

GE
Security

SecureStream IP Receiver and Operator's Software

installation & programming guide



imagination at work

Released August 2006

Copyright © GE Security Pty Ltd 2002
All Rights Reserved
Printed in Australia

GE and  are registered trademarks of the General Electric Company. Other product and company names herein may be the trademarks of their respective owners.

This publication may contain examples of screens and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual business enterprises and persons is entirely coincidental.

Disclaimer

The customer is responsible for testing and determining the suitability of this product for specific applications. In no event is GE Security Pty Ltd responsible or liable for any damages incurred by the buyer or any third party arising from its use, or their inability to use the product.

Due to ongoing product development, the contents of this manual can change without notice. We make every effort to ensure the accuracy of this manual. However, GE Security Pty Ltd assumes no responsibility for errors or omissions in this manual or their consequences. Please notify us if you find errors or omissions.

Contents

Acknowledgement	5
Introduction	5
What is SecureStream IP Receiver?	5
What is SecureStream IP?	5
SecureStream IP icons	7
Product overview: basic concepts	8
Using SecureStream IP.....	11
Logging in to SecureStream IP	11
Setting up SecureStream IP software	12
Adding the SecureStream IP Receiver IP address to the network	13
Working with configuration editor	15
Overview.....	15
Programming SecureStream IP	15
Working with the Details tab.....	16
Working with the Encryption Keys tab.....	17
Working with the Warning Events tab.....	19
Working with the Serial Comms Settings tabs.....	20
Working with the Monitoring tab	22
Working with the Panels Offline tab	22
Working with the TITAN IP Mapping tab	23
Working with the Application Status tab.....	24
Working with Challenger panels and the panel editor.....	25
Overview.....	25
How to find a Challenger panel record	28
How to set up a Challenger panel with the panel editor	29
Working with the panel editor	30
Working with the Ethernet tabs	33
Working with the security password	37
Working with the Communication tabs	38
Working with operators, qualifications (access rights) and features.....	39
Operator qualifications and features.....	39
How to create a qualification	40
How to edit an existing qualification and its features.....	40
How to add a new operator	41
How to change an operator password	44
Upgrading and re-installing SecureStream IP licenses	45
SecureStream IP license options	45
Checking your SecureStream IP license status	46
Upgrading or re-installing a SecureStream IP license.....	47
Reference topics.....	50
How to set up SecureStream IP Receiver	50

Connecting SecureStream IP to a central monitoring station.....	51
How to install SecureStream IP from the installation DVD.....	52
Connecting TITAN management software to SecureStream IP.....	55
Common Ademco CID error codes	57
Troubleshooting and technical support topics.....	58
Glossary.....	59
Index.....	61

Acknowledgement

We would like to acknowledge Dedicated Micro Systems' (DMS) contribution to the creation of this manual.

Introduction

What is SecureStream IP Receiver?

SecureStream IP Receiver is a computer that runs the SecureStream IP application, on the Linux operating system.

GE Security Pty. Ltd. (GE) provides SecureStream IP Receiver computers with SecureStream IP and Linux pre-installed.

The process of setting up a SecureStream IP Receiver is described in the Reference section. See *How to set up SecureStream IP Receiver* on page 50.

What is SecureStream IP?

Overview

SecureStream IP:

- Is an Internet protocol (IP) alarm receiver designed for the Challenger panel alarm network.
- Collects alarm events from Challenger panels and converts these into the Ademco Contact ID (CID) format, and then sends the CID events to monitoring station software, e.g., MasterMinder, SIMS, etc.
- Allows new Challenger panels to be added to an IP network by automatically adding (enrolling) their basic details to its database.
- Runs on a server (SecureStream IP Receiver) connected to the same IP network as the Challenger panels it monitors.
- Runs on the Linux operating system.

Functions

SecureStream IP performs a range of functions including:

- Receives Challenger panel events.
- Converts Challenger events to Ademco CID format.
- Exports CID events to an external monitoring station.
- Manages Challenger network encryption.
- Creates and maintains a database of Challenger panels and settings.
- Polls Challenger panels to determine panel availability and network integrity.
- Provides full-function backup and disaster recovery to other SecureStream IP Receivers on the same network.

Compatible hardware and software for SecureStream IP

SecureStream IP software can be used with:

- TS0898 Ethernet Interface.
- Third party monitoring station software such as MasterMinder.
- ARES management software, version 4.5 or later.
- Forcefield management software (all versions).
- TITAN management software (TITAN Single User, version 1.06.31 or later), when TITAN is connected to a serial port on a SecureStream IP Receiver.
- TS2000 Network Master Receiver

Typical system layout diagrams

Figure 1 is a basic system layout with three SecureStream IP Receivers (management software is not present.) The optional second and third SecureStream IP Receivers can be connected anywhere on the WAN/LAN.

Figure 2 is a basic system layout with three SecureStream IP Receivers (ARES or Forcefield management software is also present.) The optional second and third SecureStream IP Receivers can be connected anywhere on the WAN/LAN.

Figure 3 is a basic system layout with three SecureStream IP Receivers (TITAN management software is also present.) The optional second and third SecureStream IP Receivers can be connected anywhere on the WAN/LAN.

