewer</b> .....	54
<b>APPENDIX A MANAGEMENT EXAMPLES</b> .....	55
<b>Introduction</b> .....	55
<b>Great ISP Administrator</b> .....	55
Firewall Groups .....	56
Permission Groups .....	57
New Users .....	57
Permissions & Rules .....	58
Assign Permissions .....	58
Alarm Email Rules .....	60
<b>Great ISP Technician</b> .....	61
Firewall Group .....	61
Alarm Email Rules .....	62
<b>Acme IT Manager</b> .....	63
Create Subgroup .....	63
Alarm Email Rules .....	63
<b>Wickets User</b> .....	64
<b>APPENDIX B CHARTS &amp; REPORTS</b> .....	65
<b>Overview</b> .....	65
<b>Standard Charts</b> .....	65
Usage Summary .....	65
Firewall Filter Blocks .....	67
Internet Access Management .....	68
User Name .....	68
<b>Standard Reports</b> .....	69
Usage Summary .....	69
Firewall Filter Blocks .....	70
Internet Access Management .....	72
<b>INDEX</b> .....	75



# 1 Introduction

---

## About GB-Commander

GB-Commander, GTA's system for firewall management, is Windows-based enterprise software that allows administrators to monitor multiple firewalls from a central location. Firewalls can be grouped according to user-selectable criteria, providing a real-time view of network status and events.

GB-Commander reduces monitoring costs and increases efficiency. The included GTA Reporting Suite provides summary charts and reports in a variety of formats for quick analysis of network usage and trends to easily identify potential connectivity or security issues.

## Features

- Monitor multiple GTA Firewalls using one user-friendly interface.
- Define hierarchies for monitoring and configuration.
- Display status, statistics and alarms for each monitored firewall.
- Launch remote administration client to configure individual firewalls.
- Launch GTA Reporting Suite to chart collected data.
- Microsoft SQL Server Desktop Engine (MSDE) for small-scale use.

## Requirements

These are the minimum requirements for GB-Commander Server and Client. Requirements for memory, operating system and database type will increase with the number of firewalls, speed of data flow and data quantity.

### GB-Commander Server

- Supported ODBC-compliant database and associated driver.\*
- Firewalls using GNAT Box System Software version 3.4 or higher.
- Windows 2000 (SP 4), Windows XP (SP 1), or Windows 2003 Server. GTA recommends Windows server editions when managing 10 or more GTA Firewalls.
- 1 GHz Pentium III or better.
- 256 MB RAM dedicated to GB-Commander.

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

**Client**

- Windows 2000 (SP 4), Windows XP (SP 1), or Windows 2003 Server.
- ODBC driver previously selected for GB-Commander Server.
- 500 MHz Pentium III or better.

**Knowledge**

- Basic installation and function of desired database.
- Access to SMTP server and understanding of email configuration.
- Logon information for GTA Firewalls in network.
- Email addresses of those to whom alarms will be sent.
- Understanding of TCP/IP networking.

---

## **Support & Registration**

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

### **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 GB-Commander 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 may be 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 GB-Commander, a program designed to monitor the network activity of multiple GTA Firewalls. 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.
<b>BOLD SMALL CAPS</b>	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 or higher. 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 (stand-alone) .....	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 .....	User's Guide & Product Guides
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

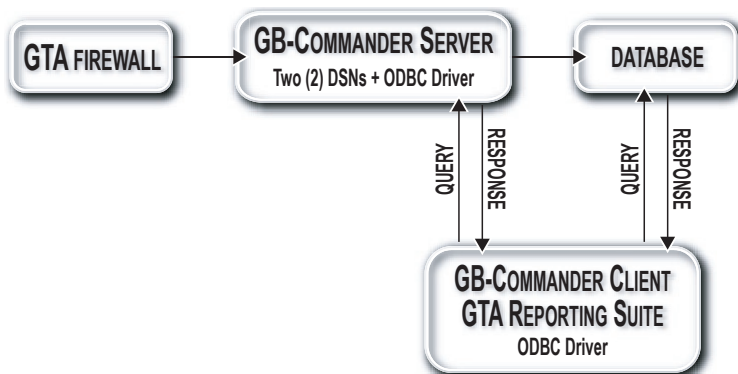
GB-Commander uses an ODBC-compliant databases. ODBC stands for Open DataBase Connectivity API (Application Programming Interface) that allows access to a database. For the most recent list of GTA's supported databases, see [www.gta.com](http://www.gta.com).

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.

---

### Network Configuration

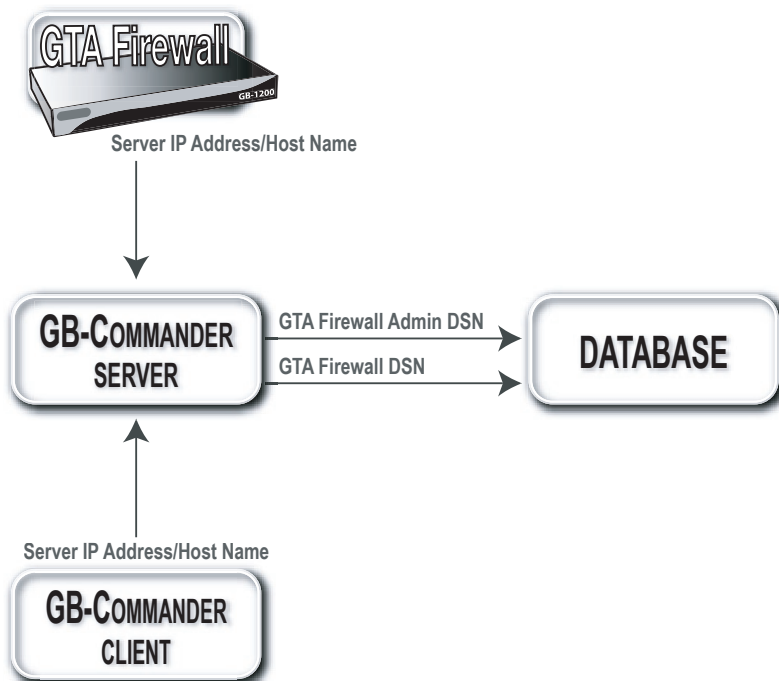
The diagram below shows GB-Commander's basic data flow. A firewall sends log data to GB-Commander Server, which parses the data and sends it to the database. GB-Commander Client can then query the server for the data, and GTA Reporting Suite can query the database directly, as illustrated below. (Multiple clients can monitor the same data.)



*Data Flow*

## Connection Initiation

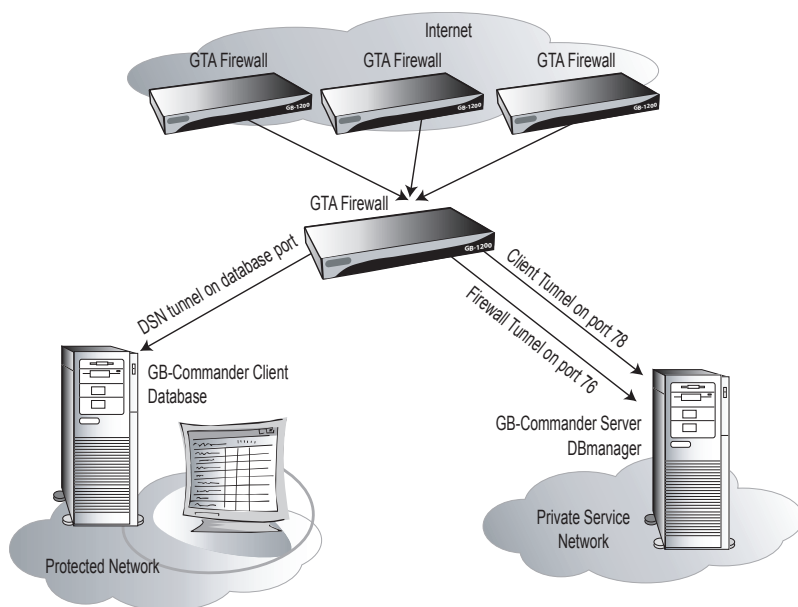
The diagram below illustrates the information required to initiate connections between the firewall, the server, the database and the client.



*Connection Initiation Requirements*

## Typical Installation

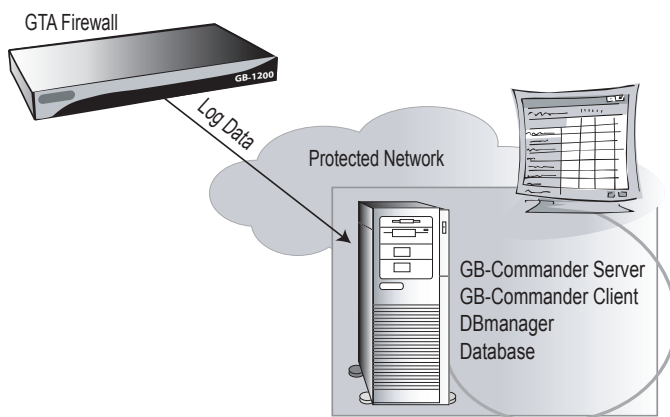
GTA recommends setting up the database on a separate machine. When multiple firewalls will be logging to GB-Commander Server, the layout on the next page is typical: the database server is housed on the PSN, with GB-Commander Client installed on the Protected Network. In the illustration, inbound tunnels will need to be added to the single GTA Firewall to allow access through the External Network interface on TCP port 76 for the GTA Firewalls accessed through the Internet.



*GB-Commander Typical Installation*

## Single-System Installation

The single-system installation illustrated below simplifies installation.



*Single System Installation*

## 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 GB-Commander Server and/or Client will be installed. (Exception: Microsoft SQL Server and MSDE use an ODBC driver installed with Microsoft products.)
4. Create two (2) DSNs, `GTA Firewall` and `GTA Firewall Admin`, on the machine where GB-Commander Server will be installed.
5. Insert the Installation CD or download GB-Commander. (A license is required to download and activate GB-Commander.)

## Database Setup

Select and install one of the supported ODBC-compliant databases. Install the database anywhere on the network accessible to GB-Commander Server. If the database is set up on a remote machine, the database server must be configured to accept connections from GB-Commander Server.

## ODBC Driver

Follow your selected database's installation instructions to install the associated ODBC driver on both GB-Commander Server and Client machines.

### **Note**

---

Microsoft SQL Server (as well as MSDE) uses an ODBC driver that is installed with Windows 2000 and later.

## DSNs (Data Sources)

A DSN connects an application with a selected database. After installing the database and ODBC driver, create two DSNs on the GB-Commander Server machine to communicate with the database: `GTA Firewall` and `GTA Firewall Admin`. See Chapter 5 – Database Management for assistance in creating the required DSNs.

## Installation

If using the installation CD, the wizard should start automatically when the disk is inserted. If using the download installer, or if the installation wizard does not start, locate and run the GB-Commander Full Install to install both Server and Client. The installation steps below may vary according to the selected options.

After the installer brings up the Export Notification dialog:

1. Read the license agreement; if you accept the terms, click **YES**.
2. Verify that you are installing GB-Commander Server and Client on the appropriate operating system; click **NEXT**. (GB-Commander Server may only be installed in one location; Client may be installed in multiple locations.)
3. Select an installation destination. (**C:\Program Files\GTA**)
4. Choose the typical (default) setup to install GB-Commander Server, Client, GTA Reporting Suite and Help files.
5. Review installation, then allow the installer to continue.
6. In the Select Service Owner window, enter a user name and password for GB-Commander Server. An administrator-level user is set up on the local machine. See the User Identity section, below.
7. Select whether to install program icons or view product notes. DB-manager (without GTAsyslog) will also be installed.
8. Select whether to install MSDE (Microsoft SQL Server Desktop Engine) as your database. (The MSDE installer is also available separately on the GB-Commander Installation CD.)
9. The license screen will appear; enter your serial number and verification code to license GB-Commander. If the license screen does not appear automatically (as when installing from download), open DBmanager, then go to Activation Code under the Utilities tab.
10. If you have a previously installed GB-Commander database, the installer will prompt you to convert it. Allow the existing database to be converted.

GB-Commander will now be installed. Any selected notes will be displayed after installation.

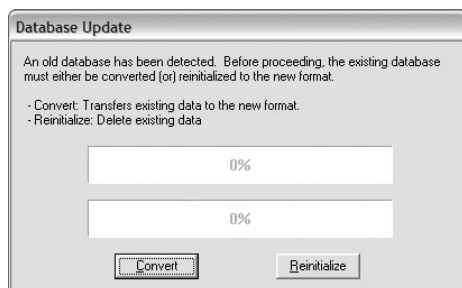
### Note

---

If you have a previous installation of the GB-Commander database, the user name and password screen will appear to allow the administrator to log on to GB-Commander Client.

## Database Conversion/Re-initialization

If an older format database already exists on your system, and the installation detects it, a conversion dialog will appear. This function can also be performed from the Database menu in DBmanager.



*Database Conversion Dialog*

## User Identity

GB-Commander Server must have a Windows user identity (logon account) on the machine where it is installed. During installation, you can set up an administrator-level user identity (user name and password) for the GB-Commander Server on the local machine. Create an separate account for the GB-Commander Server in order to set up appropriate permissions. To set up a user identity for the GB-Commander Server manually, see Chapter 6 – Troubleshooting.

### **Caution**

GTA recommends setting up the server's user identity on a local machine rather than an active directory (domain server). GB-Commander cannot authenticate the user with the domain, so the service must be started manually each time.

GB-Commander Server uses an SMTP mail server directly by default. For instructions on setting a mail server and source email address, or using a MAPI-enabled email account, see Chapter 3 – Using GB-Commander.

## Configuring the Client

When installed with GB-Commander Server, GB-Commander Client is automatically configured with the local host server IP address, 127.0.0.1. Once logged in using the default user name and password, any firewalls on which the GB-Commander service has been enabled and configured with the appropriate server IP address or host name will appear in the Not Monitored group. See Chapter 3 – Using GB-Commander, Add Firewall.



## Activation

After installation, the license screen will appear, prompting you to activate your product. Click **GET ACTIVATION CODE**. If you wish to use GB-Commander in evaluation mode, click **CLOSE WITHOUT CHANGES**. To access the license screen at other times, open DBmanager, go to **Utilities**, and click **ACTIVATION CODE**.

### Note

GTA Reporting Suite is not available in evaluation mode. Request an evaluation copy of GTA Reporting Suite at [www.gta.com](http://www.gta.com).

The License dialog box contains the following information:

Product	Serialization Code	Activation Code
GB-Commander	ZMKEDV-23793X-23793X-23793X-11P:KXV1	
GTA Reporting Suite	12E04MH-1L8ULED-1L8ULED-1L8ULED-16MRIDX	

Buttons at the bottom: Get Activation Code, Apply Activation Code, Close without changes.

*License Screen*

## Activation Information

In the Activation Information form, enter the serial number and verification code that appear on product packaging 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.

The Activation Information form includes the following sections:

- Serial Number:** [Text field]
- Verification code:** [Text field]
- Owner (Location of installation):**
  - Name: [Text field]
  - Company Name: [Text field]
  - Address: [Text field]
  - City: [Text field]
  - State: [Text field] Postal Code/Zip: [Text field]
  - Country: [Text field]
  - E-Mail: [Text field]
  - Phone: [Text field]
  - Fax: [Text field]
- System Administration:**
  - Contact Name: [Text field]
  - Company Name: [Text field]
  - Address: [Text field]
  - City: [Text field]
  - State: [Text field] Postal Code/Zip: [Text field]
  - Country: [Text field]
  - E-Mail: [Text field]
  - Phone: [Text field]
  - Fax: [Text field]

Buttons at the bottom: Print, Retrieve Activation Code, Cancel.

*Activation Form*

Click **RETRIEVE ACTIVATION CODE**. The license screen will reappear and the activation code should populate the **ACTIVATION CODE** field. Click **APPLY ACTIVATION CODE** to license GB-Commander.

### Manual Activation

If you do not have Internet access from the GB-Commander 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 - GB-Commander Activation. When you receive the activation code, enter the number in the **ACTIVATION CODE** field and click **APPLY ACTIVATION CODE** to license GB-Commander. 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.

---

## Client-Only Installation

GB-Commander Client is the user interface for GB-Commander Server. The client can be installed on workstations separate from the server.

Select the GB-Commander Client Installer icon from the Installation CD or download the latest client installer onto the selected workstation.

1. Read the GTA license agreement; if you accept the license terms, follow the instructions to install GB-Commander.
2. Select an installation destination. (**C:\Program Files\GTA**)
3. Choose the typical (default) setup to install the client components of GB-Commander.
4. Review installation, then allow the installer to continue.
5. Right-click on the globe icon and select **Properties**. Enter the host name or IP address of your GB-Commander Server.
6. Enter the preshared secret for communication between GB-Commander Server and the firewalls that will be monitored, if required.
7. Select whether to install program icons or view product notes.

GB-Commander Client will now install. Any selected notes will be displayed after installation is complete.

### Note

---

When the GB-Commander Client is installed on a workstation separate from GB-Commander Server, it must be configured with the correct server IP address or host name.

---

## Initial Logon

A password dialog will appear after the GB-Commander Client has contacted the Server. If you are a top-level administrator, enter the default: USER NAME: Administrator; PASSWORD: gnatbox. If you are a sub-administrator, enter the user name and password provided by the network administrator. The fields are case-sensitive. (The name of the current Windows user will appear automatically.)



*Password dialog box*

If the logon does not appear, and “No Connection” displays by the Globe icon, verify that the service has started, a user identity has been created for GB-Commander Server, and that the DSNs for your database have been set up correctly on the GB-Commander Server machine. Close and reopen your client. See Chapter 6 – Troubleshooting for more information.

---

## Uninstall

Select the installer used to install GB-Commander and follow the removal instructions given by the installation wizard.

Optionally:

1. Go to **Start/Settings/Control Panel/Add/Remove Programs** and select GB-Commander.
2. Select **Change/Add/Remove Programs** and follow the removal instructions.



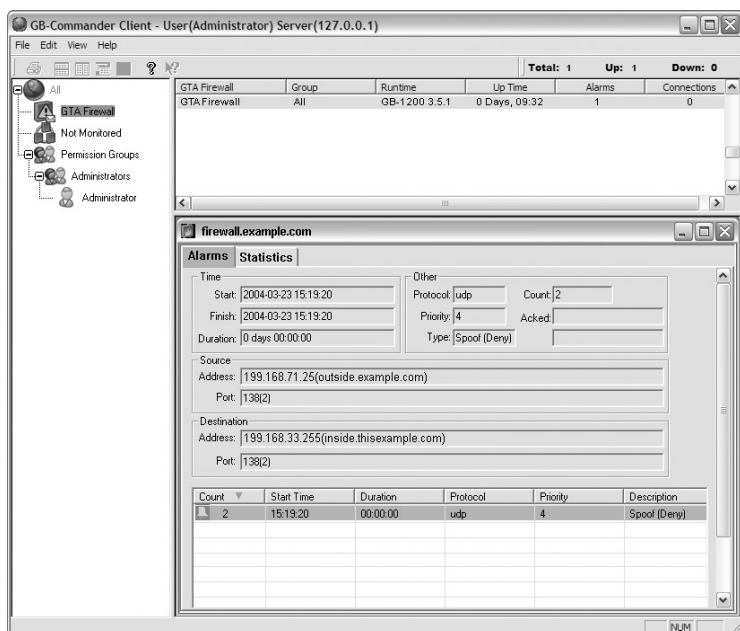
## 3 Using GB-Commander

### Overview

This chapter describes the GB-Commander interface, how to connect to a GTA Firewall, and how to create firewall groups, permissions groups and alarms. It also illustrates how to email alarm notifications and respond to alarms. See Appendix A – Management Examples for illustrations for users at various levels of the hierarchy.

### GB-Commander Client Interface

The main window of the GB-Commander Client is divided into three frames. The group hierarchy is in the left frame, the firewall status window is in the top right frame, and the statistics and alarms windows, as well as GTA Reporting Suit, are on the bottom right frame of the main window.



*GB-Commander Client Window with a GTA Firewall*

## Menus

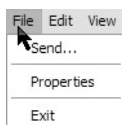
The main menu contains the GB-Commander global functions. Many of the functions available in the right-click and window menus are available in the main menu.

### File Menu – Send, Properties, Exit

Use **Send** to create and send email from the account of the user currently logged in. (If the workstation logon was `jdoe`, the email address for that user might be `jdoe@example.com`.) **Properties** opens the properties dialog box for the currently selected firewall or firewall group. Select **Exit** to quit the GB-Commander Client.

### Note

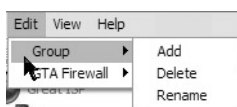
File/Send does not send email from the GB-Commander Server email account.



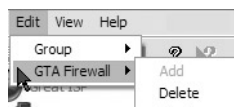
*File Menu*

### Edit Menu – Group, GTA Firewall

Select **Group/Add, Delete, Rename** to perform these functions with a firewall group; use **GTA Firewall/Add, Delete, Configure** to perform these functions with an individual GTA Firewall.



*Edit Group Menu*



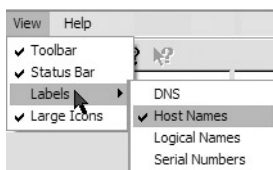
*Edit GTA Firewall Menu*

### View Menu – Toolbar, Status Bar, Labels, Icons

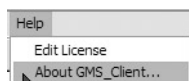
Select **Toolbar** and **Status Bar** to open these tool bars in the GB-Commander user interface. The toolbar and status bar provide quick access to windows arrangement, the GB-Commander About Box and a status summary of all GTA Firewalls that are currently monitored: total firewalls monitored, total firewalls communicating and the number of firewall being monitored that are not communicating. Use **Labels** to view GTA Firewalls by DNS entry, Host Name, user-defined Logical Name or Serial Number. **Large Icons** toggles between small and large icons in the GB-Commander hierarchy.

## Help Menu – Edit License, About GB-Commander Client

**Edit License** displays the GB-Commander and GTA Reporting Suite activation form and allows the administrator to send the GB-Commander activation request to GTA Support or print it for manual entry. **About GB-Commander Client** displays the serial number, version number, activation codes, file locations and DSNs (Data Source Names) for GB-Commander and GTA Reporting Suite, and allows the user to send this information by email to GTA Support.



*View Menu*



*Help Menu*

## Hierarchy & Alarm Icons











The hierarchy in the left-hand frame of GB-Commander Client contains a list of firewalls and firewall groups which can be viewed, accessed and modified, as well as users and permissions groups authorized to administer GB-Commander.

To modify the hierarchy, a user must be placed in a group with appropriate permissions. Administrators with full permissions will be able use all options. Users with fewer permissions may have some options greyed out, and may see only a relevant portion of the entire hierarchy.

The firewalls and users can be organized into groups, represented by a firewall group or permission group icon. In addition, each firewall state has an associated icon symbol: communicating, non-communicating, alarms generated and email configured. If a firewall or firewall group icon is greyed out, the firewall or a firewall in the group is not communicating.