In the following diagrams:

- **SecureStream IP Receiver** translates Challenger events into CID event format that the monitoring station software understands. SecureStream IP Receiver transmits CID events via serial connection to the central monitoring station computer. A SecureStream IP Receiver doesn't have to be located at the central monitoring station, it could be elsewhere (via serial connection).
- **TS0898 Ethernet Interface** enables a Challenger panel to send events via LAN/WAN.
- **TS2000 Network Master Receiver** provides a PSTN backup for events if a panel cannot communicate with any SecureStream IP Receiver.
- Optional — Each Challenger panel can have different SecureStream IP Receivers designated as main, backup, and disaster.
- Optional — Use a pair of TS0894 RS232 to RS485 Interfaces for long-distance serial connection, if needed.

Figure 1: Main, backup, and disaster SecureStream IP Receivers connected via IP to Challenger panels. No management software is used in this example.

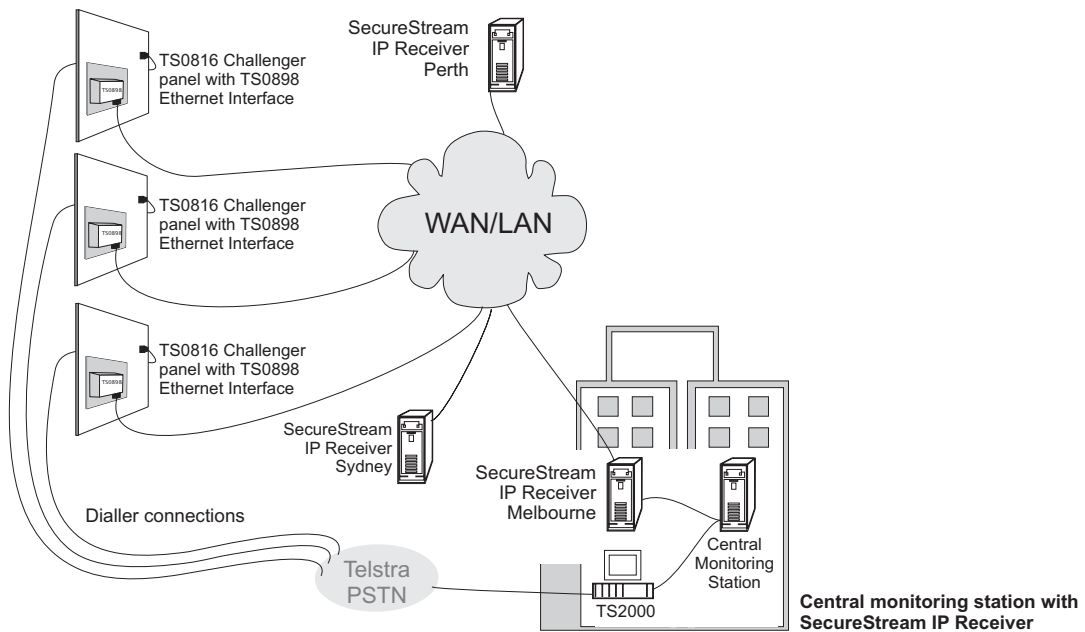


Figure 2: Main, backup, and disaster SecureStream IP Receivers connected via IP to Challenger panels and to ARES or Forcefield management software.