The globe icon represents the root group for a user. For an administrator with full permissions to the system, this is all of the groups (All Groups, by default); for a user with limited permissions, the root group will be the top group the user can monitor.

## Icons

Icon	Description
	Root Group (All by default for the top-level Administrator).
	Firewall Group
	Permission Group
	GTA Firewall, Communicating (Fire Symbol, Red)
	GTA Firewall, Non-communicating (X Symbol, Grey)
	Caution icon indicates alarms have been generated.
	Smaller caution icon indicates alarms have been acknowledged.
	The mail symbol indicates that this firewall or group of firewalls is configured to send alarm emails.
	New Alarm (Yellow Bell with Red Outline)
	Acknowledged Alarm (Yellow Bell)

## Status

The Status Window in the upper right quadrant of the GB-Commander Client interface shows information for each GTA Firewall. From this window, the administrator can see the system software version of each GTA Firewall, how long it has run uninterrupted, how many new alarms have been generated, and how many connections are currently being made.

### Status Fields

GTA Firewall	IP address or logical name of this system.
Group	Name of group.
Runtime	GNAT Box System Software runtime version.
Up Time	Length of time this system has been running.
Alarms	Number of uncleared alarms.
Connections	Number of current connections for this system.



## Statistics & Alarms

Selecting a GTA Firewall displays the alarms and statistics for that GTA Firewall in the bottom-right frame. The **Alarm** tab displays the current alarms for the firewall. Alarms generated by the same event are displayed as one line item with the number of alarms indicated in the **COUNT** column. A description of the alarms making up the line item is presented in the fields above the line item alarms. Select a line item to see its information. Up to eight windows can be displayed in the Statistics and Alarms section.

The screenshot shows the 'Alarms' window with the following details:

- Time:** Start: 2004-03-19 10:10:01, Finish: 2004-03-19 10:10:01, Duration: 0 days 00:00:00.
- Other:** Protocol: tcp, Count: 1, Priority: 4, Acked: (empty), Type: RAF (Deny).
- Source:** Address: 69.22.108.140(user - outside.example.com), Port: (77781).
- Destination:** Address: 199.120.225.77 - ourserver.insideexample.com, Port: (23871).
- Table:**

Count	Start Time	Duration	Protocol	Priority	Description
8	14:07:21	00:50:10	udp	0	Remote Access Filter (Deny)
1635	14:08:10	00:41:51	tcp	0	Remote Access Filter (Deny)
4	14:19:44	00:21:31	icmp	0	Remote Access Filter (Deny)
1	10:10:01	00:00:00	tcp	4	Remote Access Filter (Deny)

*Alarms Window*

## Alarm Description

### Time

**Start/Finish** Start and end times of the alarms in this item.

**Duration** Length of time of the alarms in this item.

**Protocol** Protocol of the underlying filter.

**Count** Number of alarms in this alarm item.

**Priority** Priority of the underlying filters in this alarm item.

**Acked** Whether this alarm item has been acknowledged, the date and time, and the user who acknowledged it.

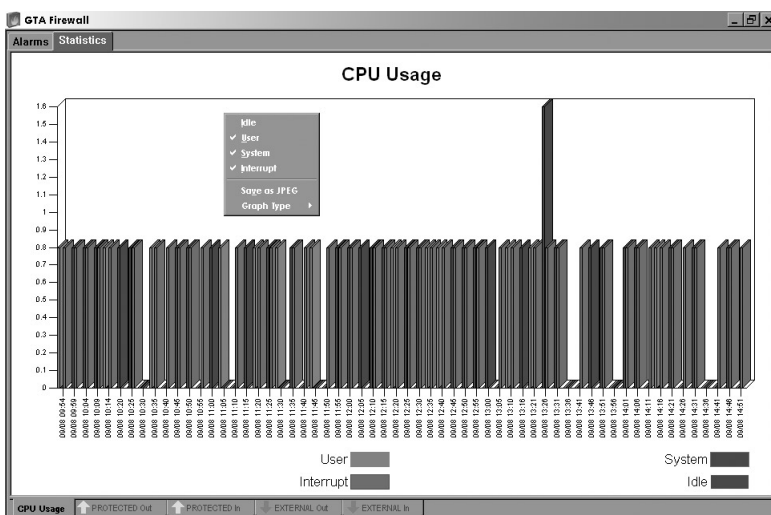
**Type/Description** Type of the underlying filter – Remote Access, Pass Through, Outbound; Deny/Accept; and description from the filter, if available.

**Source**  
**Address/Port** Source IP address and port numbers of the underlying filter. All ports applied are listed, with the number of total ports in parentheses.

**Destination**  
**Address/Port** Destination IP address and port numbers of the underlying filter. All ports applied are listed, with the total number of ports in parentheses.

## Alarms

Count	Number of alarms generated by the event.
Start Time	Time alarm event began. (Date will be included if the alarm events cover more than one day.)
Duration	Duration of event.
Source/Ports	Source IP address and ports of packet generating alarm.
Destination/Ports	Destination IP address and ports of generating packet.
Description	Description of event that generated alarm.



*Statistics Window with right-click menu*

## Statistics

CPU Usage	User, Interrupt, System and Idle process memory use.
In/Out	Average number of connections, packets sent and packets received by each network (e.g., Protected, External, PSN).

## Top-Level Group Properties

Right-click on the top-level globe icon (“All” by default) and select Properties. The top-level group properties allow the administrator to connect to GB-Commander Server; set a global preshared secret; see a list of reporting firewalls and their status; set SMTP mail properties; and set up global alarm emails. For instructions on using the alarm email (electronic mail) tab, see the Firewalls Groups and Firewalls sections on page 25.

### Connect to Server

In the General Tab, enter the host name or IP address of the machine on which GB-Commander Server is running in the HOST ADDRESS OR NAME field. The IP address 127.0.0.1 is equivalent to the local host name.

### Preshared Secrets

Preshared secrets allow two systems to exchange an agreed on password before beginning communication. The physical firewalls represented in the hierarchy must have an appropriate preshared secret entered in the GB-Commander service before they can communicate with GB-Commander. GTA recommends setting up preshared secrets after initial communication has been established.

### Preshared Secret Inheritance

Preshared secrets in GB-Commander are inheritable—in other words, if a group at one level of the hierarchy has a preshared secret, all groups and individual firewalls beneath that group will have the same secret, unless the groups or firewalls have another preshared secret set. This means that if the administrator does not want to share a preshared secret set at the top level of the hierarchy, sub-administrators must set a separate preshared secret at their root level.



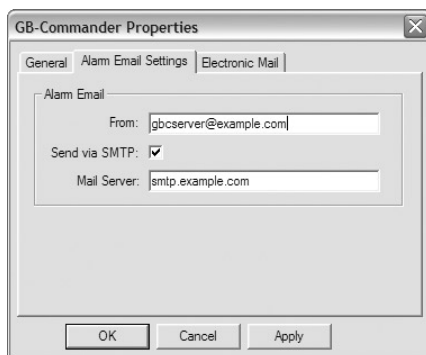
*GB-Commander Properties*

## SMTP Email Settings

SMTP Email Settings are configured for GB-Commander Server in the Alarm Email Settings tab of the top-level group properties. GB-Commander Server requires access to an SMTP server to send alarms, and, when sending mail on to another mail server, permission to relay mail through it. Mail uses the standard TCP port 25. See the illustration below for an example of using an SMTP server directly.

### Server Email Configuration

From	Enter a distinguishing email address for your source email address.
Send via SMTP	Select to use SMTP directly.
Mail Server	Enter the host name or IP address of a configured SMTP mail server accessible by GB-Commander server on TCP port 25.



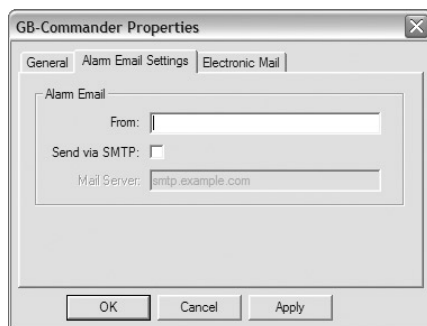
*SMTP (Email) Settings*

### MAPI Email Account

To use MAPI, deselect **SEND VIA SMTP** in the **Alarm Email Settings** tab. Values in other fields will be ignored.

Set up an account in a MAPI-enabled client using the same name and password created for the GB-Commander Server user identity. Specify an SMTP and POP3 server, then deselect the option that requires the client to create a warning message if another application attempts to send email.

GTA recommends using a client such as Outlook Express or Eudora. If using a Microsoft Exchange server (as with Microsoft Outlook), a policy must be created to allow access by an enterprise server. To set up appropriate policy settings for Microsoft Outlook 98 and 2000, use the instructions in **CUSTOMIZING THE OUTLOOK 98/2000 E-MAIL SECURITY UPDATE** at <http://www.microsoft.com/office/ork/2000/journ/outsecupdate.htm>.



*MAPI Email Settings*

## Administration

The Root Group (represented by a globe icon) is the base of the hierarchy for a given user. The root group for a sub-administrator is not the same as the top-level group, which can only be seen and accessed by administrators with appropriate permissions.

Each level beneath the root group is represented by a Firewall, Firewall Group or a Permission Group icon. GTA Firewalls are placed in one of the firewall groups, while users are given permissions to view or modify the hierarchy by being placed in permission groups. There can be any number of groups, and each group can be divided into subgroups. One firewall group, Not Monitored, will appear automatically and cannot be deleted. In addition, neither the Administrator permission group nor the main administrator account can be deleted. Other groups can be viewed, added, deleted and renamed as the user's permissions allow.

### Note

Group names must be unique throughout the system.

## Add Firewall

For GB-Commander Server to receive information from a firewall, the GB-Commander Service on the firewall must be configured. Log in to the GTA Firewall using the Web interface or GBAdmin. Select **GB-Commander Server** under the Services menu and click **Enable**. Leave the BINDING INTERFACE field set to "<Auto>," the firewall will detect the correct IP address. Enter the Server IP address or host name of the GB-Commander Server and define a port number, if desired.

The firewall should now send information to the GB-Commander database and appear in the GB-Commander Client hierarchy.

The binding interface is used to communicate with GB-Commander Server when using High Availability or accessing through a VPN.

Firewalls that have been configured, but not yet defined in the hierarchy, will appear in the Not Monitored group, where they can be moved into a named group. Firewalls cannot be manually added to the Not Monitored group.

### Note

GB-Commander is activated separately, and does not require a feature activation code on the firewall.

## GB-Commander Service

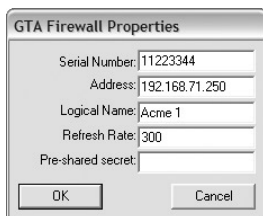
Enable	Enable communication from the firewall to GB-Commander Server.
Binding interface	Address from which GB-Commander Server is sourced. <b>&lt;Auto&gt;</b> indicates that the firewall should use its usual source IP address. To force data packets to have another source IP address, choose the desired interface object from the dropdown list. Auto by default.
Server	IP address or host name of the system on which GB-Commander Server is installed, and to which firewall data will be sent. To use a different port, enter the IP address and port number in the standard format, e.g., 192.168.71.2:76 or example.gta.com:76. The default is TCP port 76.
Preshared secret	ASCII or HEX value. The preshared secret as defined in GB-Commander. This field is case-sensitive.