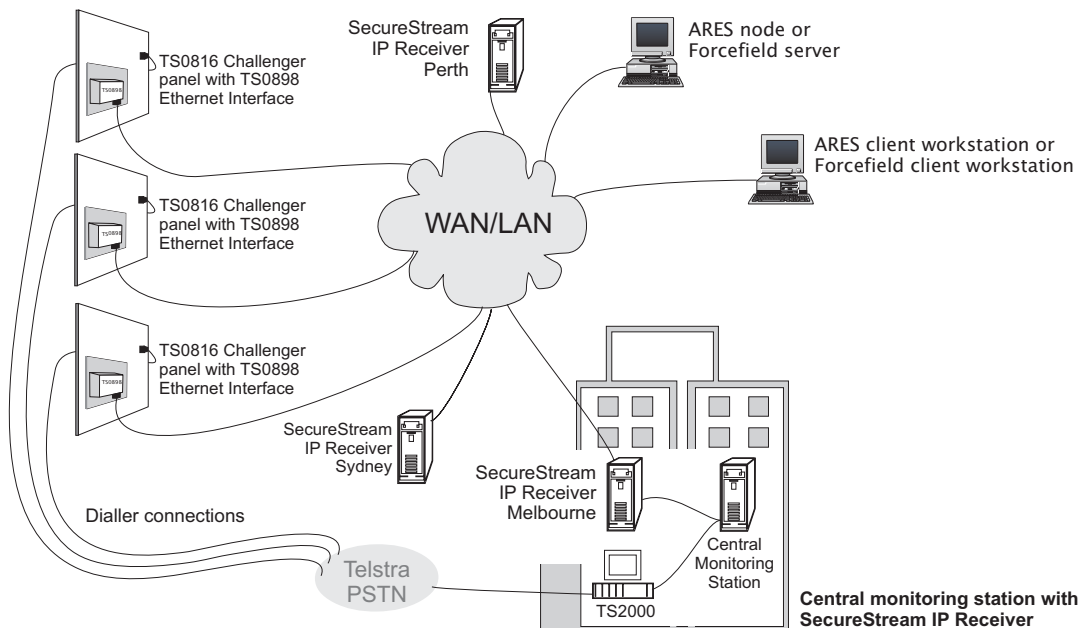
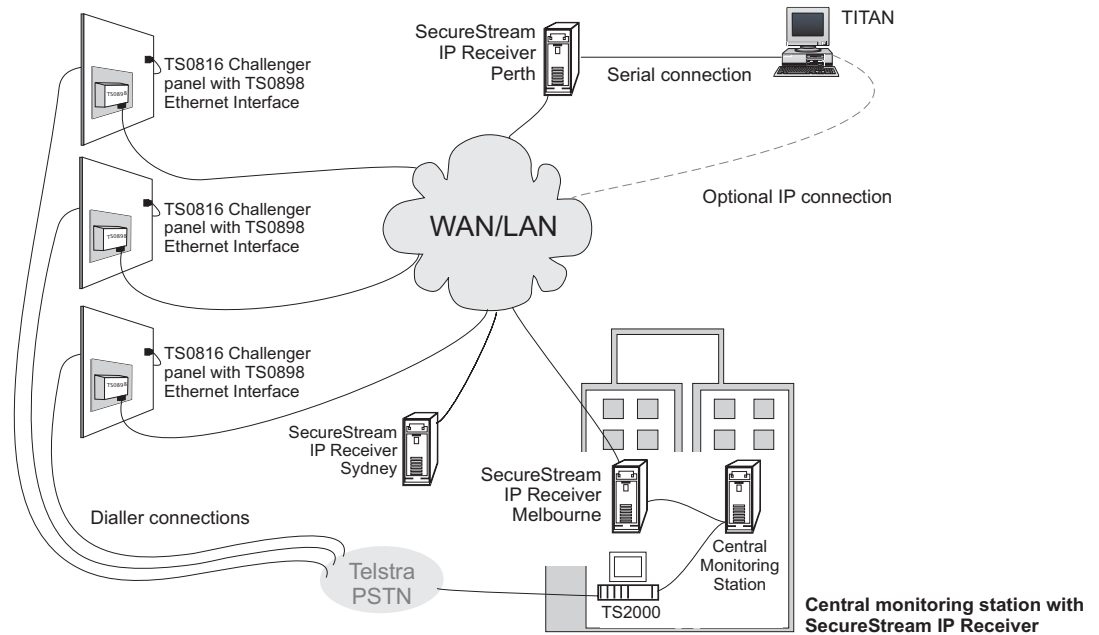


Figure 3: Main, backup, and disaster SecureStream IP Receivers connected via IP to Challenger panels and to TITAN management software.



SecureStream IP icons

Table 1 lists the SecureStream IP navigation icons. Table 2 lists the SecureStream IP database record tree icons.

Navigation icon	Description
	New record Create a new panel or operator record. Can only be used with the <i>Finder</i> (see below).
	Save Save changes on any screen. If you forget to click this, your changes will be lost.
	Remove Remove the current operator, panel or application record.
	Show tree Display the database record tree.
	Hide tree Hide the database record tree.
	Browser Launch the Help browser.
	Logoff Log the operator off SecureStream IP.
	What's this Click this icon and then click the item on which you want help.
	Finder Locate and open a Challenger panel or an operator record. Once found, panels or operators can be added, edited, or deleted.
	Resources Create and edit qualifications (pre-defined access rights) for operators.
	Edit records Edit individual records for panels and operators, but only when a record has been opened with the <i>Finder</i> .
	Configuration editor Start the configuration editor to configure SecureStream IP's global settings e.g., default encryption.
	Sysmon Diagnose SecureStream IP networking (technician use only).

Navigation icon		Description
	Honeycomb	Network overview tool.

Table 1: SecureStream IP navigation icons. Navigation icons display their names when you place the cursor over them.

Database record tree icon		Description
	Parcel	Storage area for SecureStream IP's database tables. Click the + box to expand the tree. A parcel appears in blue if it contains unsaved changes.
	Folder	Storage area for sets of common data (parcels). Click the – box to collapse an expanded tree.

Table 2: SecureStream IP database record tree icons

Product overview: basic concepts

Purpose of SecureStream IP software

SecureStream IP software converts Challenger events sent over a LAN or WAN into serial CID format. It is faster at sending events than TS2000 Network Master Receiver, and eliminates leased line costs.

Once translated into CID, SecureStream IP sends the events to a third-party software package at the monitoring station for alarm event reporting and management.

We **strongly recommend** that encryption in SecureStream IP is enabled, and only trusted personnel have access to the Encryption Keys.

Maximum Challenger panels

The maximum number of Challenger panels supported by SecureStream IP depends on the particular license purchased (see *SecureStream IP license options* on page 45).

SecureStream IP Receivers

Each Challenger panel can communicate with up to three SecureStream IP Receivers (main, backup, and disaster). Three SecureStream IP licenses are required in such a configuration.

CID defined

CID (Ademco Contact ID) is an alarm event code format.

Support for specific CID event codes may differ between monitoring companies.

Auto-enrolment

When SecureStream IP detects communication from a correctly-configured Challenger panel on the network at an IP address that is not in its database, SecureStream IP attempts to add the panel to its database by enrolling it.

Using ARES or Forcefield management software

If ARES or Forcefield management software is used, basic panel details such as IP and computer addresses are first entered at each Challenger via an LCD RAS keypad. Other options such as encryption are programmed using the management software, and then downloaded to the panels.

SecureStream IP auto-enrols the panel's Ethernet configuration.

Using TITAN management software

When TITAN management software (TITAN Single User, version 1.06.31 or later) is connected to SecureStream IP, TITAN can be used to:

- Upload and store the database for various Challenger panels.
- Modify and download the database for each Challenger panel.
- Control areas and check the status of a particular Challenger panel. (If network commands set to 'Yes' in Communications option 9 in the Challenger Installer menu.)

Note: TITAN won't receive events from Challenger panels when TITAN is connected to SecureStream IP.

Basic requirements for auto-enrolment of Challengers

SecureStream IP's basic requirements for Challenger auto-enrolment are:

- Each Challenger panel has a unique, static IP address.
- IP addresses for at least one SecureStream IP Receiver must be programmed in the Challenger. If the Challenger panel is reporting to separate main, backup, and disaster SecureStream IP Receivers, then the IP addresses for SecureStream IP Receivers 1, 2, and 3 must be programmed in the Challenger.
- The Heartbeat timeout and event acknowledgement (ack) timeout must be programmed.

These options are programmed via an LCD RAS keypad on the Challenger's LAN (see the *TS0898 Ethernet Interface Installation and Programming Guide* for details). After initial programming, other options can be programmed via management software.

Event acknowledgement basics

How does third-party monitoring station software acknowledge events sent by Challenger via SecureStream IP software? When Challenger sends an event to SecureStream IP, SecureStream IP passes the event to the third-party monitoring station software, which then sends an acknowledgement (ack) to SecureStream IP, which in turn sends an acknowledgement to the Challenger panel.

Once the Challenger panel receives this acknowledgement, the original event is deleted from the Challenger communications (comms) buffer. If the third-party monitoring station software doesn't acknowledge the event within the timeout time, Challenger assumes that SecureStream IP Receiver 1 is unavailable.

SecureStream IP does not queue messages internally. It does end-to-end acknowledgement between the monitoring station and Challenger on a panel-by-panel basis so that a message cannot be lost if the SecureStream IP computer crashes.

Heartbeat defined

Heartbeat is used to describe a special data transmission sent at user-programmable intervals by SecureStream IP to enrolled Challenger panels to check that the connections are active. A heartbeat failure indicates to SecureStream IP that the Challenger is offline.

Event retry mechanism overview

The retry mechanism works as follows:

1. Challenger attempts to communicate with SecureStream IP Receiver 1 (main).
2. If SecureStream IP Receiver 1 isn't accessible (due to a faulty link or faulty SecureStream IP Receiver), Challenger tries three more times.
3. After three unsuccessful retries, Challenger attempts to communicate with SecureStream IP Receiver 2 (backup).
4. If SecureStream IP Receiver 2 isn't accessible, Challenger tries one more time.
5. After one unsuccessful retry, Challenger attempts to communicate with SecureStream IP Receiver 3 (disaster).
6. If SecureStream IP Receiver 3 isn't accessible, Challenger tries one more time.
7. After one unsuccessful retry, Challenger uses its dialler backup.

Each time Challenger reports an error to any other SecureStream IP or dialler, other than SecureStream IP Receiver 1, Challenger will also poll SecureStream IP Receiver 1 to check if SecureStream IP Receiver 1 is alive (up).

Uploading and downloading data

Downloading and **uploading** are terms for sending data to and from Challenger panels. SecureStream IP allows some data in the panel editor fields to be downloaded to, or uploaded from a panel — but this depends on whether management software is present:

- When management software is present, then only uploading from a panel to SecureStream IP is possible (uploading requires the encryption key details to match at both ends). Downloading data to a panel is not possible.
- When management software is **not** present, then both uploading and downloading are possible (uploading requires the encryption key details to match at both ends).

Working with multiple SecureStream IP Receivers

Each Challenger panel can send IP event traffic to up to three SecureStream IP Receivers, designated as main, backup, and disaster roles.

The reason we refer to a Challenger panel and 'its' main SecureStream IP Receiver or 'its' backup SecureStream IP Receiver is that there can be several SecureStream IP Receivers on a network, and any SecureStream IP Receiver can fill one of the three possible roles for any Challenger panel.

One SecureStream IP Receiver is not necessarily designated as the main SecureStream IP Receiver for an entire Challenger network, because a particular SecureStream IP Receiver can simultaneously be the main SecureStream IP Receiver for one or more Challenger panels, and the backup or disaster SecureStream IP Receiver for other Challenger panels in the same system.

IP addresses of main, backup, and disaster SecureStream IP Receivers are programmed via the management software or via the Challenger's RAS keypad (not via SecureStream IP).

Table 3 describes the main, backup, and disaster roles of SecureStream IP Receiver.