GNAT-Box GB-Commander	
Enable:	<input type="checkbox"/>
Binding interface:	<AUTO> ▼
Server:	<input type="text"/>
Pre-shared secret:	<input type="text"/>
<input type="button" value="Default"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>	

*GB-Commander Service*

## Add Firewall from GB-Commander Client

The administrator may set up and add each firewall from GB-Commander Client. Right-click within the hierarchy and select **Add GTA Firewall** from the menu. In the dialog box that appears, enter the IP address, Logical Name and desired Refresh Rate of the GTA Firewall being added.

A screenshot of the 'GTA Firewall Properties' dialog box. It contains five text input fields: 'Serial Number' with the value '11223344', 'Address' with '192.168.71.250', 'Logical Name' with 'Acme 1', 'Refresh Rate' with '300', and 'Pre-shared secret' which is empty. At the bottom are 'OK' and 'Cancel' buttons.

GTA Firewall Properties	
Serial Number:	11223344
Address:	192.168.71.250
Logical Name:	Acme 1
Refresh Rate:	300
Pre-shared secret:	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### *Add GTA Firewall*

Right-click the newly defined firewall in the hierarchy and select **Configure** to access the firewall via the Web interface using SSL, the default interface. (Once the firewall has been configured, the user interface for configuration can be changed.)

## Modify Firewall Configuration

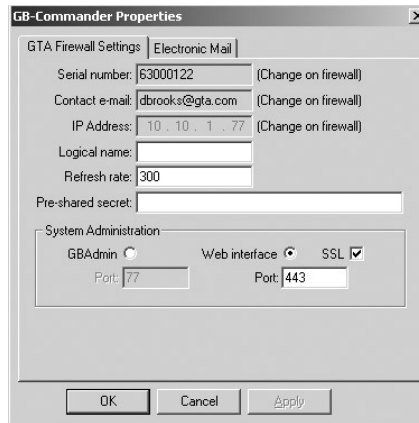
To change the logical name, administration user interface, refresh rate or enter a preshared secret, or to view the serial number, contact email and IP address of a GTA Firewall, right-click the firewall and select **Properties**. (The preshared secret must match the preshared secret configured on the GTA Firewall under GB-Commander Server.)

## Firewall Groups

To add a group, right-click on the appropriate level of the hierarchy and select **Add Group**. A group may also be created and then dragged to the desired location in the hierarchy. Right-click on a group and select **Rename** to highlight the name and allow it to be changed. The name may also be changed by entering it in the `Group Name` field under Properties. To delete a group and all the firewalls in the group, select the group, right-click on it and select Delete. Active GTA Firewalls will reappear in the hierarchy in the Not Monitored group.

## Firewalls

To make changes to the logical name, number of seconds between refresh, administration user interface and port and the preshared secret, bring up the GB-Commander GTA Firewall properties by right-clicking on the group or firewall's icon and selecting **Properties**. The serial number, contact email and IP address of the selected firewall will also appear in the GTA Firewall properties box, but these cannot be changed from the GB-Commander interface. (The preshared secret must match the preshared secret configured on the GTA Firewall under GB-Commander Server.)



*GB-Commander GTA Firewall Properties*

## GTA Firewall Settings

Serial Number	GTA Firewall serial number (static field from firewall).
Contact email	Contact email for this firewall (static field from firewall).
IP address	IP address of this firewall (static field from firewall).
Logical name	Name applied to this firewall in GB-Commander.
Refresh rate	Number of seconds between refresh of firewall statistical data, such as bandwidth, up time and runtime.
Preshared secret	The preshared secret must match the preshared secret configured on the GTA Firewall under GB-Commander Server.
User interface	Select GBAdmin or the Web Interface, then enter the for administration desired port. Defaults: GBAdmin: port 77. Web Interface: port 443, using SSL (default).



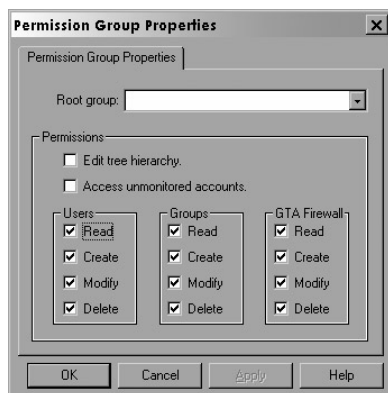
## Not Monitored Group

GTA Firewalls that have been configured to send their status information to the GB-Commander Server, but have not yet been placed in a group, will appear in the Not Monitored group when detected by the GB-Commander Server. Firewalls cannot be added manually to the Not Monitored Group, and only users with appropriate permissions can move firewalls from the Not Monitored Group.

## Permission Groups

Permission Groups allow the administrator to specify which users have access to various parts of the Hierarchy by placing the user in a Permission Group. Users at lower levels of the hierarchy can be given increasingly limited permissions, so that a user at one site can just view, or view and make modifications, only to the GTA Firewalls at that site or level. See example in Appendix A–Examples.

To create a permission group, right-click within the Permission Groups in the hierarchy and select Add Permission Group. A group with no permissions and the name New Group will appear. Enter a new name. Right-click on the permission group and select Properties. New groups and users have no permissions by default.



*Permission Group Properties*

Select the appropriate Root Group and permissions and click **OK** to save the permissions and close Properties. Click **Apply** to save the permissions without leaving the screen. The Root Group for a user is the firewall group at the top of that user's hierarchy.

## Users

To add a user, select the group, then right-click and select Add User from the menu. A New User (represented by a user icon) will be added to the group. To set a password, right-click on the user and select Properties. To give the user a new name, right-click on the user and select Rename. Move the user to a new group by selecting the user icon and dragging to the desired group. To delete, select the user and then select Delete.

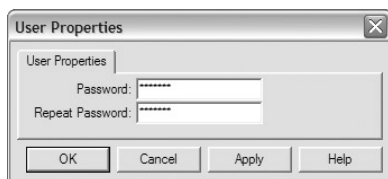
## Administrators Permission Group

An Administrators Permission Group is created with all permissions, with the default Administrator added as a user within it. Any user created or moved into this group has all its privileges. It is suggested that full permissions be granted only to a limited number of users.

## Change Default Administrator Password

The default Administrator has the user name “Administrator” and password “gnatbox.” The password should be changed; once it is changed, the administrator must log on using the new password.

To change a password, click on the plus “+” sign to open the group, then right-click on the user icon. Select **Properties**. Enter the desired password and then repeat the password for confirmation. Click **OK** or **Apply** to change the password. Click **Cancel** to cancel the password change.



*User Properties*

## Delete GTA Firewall

To delete a GTA Firewall from the hierarchy, right-click on the firewall and select **Delete**. If the firewall is still sending data to GB-Commander Server, it will reappear in the Not Monitored group.

## Monitoring

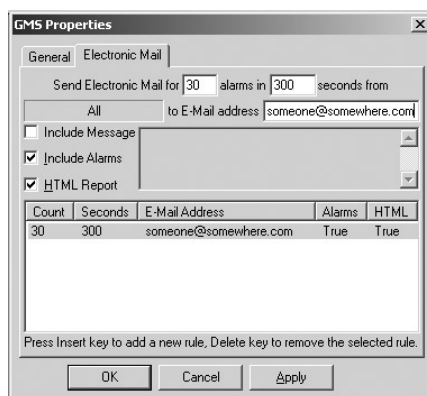
Alarm Email Rules enable GB-Commander to automatically notify a user that an alarm threshold has been reached (i.e., a certain number of alarm events have occurred within a specified time), indicating a possible attempt to invade the network or another problem requiring attention.

An Alarm Event occurs when a filter on a GTA Firewall is matched, and the alarm action for that filter is enabled. Each alarm event increments the alarm count by one. If the alarm threshold is reached within the specified time, a notification will be sent to the designated email address.

Each email includes all the alarm events that happened within a specified period, up to 500 alarm events. To learn more about how to trigger an alarm for a specific event, see the **GNAT BOX SYSTEM SOFTWARE USER'S GUIDE**.

### Set Alarm Notification

To set up an Alarm notification by email, right-click on the GTA Firewall or group and select **Properties**, then the **Electronic Mail** tab.



*Alarm Email Configuration*

Press the **<INSERT>** key to create a new alarm email. This will create a default rule that you can edit. Once you have edited an Alarm rule, click the **Apply** button at the bottom of the Properties dialog box. To add more rules, click outside the edit fields and press the **<INSERT>** key. To delete an Alarm Email Rule, select the rule in the window and press **<DELETE>**.

## Alarm Email Fields

Number & Time	Enter the number of alarm events and number of seconds to set the alarm threshold so that if at least X alarms occur within Y seconds, an email will be sent.
(Firewall or Group)	Logical name or serial number of the firewall or group to which this alarm rule is applied.
Email Address	Email address of the alarm notification recipient. Alarm emails can be sent to any email address. When sent to a pager, GTA recommends sending a short message with no alarms or HTML.
Include Message (Message body)	Allows the user to add a short message to the email. Enter the desired message. Basic HTML elements can be used in the text if HTML Report is selected.
Include Alarms	Adds the alarm log to the email. Selected by default.
HTML Report	Renders the alarm event log and message in HTML format. Selected by default.
Count	Threshold number of alarms to initiate notification.
Seconds	Time in which threshold number of alarms must occur.
Email Address	Address to which alarm notification will be sent.
Alarms	True = Send Alarms. False = Do Not Send Alarms
HTML	True = Send HTML report; False = Do Not Send HTML

## Alarm Events

Alarm events are logged and displayed in the Statistics and Alarms window of GB-Commander. The administrator may view an alarm, acknowledge it, investigate further if necessary, and clear the alarm. See a description of the alarm window fields on page 23.

Count	Start Time	Duration	Protocol	Priority	Description
8	14:07:21	00:50:10	udp	0	Remote Access Filter (Deny)
1635	14:08:10	00:41:51	tcp	0	Remote Access Filter (Deny)
4	14:19:44	00:21:31	icmp	0	Remote Access Filter (Deny)
1	10:10:01	00:00:00	tcp	4	Remote Access Filter (Deny)

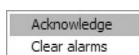
*Alarms Window*

To select more than one alarm, hold down the <CTRL> key while selecting each alarm with the mouse pointer; or press the key combination <CTRL-A> to select all the alarms in the Alarm view.

### Acknowledge Alarm

When an alarm first appears in the Alarm window, it is represented by a yellow bell icon outlined in red. This indicates an unacknowledged new alarm.

To indicate that you have seen a new alarm, right-click on the alarm or alarms and select **Acknowledge** from the menu or double-click the alarm. The alarm is now represented by a yellow bell icon without the red outline.



*Alarm right-click menu*

### Clear Alarm

Once an alarm has been acknowledged, it can be cleared. Select the alarm or alarms, right-click, and select **Clear Alarm** from the menu. The alarm line item will be removed from the display. Cleared alarms remain stored in the database until they are purged. Unacknowledged alarms can be cleared. (They will be automatically acknowledged.)

## Statistics

Using the Statistics Window, the administrator can review the bandwidth use for each GTA Firewall monitored by GB-Commander, and individually for each network on the firewall. Each GTA Firewall will have at least five statistics windows—overall usage, and in/out usage for the protected and the external networks. Using the right-click menu, the administrator can select any of four system measures: **Idle**, **User**, **System** and **Interrupt**.

If the correct statistics do not appear, you may have your GB-Commander Server DSN set to the wrong database location. See Chapter 5 – Database Management for information on how to set up a DSN for a database on a non-local machine.

### Graph Type

A Statistics graph can be displayed in 2D or 3D, as a pie graph, an area, step or strata line graph, or as a stacked or strata bar graph. The graph displayed can be saved as a jpeg. To display a part of a graph, select the desired section of the graph by clicking and dragging the mouse pointer. The selected information will be displayed in the statistics window.