Role	Function
Main	The Challenger will send all events to this SecureStream IP Receiver unless the SecureStream IP Receiver doesn't acknowledge the receipt of an event. An event sent to a main SecureStream IP Receiver that isn't acknowledged indicates to a Challenger that its main SecureStream IP Receiver is unavailable for some reason. After three retries the Challenger immediately reroutes all unacknowledged events and new events to its backup SecureStream IP Receiver, including a CID event code indicating that the main SecureStream IP Receiver is offline. Refer to <i>Common Ademco CID error codes</i> on page 57 for details.
Backup	This is the SecureStream IP Receiver that the Challenger panel sends events to if its main SecureStream IP Receiver is unavailable. The Challenger will continue to send events to its backup SecureStream IP Receiver until its main SecureStream IP Receiver sends a poll to the Challenger indicating it is online. If the Challenger's backup SecureStream IP becomes unavailable, the Challenger immediately reroutes all unacknowledged events and new events to its Disaster SecureStream IP, including an event indicating its backup SecureStream IP is offline.
Disaster	This is the SecureStream IP that the Challenger panel sends events to if its main and backup SecureStream IP Receivers are unavailable. The Challenger will continue to send events to its Disaster SecureStream IP Receiver until its main or backup SecureStream IP Receiver sends a poll to the Challenger to indicate the main or backup SecureStream IP Receiver is online. The main SecureStream IP Receiver is the preferred unit, and the Challenger will always send events to the main SecureStream IP Receiver if it is available. If the Disaster SecureStream IP Receiver becomes unavailable, the Challenger reroutes all unacknowledged events and new events to its dialler receiver, including an event indicating its Disaster SecureStream IP Receiver is offline.

Table 3: Main, backup, and disaster roles of SecureStream IP Receiver

Main, backup, and disaster roles are configured in the Challenger Installer menu 47. Each SecureStream IP Receiver's role is nominated by entering its IP address. See the previous section and the *TS0898 Ethernet Interface Installation and Programming Guide* for more details on programming the Challenger CID station via RAS.

Example:

CID station 1 IP: 201.107.008.025 = Main

CID station 2 IP: 201.107.008.036 = Backup

CID station 3 IP: 208.126.192.002 = Disaster

Using SecureStream IP

Logging in to SecureStream IP

SecureStream IP software is installed on a SecureStream IP Receiver, which runs a Linux operating system. To log into SecureStream, you must first log on to Linux as described below.

Use the following process to log on to SecureStream IP.

Step	Instructions
1	Start the PC. Linux will go through a lengthy system check.
2	When you see the login screen, type the administrator login ID root and the default password tecom4346 . Refer to the Linux help files for information on changing Linux passwords if required.
3	<i>When the SecureStream IP login screen displays (see Figure 4), click the Login button, and then type the Login/operator ID (master is the default) and the password (4346 is the default).</i>
4	When the SecureStream IP start screen displays (see Figure 5), select the icon required from the icons at the left of the screen. See <i>SecureStream IP icons</i> on page 7 for more information.

Figure 4: SecureStream IP login screen

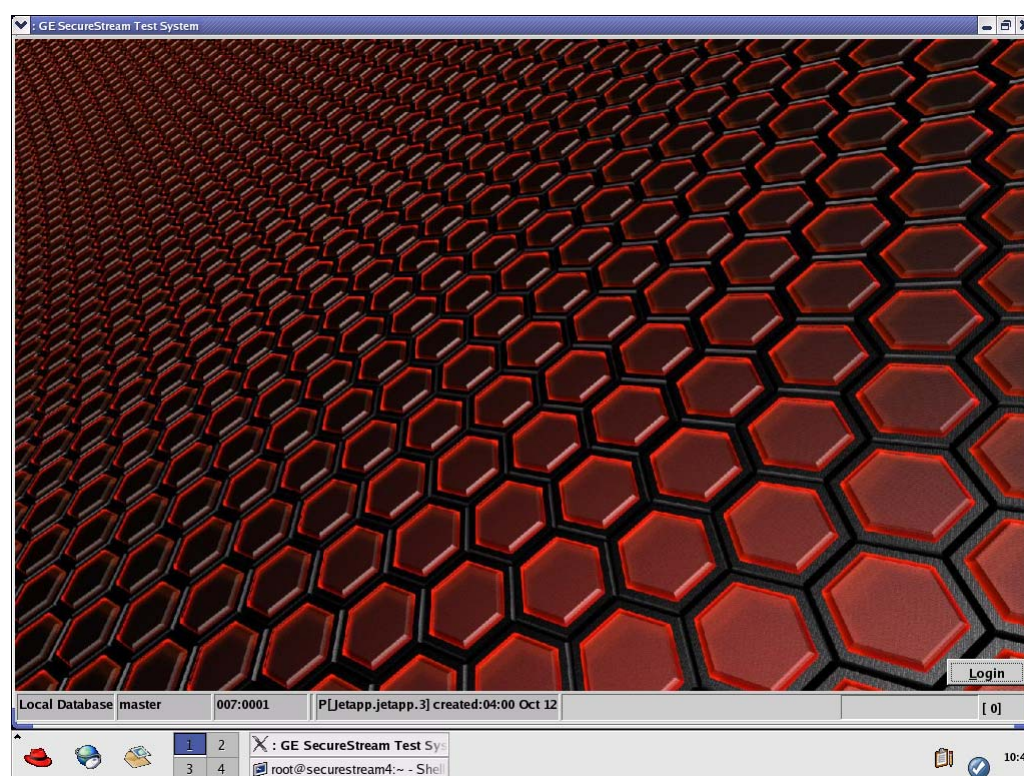
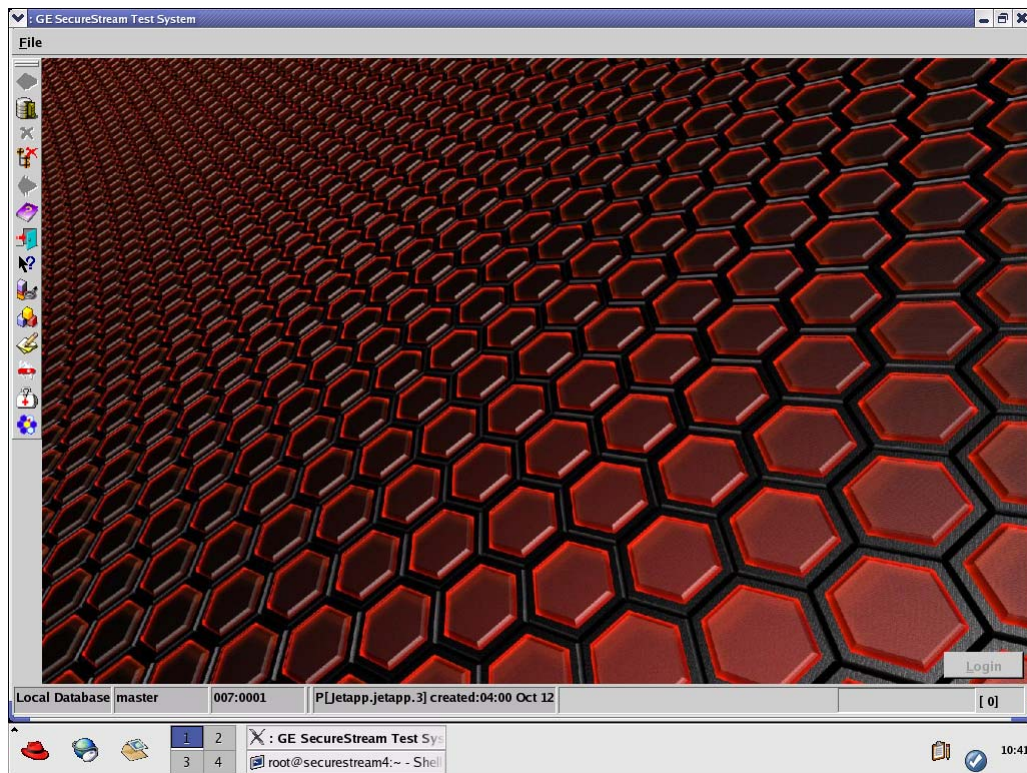


Figure 5: SecureStream IP start screen



Setting up SecureStream IP software

This procedure assumes that the following are successfully installed and configured:

- Challenger panel(s) with TS0898 Ethernet Interfaces installed.
- One or more SecureStream IP Receivers.
- The central monitoring station software.
- Suitable management software.

Trained Installation Technicians may use the following overall process to set up SecureStream IP software.

Step	Instructions
1	Configure the Challenger panels for event-driven mode (i.e. UDP/IP mode). See the <i>TS0898 Ethernet Interface Installation and Programming Guide</i> for details.
2	If ARES or Forcefield management software is present, set up the IP configuration for SecureStream IP Receiver and the panels for your network.
3	Change the network address in Linux (using the Network configuration editor) for the SecureStream IP Receiver.
4	Use the SecureStream IP configuration editor to set up various global options related to various SecureStream IP Challenger panels.
5	Set up SecureStream IP operators' qualifications (i.e., access rights).
6	Add SecureStream IP operators, give them passwords, and assign qualifications to them.
7	Check that the panels in the system are online and the monitoring station is receiving CID events.
8	Set up any Challenger panels using management software.
9	Resolve any problems with offline panels, such as incorrect host names.

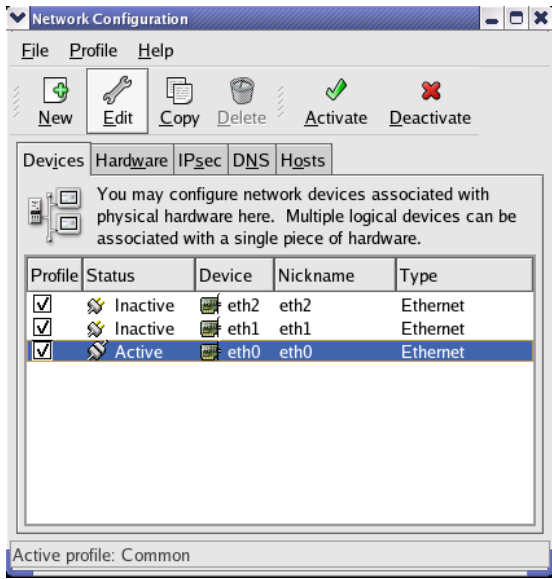
Step	Instructions
10	If reinstalling, register SecureStream IP licenses.
11	Set up encryption if required.