### Graph Type Persistence

Graph type persists across all windows of the same type displayed until a new graph type is selected, subject to the refresh rate. For instance, if the CPU Usage graph type is changed, all CPU Usage graphs will display that graph type once their windows refresh. Newly opened windows showing CPU Usage will also display the selected graph type. In and Out windows for each interface will also display the same graph type.

## Run Reports

To run a report or chart on the selected firewall using GTA Reporting Suite, right-click the firewall and select **Reports/Charts** or **Reports/Reports**. See **Chapter 4 – Using GTA Reporting Suite** for more information.

## 4 Using GTA Reporting Suite

---

### Overview

GTA Reporting Suite queries data stored in the GB-Commander database to create reports, charts and graphs. GTA Reporting Suite provides a convenient way to analyze GTA Firewall log data and monitor firewall traffic.

To use GTA Reporting Suite, right-click the selected firewall or firewall group from the GB-Commander hierarchy menu. GTA Reporting Suite will open in a window within GB-Commander. Select the type and content of the report or chart from the right-click menu.

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.

#### **Note**

Only the licensed version of GB-Commander contains GTA Reporting Suite. Contact GTA Sales for more information about licensing, or see [www.gta.com](http://www.gta.com) to download an evaluation version of GTA Reporting Suite.

GTA Reporting Suite is consistent with a standard Windows interface, providing column sorting, column sizing and right-click menus. The window menu contains options available for each report or chart. Select options are also available using the right-click menu within the report or chart window.

---

### Chart and Report Functions

Chart and Report functions are selected from each chart or report window menu. Functions common to both windows are described below. Chart and report window menus display options available for the report or chart.



*Chart Icon*

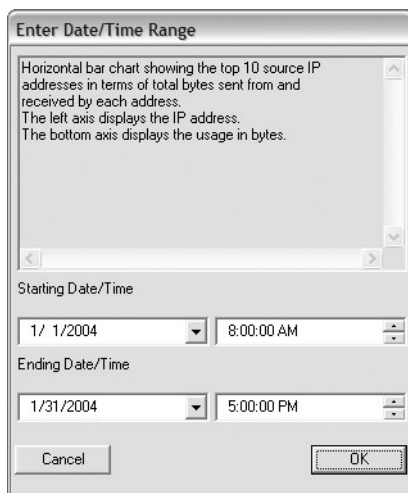


*Report Icon*

## Query Parameters

Both Charts and Reports use the Query Parameters dialog. Choose a firewall or firewall group, and then select a chart or report to run. The Query Parameters dialog will appear. The available parameters will vary by the type of chart or report.

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 a single asterisk “\*” to select all IP addresses; a complete IP address to restrict the selection to the specified address; and a partial IP address terminated by an asterisk, e.g., 192.168.1.\*, 192.168.\*, 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.

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

## 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 Menus

From these chart window menu items, select new charts or reports. Charts and reports run from this menu will share the parameters chosen for the parent window, including the firewall or group the chart covers and the chart parameters. The secondary chart or report will replace the parent window.

---

## Charts Window

Select a chart from the **Charts** menu. Enter parameters in the Query Parameters dialog. The chart will display in a new window using the firewall or firewall group 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.

The right-click menu for charts contains the window functions **Minimize**, **Maximize**, **Restore**, **Move and Size**; the chart functions **Export**, **Change Chart Title**, **Choose Different Chart Type (Chart Parameters)**, **Display Report Text** and **Print...**; the **Close** command; and secondary charts and reports menus.

## 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.

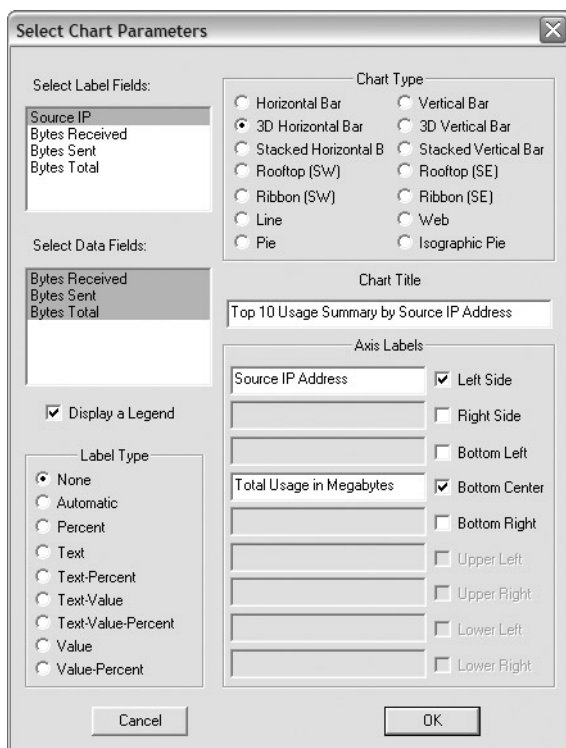
---

### 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	Adds labels to individual data items. None; Automatic; Percent: used in pie charts, expressing the percentage of the value represented in the chart; Text: uses the Axis Label text; Value: expresses the exact numeric value of the labelled data; Text-Percent; Text-Value; Text-Value-Percent; Value-Percent.
Chart Type	The layout for the selected chart: 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. The label position must be specified to use an Axis label. Defaults labels are entered.
Label Position	Required to use chart labels. Left, Right, Bottom Left, Bottom Right, Bottom Center, Lower Left, Lower Right, Upper Left, Upper Right.

---



**Select Chart Parameters**

Select Label Fields:

- Source IP
- Bytes Received
- Bytes Sent
- Bytes Total

Select Data Fields:

- Bytes Received
- Bytes Sent
- Bytes Total

☒ Display a Legend

Label Type

- ☒ None
- ☐ Automatic
- ☐ Percent
- ☐ Text
- ☐ Text-Percent
- ☐ Text-Value
- ☐ Text-Value-Percent
- ☐ Value
- ☐ Value-Percent

Chart Type

- ☐ Horizontal Bar
- ☒ 3D Horizontal Bar
- ☐ Stacked Horizontal B
- ☐ Rooftop (SW)
- ☐ Ribbon (SW)
- ☐ Line
- ☐ Pie
- ☐ Vertical Bar
- ☐ 3D Vertical Bar
- ☐ Stacked Vertical Bar
- ☐ Rooftop (SE)
- ☐ Ribbon (SE)
- ☐ Web
- ☐ Isographic Pie

Chart Title

Top 10 Usage Summary by Source IP Address

Axis Labels

Source IP Address	<input checked="" type="checkbox"/> Left Side
	<input type="checkbox"/> Right Side
	<input type="checkbox"/> Bottom Left
Total Usage in Megabytes	<input checked="" type="checkbox"/> Bottom Center
	<input type="checkbox"/> Bottom Right
	<input type="checkbox"/> Upper Left
	<input type="checkbox"/> Upper Right
	<input type="checkbox"/> Lower Left
	<input type="checkbox"/> Lower Right

Cancel OK

*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.

## Reports Window

Select a report from the **Reports** menu. Enter parameters in the Query Parameters dialog. The report will display in a new window using firewall or 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.

The Report right-click menu contains the window functions **Minimize, Maximize, Restore, Move and Size**; the report functions **Export, Change Report Title, Chart Current Report**, and **Print...**; the **Close** command; the editing functions **Copy, Find, Find Again**, and **Select All**; and secondary charts and reports menus.

### Change Report Title

Use **Change Report Title** under the windows 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.

## 5 Database Management

---

### Overview

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

---

### DBmanager

DBmanager provides a licensing interface, verifies installation success and maintains the database by performing backups, data purges, data restores, log imports, format conversions, re-initializations, unlocking and repairs. Functions in DBmanager used by GB-Commander with built-in GTA Reporting Suite 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

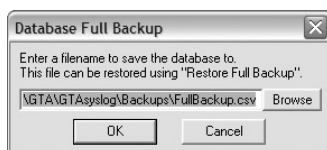
Backups and purges of old records can be done daily, weekly or monthly, depending on corporate requirements. Restore functions are used in case of a system failure or to search for evidence in a previously unrealized attack.

#### 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. As with all backup files, 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 alarm 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).

#### **Note**

DBmanager locks open backup files for use by other applications.

### Convert to New Format

Convert a stored database to the current database format.

### Re-initialize

Re-initialize 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, attempts to restore 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 controls it, and the database is again locked.

## Utilities

The **Utilities** menu in DBmanager contains the GB-Commander Activation Code interface and the Import Logs function to import old logs into the database. Instructions for activating GB-Commander are in Chapter 2 – Installation.



*DBmanager – Utilities Tab*

## Import Logs Utility

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

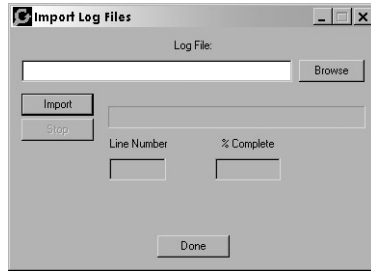
To use the Import Logs function, click **BROWSE** and select one or more of log files in **C:\Program Files\GTA\GTAsyslog\Logs** or from any other location in which you have stored log files. Press the **<CTRL>** key while selecting file names to select more than one file.

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

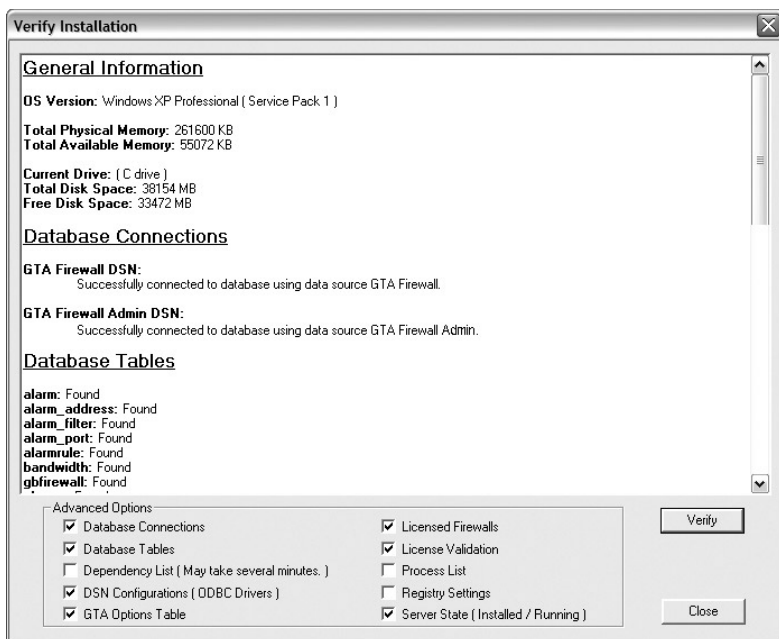
Verify Installation for GB-Commander and the About dialog box are found under DBmanager's **Help** menu.

### 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 GB-Commander 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

A DSN connects an application with a selected database. The DSNs required for GB-Commander should be set up before installation. Two DSNs must be set up on the GB-Commander Server machine: GTA Firewall and GTA Firewall Admin.