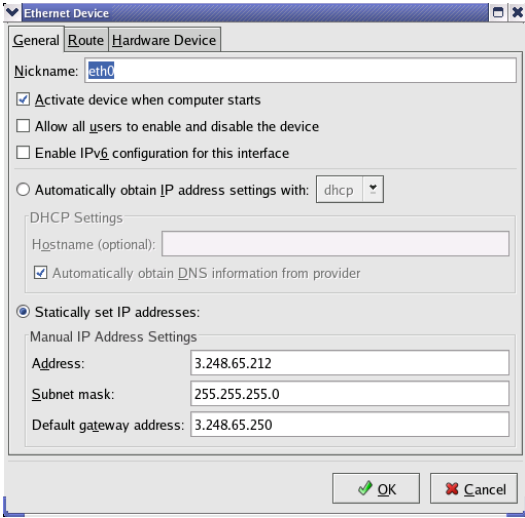
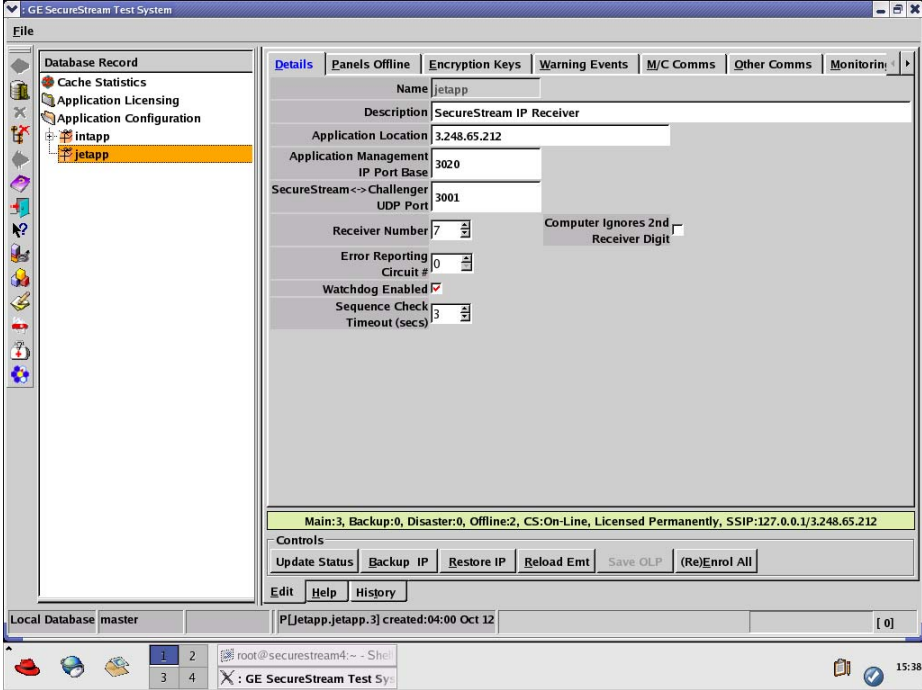
Adding the SecureStream IP Receiver IP address to the network

Before you can start configuring SecureStream IP, you'll need to modify the IP address of the SecureStream IP Receiver to suit the particular network. A system administrator will have the local site details.

This procedure assumes Linux is already installed. (See the help files on the Linux installation CD-ROMs.)

Trained Installation Technicians may use the following process to add the SecureStream IP Receiver to Linux.

Step	Instructions
1	From the KDE desktop, start the Network Administration tool. 
2	On the Devices tab, select eth0 and click Edit . 

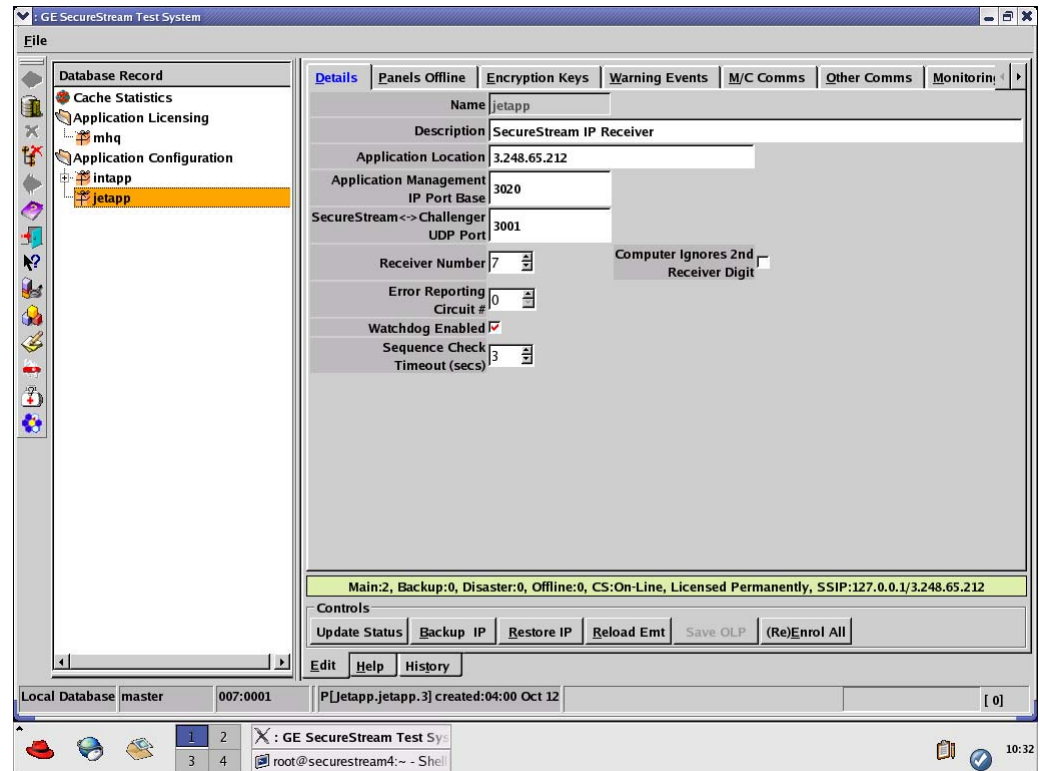
Step	Instructions
3	Type the IP address of the SecureStream IP, the subnet mask, and the default gateway address. Select 'Activate device when computer starts'.  Note: you must use a static IP address.
4	Click OK , and then select File > Save .
5	Restart the SecureStream IP Receiver computer.
6	Log into SecureStream IP with the administrator's password.
7	Click the Configuration editor icon (see Table 1).
8	In the configuration editor double-click the Application Configuration folder, and then select jetapp. The Details tab lists "SecureStream IP Receiver" in the Description field. 
9	Type the SecureStream IP Receiver's IP address in the Application Location field.
10	Click the Save icon.