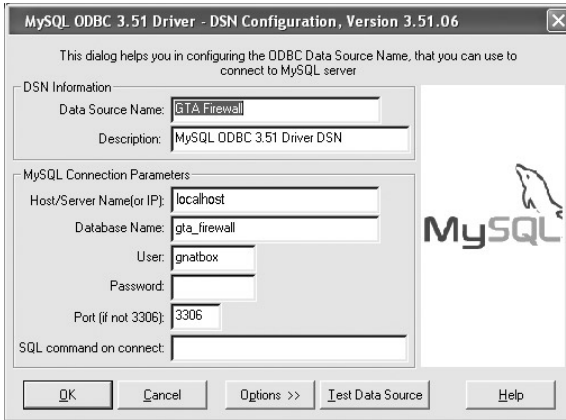
Use a standard Windows interface to create a DSN. On a Windows 2000 system, go to **Start/Control Panel/Administrative Tools** and select **Data Sources (ODBC)**. Click on the **System DSN** tab and choose **ADD** to open the **Create New Datasource** window. Scroll down and select the driver for your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

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

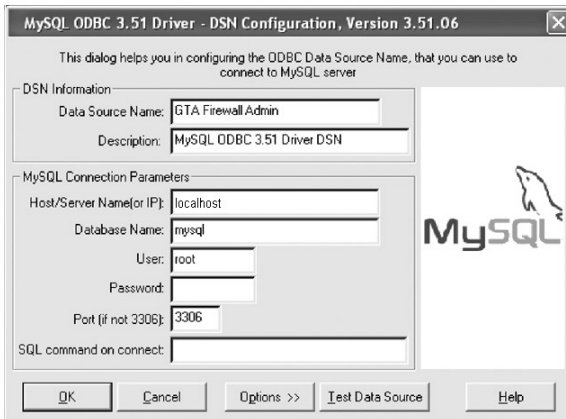
The configuration of DSNs will vary by database. See below for examples and suggested settings to apply to the DSNs of three supported databases.

## 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

The screenshot shows the 'PostgreSQL ODBC Driver (psqlODBC) Setup' dialog box. The 'Data Source' field is set to 'GTA Firewall'. The 'Database' field is 'gta\_firewall', 'Server' is 'localhost', and 'User Name' is 'gnatbox'. The 'Port' is '5432'. The 'Description' field is empty. The 'Password' field is empty. The 'Options' section has 'Datasource' selected. There are 'Save', 'Cancel', and 'Manage (DSN)' buttons.

*GTA Firewall DSN Driver Setup*

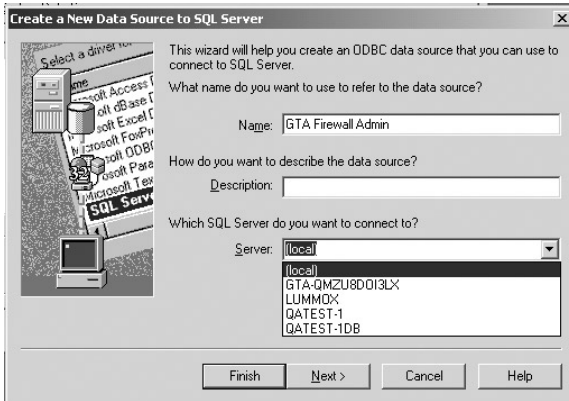
The screenshot shows the 'PostgreSQL ODBC Driver (psqlODBC) Setup' dialog box. The 'Data Source' field is set to 'GTA Firewall Admin'. The 'Database' field is 'template1', 'Server' is 'localhost', and 'User Name' is 'admin'. The 'Port' is '5432'. The 'Description' field is empty. The 'Password' field is empty. The 'Options' section has 'Datasource' selected. There are 'Save', 'Cancel', and 'Manage (DSN)' buttons.

*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.)

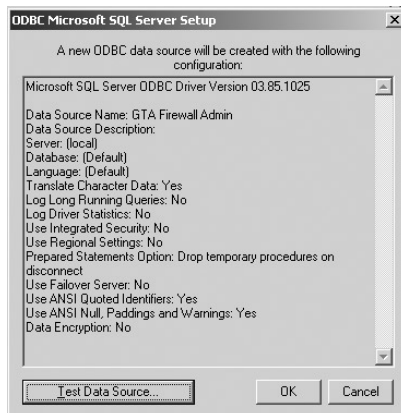
Data Source	GTA Firewall	GTA Firewall Admin
Database	gta_firewall	master
Host/Server	("localhost" or database IP address)	
User	gnatbox	sa (default)
Password	gnatbox	None (default)
Port	1433	1433



*SQL Server DSN Wizard*

### GTA Firewall Admin DSN

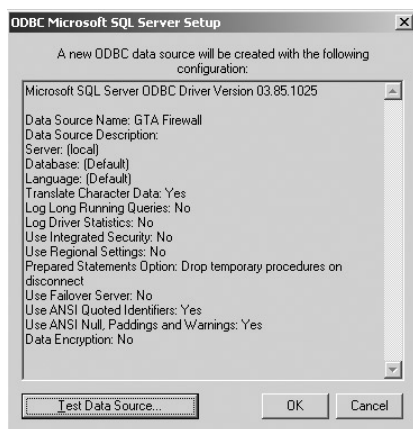
1. Create a new DSN named “GTA Firewall Admin,” select the SQL Server where the database will be installed.
2. Check “with Windows SQL Server authentication...” and “Connect to SQL Server...,” then enter “sa” (default) or a specified ID in the LOGIN ID field. Leave the PASSWORD field blank (default), or enter a password. (If using a password, see the following section, “Password Registry Settings.”)
3. Select “Change the default database...” and select “master.” Uncheck “Attach database filename.” Check both “Ansi...” boxes.
4. Check “Perform translation for character data” and uncheck everything else on screen.



*GTA Firewall Admin DSN Driver Setup*

## GTA Firewall DSN

1. Create a new DSN named “GTA Firewall,” select the SQL Server where the database will be installed.
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 “gta\_firewall.” Uncheck “Attach database filename.” Check both “Ansi...” boxes.
4. Check “Perform translation for character data” and uncheck everything else on screen.



*GTA Firewall DSN Driver Setup*

### Note

In GB-Commander, GB-Commander Client and GTA Reporting Suite share the database.

## Password Registry Settings

SQL Server requires that a user and password external to the DSN be modified in the registry. If entering a user name or password other than the default, as when you have an existing database and would like to use its password, set up your DSNs accordingly and then modify the user name and password in your registry settings in the registry key: \\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\GTA\\Database\\DSN Admin, and: \\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\GTA\\Database\\DSN User.

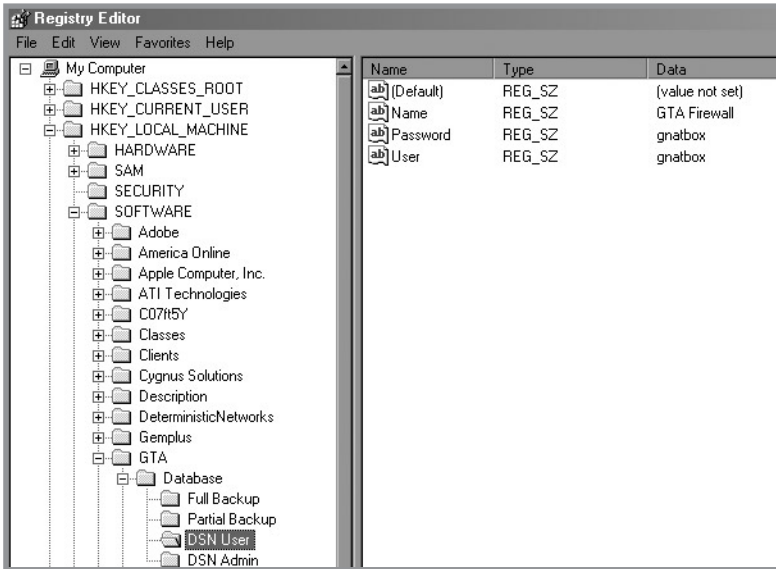
In the illustration of DSN User, all of the settings are set to defaults.

### Note

Your DSN setup should match your registry settings.

**DSN User – \\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\GTA\\Database\\DSN User**

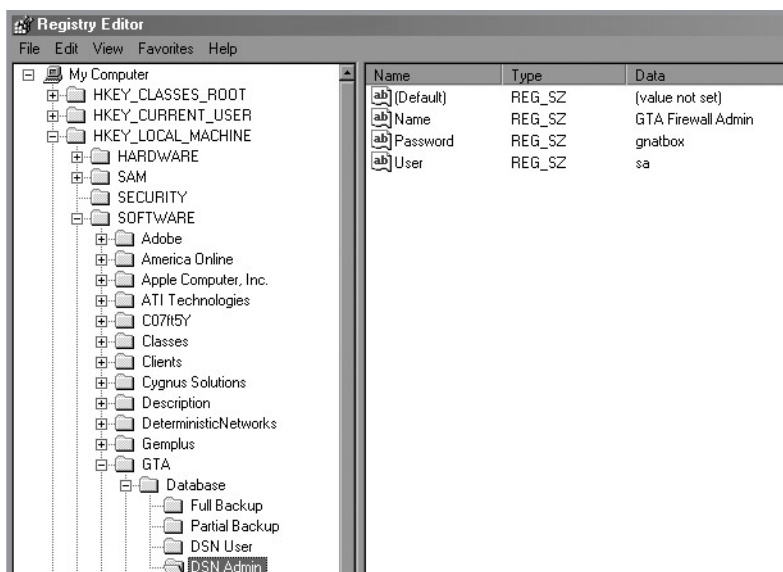
Registry Name	Description	Default
Name	Name of DSN to use	GTA Firewall
User	Login name	gnatbox
Password	Login password	gnatbox

*DSN User Registry Settings (default values)*

In the illustration of DSN Admin, the registry settings have been modified by entering a password, “gnatbox.” (The default setting has no password.)

**DSN Admin – \\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\GTA\\Database\\DSN Admin**

Registry Name	Description	Default
Name	Name of DSN to use	GTA Firewall Admin
User	Login name	sa
Password	Login password	(None)



*DSN Admin Registry Settings (password, "gnatbox")*



## 6 Troubleshooting

---

### Q&A

For more Troubleshooting suggestions, see the **GNAT BOX SYSTEM SOFTWARE USER'S MANUAL**

#### 1. 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.

#### 2. 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).

#### 3. I have GB-Commander with GTA Reporting Suite, but I can't run reports, and no data appears under Statistics.

If you have verified that your firewalls are sending data to GB-Commander Server, this problem 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.

#### 4. After upgrade I get the following message: "The version of the database is not correct for this version of the GB-Commander."

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.

### 5. After installing GB-Commander, I get the following message: “Error: unable to find the database gta\_firewall.”

This message indicates that the gta\_firewall database is unreachable; the installer may have failed to create the database. To manually create the database, open a command prompt and move to the sql directory or your database, e.g., `c:\mysql\bin`. Start your database, then enter the following command: `Create database gta_firewall;` Press **<ENTER>** to create the database.

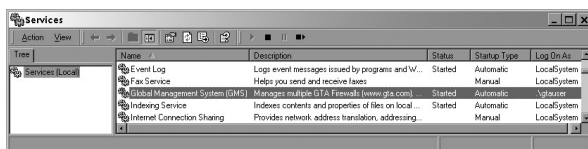
### 6. After opening the GB-Commander Client and loading GB-Commander, I see an error message similar to: “SQL Connect Failed!” when I try to run a report.

Check that your database is running. Verify that your DSNs are in place and set to point to the correct IP address of your database. Ensure that the correct ODBC driver is installed on your server and client machines.

### 7. How do I start the GB-Commander Service manually?

Occasionally, you may need to restart the GB-Commander service, e.g., if you have used a domain account; if you install the service without creating an account; or if the service shuts down. For example, from Windows 2000:

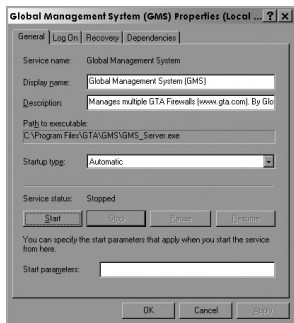
1. Select **Start/Settings/Control Panel/Administrative Tools/Services**.
2. In the Services applet, select **system for firewall management**.
3. If database manager has stopped, click the **Start Services** icon.



*Services*

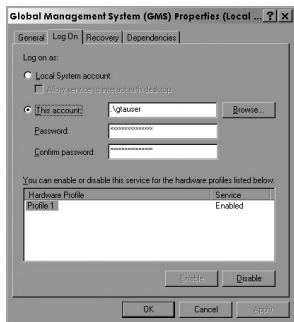
### 8. How do I set up a Server User Identity Account?

The GB-Commander Server must be a recognized user on the machine where it is installed. If you did not create a user and password during installation, Service Properties will appear when you select **Start Services**. Use this screen to set up a user identity for the GB-Commander Server. Under the Log On tab, select **THIS ACCOUNT** and enter a valid account and password.



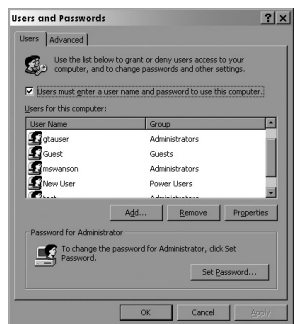
*General Tab*

Under the General tab, select Automatic in the STARTUP TYPE field (recommended). Click **Start Services**. Click **OK** to save and close Properties.



*Log On Tab*

Optionally, to set up a user identity and password for the GB-Commander Server, select **Start/Settings/Control Panel/User & Passwords** and enter the GB-Commander Server user identity information (Windows 2000).



*Users & Passwords*

## 9. How do I change the User Identity?

The 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 GB-Commander Service.
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.

## 10. I changed the IP address of my GB-Commander Server, and now an error message indicates that the client is no longer authorized to access the server.

To release the database to GB-Commander Server's new IP address, you must clear the gta\_options table using the Unlock feature in DBmanager. See Chapter 5 – Database Management.

---

## Event Viewer

The Windows Event Viewer, available under Windows in **Start/Settings/Control Panel/Administrative Tools/Event Viewer** allows the user to obtain information about the status of GB-Commander's events. This information can assist you in basic troubleshooting.

---

### Field Descriptions

---

Type	General description of event.
Date	Date when event was logged.
Time	Time when event was logged.
Source	Source of the logged event.
Category	Category of event.
Event	Event numbers defined in on-screen documentation.
User	Service user.
Computer	Name/Designation of computer.

---

# Appendix A Management Examples

---

## Introduction

The examples in this chapter describe setting up the account, providing appropriate permissions, setting up firewalls, creating users and setting up alarm emails. The examples cover four levels of administrative permissions within GB-Commander: an administrator with full permissions for the whole enterprise; a technician with permissions that allow access to specific firewalls within the enterprise; an administrator with full permissions to one section of the enterprise; and a user with viewing privileges only to one section of the enterprise. The examples assume that both GB-Commander Client and GB-Commander Server are installed on the same system.

---

## Great ISP Administrator

This example is for an ISP administrator with full permissions.

Great ISP is a fictional Internet Service Provider with two customers, Acme and Wickets, who will use GTA Firewall products to protect their networks. Acme wants to deploy its own firewalls and do most of its own firewall monitoring. Wickets, on the other hand, requires Great ISP to deploy its firewalls and provide management services.

In these examples, you will see how Great ISP can set up GB-Commander to monitor these two companies from one interface, allowing Acme to be involved in the monitoring process, while giving Wickets only viewing access. Only the Great ISP administrator will be able to see the whole enterprise.

After creating both a system and an email account, installing GB-Commander and directing the GTA Firewalls of both companies to the GB-Commander Server, Great ISP's administrator opens GB-Commander Client. All GTA Firewalls are in the Not Monitored group, and the Permissions Group contains the default ADMINISTRATORS group with one Administrator.

## Firewall Groups

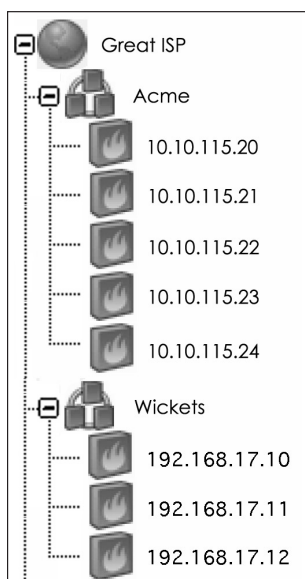
Great ISP's administrator must create a group for each company. To create a group, the administrator right-clicks on the Root, which is at the top left of the hierarchy, and selects **Add Group**. A new group will appear, below and to the right of the Root group.

The administrator names this group Acme by right-clicking on the group and selecting **Rename** from the menu. The administrator repeats this process to create the Wickets group.

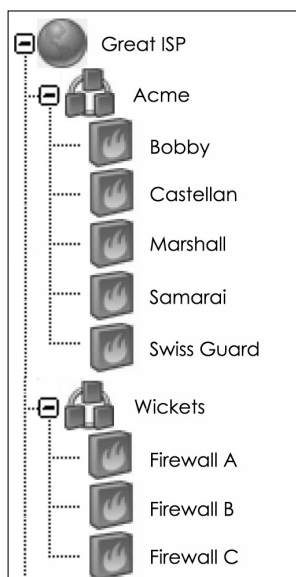
To add firewalls to each group, the administrator clicks on each GTA Firewall icon in the Not Monitored group and drags it to the correct company's group.

In the illustration below on the left, there are five GTA Firewalls in the Acme Group and three in the Wickets group, each represented by its IP address. By default, systems are represented by their IP addresses. To change to Logical Name view, go to the Main menu at the top of the page and select **View/Labels**.

In the illustration on the right, the administrator is viewing the firewalls in the hierarchy by the LOGICAL NAME used by Acme and Wickets. These names are arbitrary, and can be anything that helps identify the firewall system to the administrator and technicians.



*Groups viewed by IP Address*

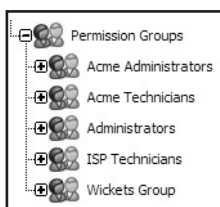


*Groups viewed by Logical Name*

## Permission Groups

Great ISP’s administrator must create Permission Groups for Great ISP technicians, for Acme administrators and technicians, and for the Wickets group.

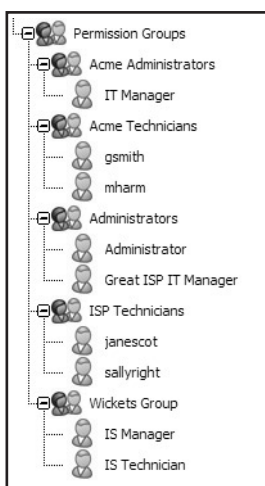
The administrator right-clicks on the Permission Groups and selects **Add Permission Group**. Once the group is added, the administrator renames the group “Acme Administrators.” The administrator can then add other permission groups.



*Permission Groups for Great ISP, Acme and Wickets*

## New Users

The administrator must now create users within each permission group. The administrator right-clicks on the group and selects **New User**, enters a name for the user and presses **<ENTER>**. Each user within a group will have the permissions of that group. The administrator must assign a password to each user. Passwords can be modified by right-clicking on the user and entering and confirming a new password.



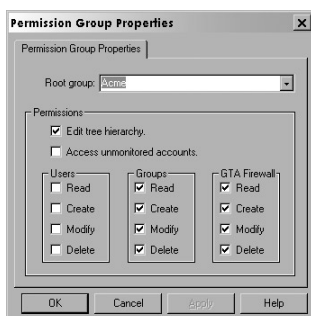
*Users for each group in Great ISP’s permissions groups*

## Permissions & Rules

After setting up the structure, the administrator begins to assign permissions to and make Alarm Rules for the groups and individual GTA Firewalls.

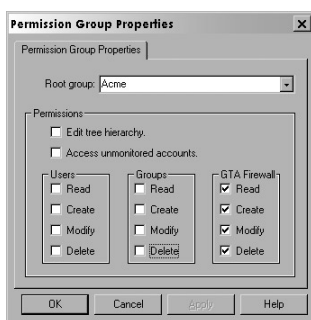
### Assign Permissions

To assign properties to each of the groups, the administrator right-clicks on the permission group and selects Properties. New permission groups have no permissions by default. For the Acme Administrators group, (note that this is not the default Administrators Group, which has all permissions selected), the Great ISP Administrator disallows: seeing or accessing the Not Monitored group; seeing, creating, modifying or deleting Users; and seeing the entire hierarchy (Acme is the Root); and allows (at the Acme level only): editing the tree hierarchy; seeing, creating, modifying and deleting Groups; and seeing, creating, modifying and deleting GTA Firewalls. To create these conditions, the administrator selects these permissions:



*Acme Administrator group permissions*

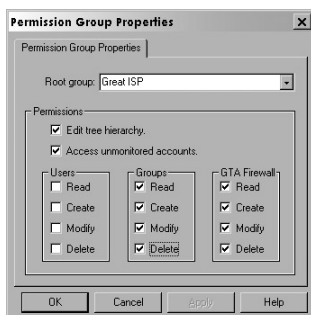
For Acme Technicians, the permissions are more restricted.



*Acme Technician permissions*

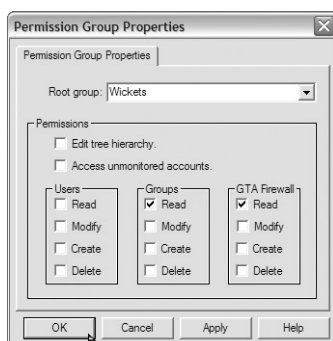


Great ISP's technicians can see the entire enterprise, edit the hierarchy and access GTA Firewalls in the Not Monitored group, but cannot see Users.



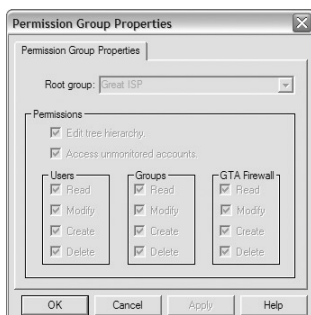
*Great ISP Technician permissions*

The Wickets group permissions are very restricted, as Wickets wants Great ISP to manage their firewalls.



*Wickets Group permissions*

All permissions are selected in the default Administrators Group, and the root group is the top-level root group. These properties cannot be changed.



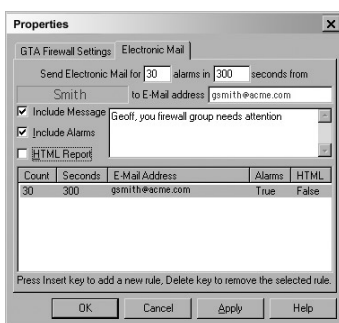
*Great ISP's Administrator group permissions*

## Alarm Email Rules

Next, the administrator adds Alarm Email rules. Generally, in these examples, Great ISP's administrator is sending emails to a local technician for a certain number of alarms in a specified time; to a Great ISP technician and an Acme IT Manager for a larger number of alarms in a specified time; and to himself, the administrator, for an even larger number of alarms in the specified time.

## Firewall Email Rules

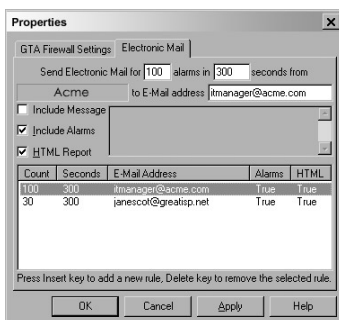
At the individual firewall level, Great ISP's administrator decides to send alarm notifications only to the technician in charge of that firewall. If the alarms were to be set the same for all firewalls within the group, this would be set up at the group level.



*Alarms notifications from IP address 10.10.115.20, logical name Samurai.*

## Group Alarm Email Rules

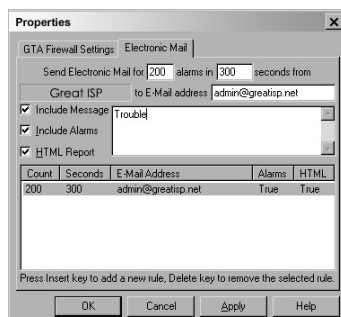
At the group level, Great ISP's administrator decides to send alarm notifications to Acme's IT Manager and to a technician at Great ISP in charge of that firewall. If the alarms were to be set the same for all firewalls in the hierarchy, this would be set up at Great ISP's Root level.



*Alarms notifications from any of the firewalls in the Acme Group.*

## Group Email Rules

At the Great ISP group level (the whole hierarchy), Great ISP's administrator decides to send alarm notifications to himself.



*Alarms notifications from any of the firewalls in the whole enterprise.*

Once the alarm email rules are set, the administrator is finished with the initial configuration of GB-Commander. The administrator may now begin monitoring alarm events, if desired. (See Chapter 3—Using GB-Commander.)

## Great ISP Technician

This example is for a technical user for the ISP with partial permissions.

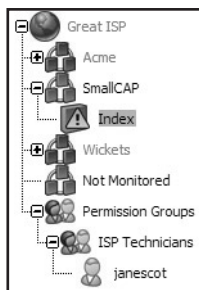
The Great ISP technician has access to all the firewalls and firewall groups in the hierarchy, but has access only to her own password in the Permission Groups.

After installation, the Great ISP technician opens GB-Commander Client and enters the user name and password provided by the administrator. The technician may now change the password given to her to sign into the system. Once it is changed, she must log on under the new password.

## Firewall Group

Great ISP's technician now must modify the hierarchy by creating a new group and moving a firewall into it from the Not Monitored group for a company that Great ISP will be monitoring. The firewall has already been directed to send information to the GB-Commander Server. The technician right-clicks on the Root at the top left of the hierarchy and selects **Add Group**. A new group appears, below and to the right of the Root. The technician names this group "SmallCAP" by right-clicking on the group and selecting **Rename**.

To add a GTA Firewall to the group, the technician clicks on the correct GTA Firewall icon in the Not Monitored group and drags it to the company's group. The technician gives the GTA Firewall the Logical Name used by SmallCAP to further identify it.

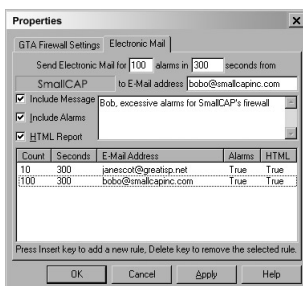


*New Group “SmallCAP” with a firewall added and renamed*

Permission groups and users for the new company will be added by the Great ISP administrator, who has exclusive access to this function.

## Alarm Email Rules

Next, the technician adds Alarm Email Rules. She needs only to create rules at the group level. The enterprise level rules will apply to the new group, and at the firewall level, there is only one firewall. She sets the alarm emails to herself and to SmallCAP's IS Manager, Bob Owens, at the group level.



*Alarm Email Rules for SmallCAP's Group*

The technician may now begin monitoring the alarm events for the firewalls and Groups for which she is responsible. (See Chapter 3—Using GB-Commander.)

---

## Acme IT Manager

This example is for an administrative user for a company within the ISP enterprise with full permissions at a secondary root level.

The Acme IT Manager has access to only the Acme portion of the hierarchy, and does not have access to either the Not Monitored group or the user permission groups.

After installation, the Acme IT Manager opens GB-Commander Client and enters the user name and password provided by the administrator. The Acme IT Manager can see the Acme Hierarchy (in which Acme is the Root), and has access only to his own password in the Permission Groups. The technician may now change the password given to him to sign into the system. Once it is changed, he must log on under the new password.

### Create Subgroup

Next, the Acme IT Manager creates a new subgroup of the Acme Hierarchy that will be monitored by a technician and moves three of the Acme Firewalls into it. In this way, he may set group Alarm Email Rules, rather than setting them individually for each GTA Firewall.

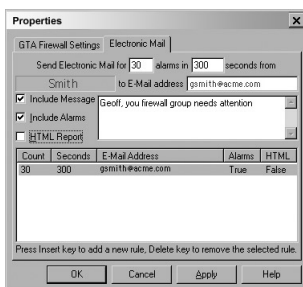
The Acme IT Manager right-clicks on the Acme root and selects **Add Group**. A new group will appear within the Acme group. The Acme IT Manager names this group “Smith” by right-clicking on the group and selecting **Rename**. To move a GTA Firewall to the group, the administrator clicks on the correct GTA Firewall icon and drags it to the new Smith group.

The firewalls are already set up, so all that is required is to modify the Smith group Alarm Email Rules. Permission groups and users will be added by the Great ISP administrator, who has exclusive access to this function in this example.

### Alarm Email Rules

Next, the Acme IT Manager adds Alarm Email Rules for the new Group. He needs only to create rules at the group level and modify or delete the repetitive rules at the firewall level as the Great ISP level rules will apply to the new Group.

He sets the alarm emails to go to the Acme technician in charge of the GTA Firewalls. There is no need for individual alarm email rules at the firewall level because both firewalls will be overseen by the same technician, so the Acme IT Manager deletes the GTA Firewall level Alarm Email Rules that are being sent to an Acme Technician.



*Alarm Email Rules for Acme's Smith Group*

The Acme Administrator may now begin monitoring alarm events, if desired.

## Wickets User

### **A User for a Company within the ISP Enterprise with Limited Permissions at a Secondary Root Level**

Any Wickets user has access to only the Wickets portion of the hierarchy, and does not have access to either the Not Monitored group or the users. He may not modify the hierarchy, or add or delete firewalls.

After installation, the Wickets user opens GB-Commander Client and enters the user name and password provided by the administrator. The Wickets user may now change the password given to him to sign into the system. Once it is changed, he must log on under the new password.

The Wickets user may not modify the hierarchy. The Wickets user has no access other than his own password to the Permissions group. The Great ISP administrator has exclusive access to this function.

The Wickets user does not have access to the Alarm Email Rules of the GTA Firewalls in the Wickets group.

The Wickets user may now begin monitoring the alarm events for the firewalls and groups for which he is responsible.

---

## Appendix B Charts & Reports

---

### Overview

GB-Commander database information can be used in both charts and reports. Data from a chart can be used to create a report and vice versa, therefore any of the 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 organize and display information gathered by content filtering. Internet Access Management reports are available to those with an optional Surf Sentinel subscription. You may request an evaluation version of Surf Sentinel from GTA's website at [www.gta.com](http://www.gta.com). For more information about obtaining a Surf Sentinel subscription, contact 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 percent 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.

**Acknowledged Alarms**

Reports acknowledged alarms, whom they were acknowledged by, the time and date they were acknowledged, and the alarm type by firewall serial number.

Input prompt	Date/time range.
Columns	Firewall (serial number), Acknowledged By, Acknowledgement Time, Alarm Type

**Unacknowledged Alarms by Source IP Address**

Reports the total number of unacknowledged alarms within the selected time range from each source IP address by firewall serial number.

Input prompt	Date/time range.
Columns	Firewall (serial number), Alarm Type, Source 1 and 2, Unacknowledged Alarms.

**Unacknowledged Alarms by Destination IP Address**

Reports the total number of unacknowledged alarms within the selected time range to each destination IP address by firewall serial number.

Input prompt	Date/time range.
Columns	Firewall (serial number), Alarm Type, Destination 1 and 2, Unacknowledged Alarms.

**Unacknowledged Alarms by Source Port**

Reports the total number of unacknowledged alarms within the selected time range from each source port by firewall serial number.

Input prompt	Date/time range.
Columns	Firewall (serial number), Alarm Type, Source Port 1 and 2, Unacknowledged Alarms.

**Unacknowledged Alarms by Destination Port**

Reports the total number of unacknowledged alarms within the selected time range from each source port by firewall serial number.

Input prompt	Date/time range.
Columns	Firewall (serial number), Alarm Type, Dest Port 1 and 2, Unacknowledged Alarms.

**Internet Access Management**

Internet Access Management Reports organize and display information gathered by content filtering. See the previous section about Internet Access Management Charts for more information.

**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 ; 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



## Index

### Symbols

\* 34

.csv, .doc, .html, .txt 35

### A

acknowledged alarm 31, 71, 72

alarm

clear 31

event 29

threshold 30

asterisk 34

attack 40

### B

back up

full 40

incremental 40, 41

browsers

Internet Explorer ii

### C

case-sensitive 12, 13

Change Chart/Report Title 36, 38

Chart Icon 33

column sizing 33

column sorting 33

Console interface 4

Content Filtering 4

conventions, documentation 3

CSV 35

### D

Database 45, 46

database maintenance 39–41

Data Source 45, 46

default

administrator 28

default setup 9

DOC 35

Documentation

additional 3

map 3

Drivers 4

Driver Setup 45, 46, 47, 48

DSN 31, 44

DSNs 8

### E

e-mail

Eudora 22

email address

support ii

Eudora 22

evaluation 5, 11, 33, 68

Event Viewer 54

export a file 34

### F

file format

csv 34

doc 34

html 34

txt 34

file output format 34

### G

GBAdmin 1, 4

GBAdmin interface 4

globe icon 17, 23

Graph Type 31

GTA Firewall

delete 28

GTA Firewall Admin 45, 46

GTA Support ii

### H

help ii

hierarchy 1

High Availability 4

horizontal bar chart 65, 66, 68

HTML 35

### I

icon

acknowledged alarm, yellow bell 18

firewall 18

firewall, non-communicating 18

firewall group 18

globe 17

mail symbol 18

new alarm, bell 18

permission group 18

Idle statistic 31

Internet Explorer ii

Interrupt 31

Isographic pie chart 36

## J

Java ii

## L

license 9, 12

Line Chart 36

lock files 41

lost license activation 51

## M

mail symbol 18

maintenance, database 39

Microsoft SQL Server 1, 8, 46–50

MSDE 1, 8

## N

note 4, 34

Not Monitored 27

No Connection 13

## O

ODBC 5

ODBC-compliant 1, 5, 8

ODBC driver 2, 8, 43, 52

Owner 9, 11

## P

password

    default 13

PDF 3, 4

port

    3306, MySQL 45

    514, GTAsyslog 6

    5432, PostgreSQL 46

Protected Network 6

PSN 6

purge/restore 40

## R

registration

    GTA Firewall 3

reinitialize database 41

removal instructions 13

repair database 41

Report Icon 33

right-click menus 33

Rooftop 36

root

    level 56

    secondary 63

root group 17, 27, 59

runtime

    version 18

## S

Serial Number 11

Server

    IP Address 23

Services applet 51, 52, 54

sizing columns 33

SMTP 2, 10, 21, 22

sorting 33

statistics 1

Support ii

System statistic 31

## T

TCP

    port

*number* 23

Technical Support ii

TXT 35

## U

unacknowledged alarm 71, 72

unique groups names 23

unlock database 41

URL 65, 69, 73, 74

User Name

    DSN 45, 46

User statistic 31

## V

Verification Code 11

Verify Installation in DBmanager 43

Vertical Bar 36

VPN 4

## W

Web chart 36

Web interface 4

WELF (WebTrends Enhanced Log  
Format) ii

Windows

    Event Viewer 54