Working with configuration editor

Overview

SecureStream IP's 'Jetapp' configuration editor affects the global software and hardware settings of SecureStream IP, and how SecureStream IP handles the data received from the Challenger panels. This section discusses how to use the 'Jetapp' configuration editor to set up or interpret the data in each tab (or screen) area.

Figure 6: Jetapp configuration editor, Details tab



Programming SecureStream IP

For SecureStream IP to communicate and work with Challenger panels, a series of configuration details must be entered in the tabs of the configuration editor.

When using SecureStream IP for the first time, work your way from the configuration editor Details tab on the left to the Other Comms tab on the right. Each of the configuration editor tabs and their options are described in the following pages. Some fields are mandatory and some are optional.

The tabs: Panels Offline, Monitoring, TITAN IP Mapping, Application Status, Cache and About require no input.

Trained Installation Technicians may use the Jetapp configuration editor.

Step	Instructions
1	Log on to SecureStream IP.
2	Click the Configuration editor icon (see Table 1).
3	Double-click the Application Configuration folder.
4	Double-click Jetapp parcel to display the configuration editor tabs: Details, Panels Offline, Encryption Keys, etc.
5	Enter configuration details as described in the following pages.
6	Once the details are entered, press the Save icon to save the configuration details.

Working with the Details tab

The Details tab is the first tab in the configuration editor

Trained Installation Technicians may complete the fields in the *Details* tab.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Optional — In the Description field, type a description as you wish it to appear in the Applications folder list.
3	In the SecureStream IP <-> Challenger port field, Type a number for the IP port SecureStream IP 'listens' for event traffic from Challenger panels on the network. This must match the 'TCP/IP Port Number' setting in Installer menu 47 on the Challenger. The default setting is 3001 .
4	In the Application Management IP Port Base field, type a port number for the IP port SecureStream IP listens to for commands from the GUI applications. The default is 3020 .
5	In the Receiver Number field, type a number from 0-99 (supplied by the monitoring station staff) to set the first two digits of the address part of the CID message. The monitoring computer uses the receiver number to identify this SecureStream IP Receiver, and to differentiate between other SecureStream IP Receivers if multiple receiver units are used. If the Monitoring computer only uses the first of these two digits to identify the receiver, also check the Computer Ignores 2nd Receiver Digit check box.
6	In the Error Reporting Circuit # field, type the circuit number that identifies the SecureStream IP to the monitoring station when the SecureStream must report things about its internal operation (e.g. IP license expired). Use a four-digit number supplied by the monitoring station staff.
7	Check the Watchdog enabled option if you want the backup SecureStream IP Receiver to change its heartbeat rate to the main SecureStream IP Receiver heartbeat rate if the main SecureStream IP fails.
8	In the Sequence Check Timeout field, enter the number of seconds a backup or disaster SecureStream IP Receiver should wait to receive clarification from its immediate superior SecureStream IP Receiver of an out-of-sequence event before generating an 'Out Of Sequence' alarm.
9	Click the (Re)Enrol button at the base of the details tab if the max silence/heartbeat details for a panel have been changed in management software to ensure the details in SecureStream IP match. Controls Update Status Backup IP Restore IP Reload Emt Save OLP (Re)Enrol All
10	Optional backup functions: Update Status refreshes any live data on the page. Backup IP saves SecureStream IP's Challenger database, including the IP address, security password, encryption key and computer address to a file on a floppy disk. Note that SecureStream IP is continuously updating a hard disk-based copy of this data which it will use to automatically rebuild its database in the event of a catastrophe (e.g. the SQL database is deleted). You can use Backup IP as a safety precaution to back up a Challenger database, or to transfer a Challenger database from one SecureStream IP Receiver to another. (Caution! Make sure you restore the correct Challenger database, as the restore function <i>overwrites</i> the Challenger database on the SecureStream IP Receiver to which you restore the file). Restore IP. Click the Restore IP button to copy a Challenger database from the disk to restore or overwrite a Challenger database to a SecureStream IP Receiver.
11	Click the Save icon.

Working with the Encryption Keys tab

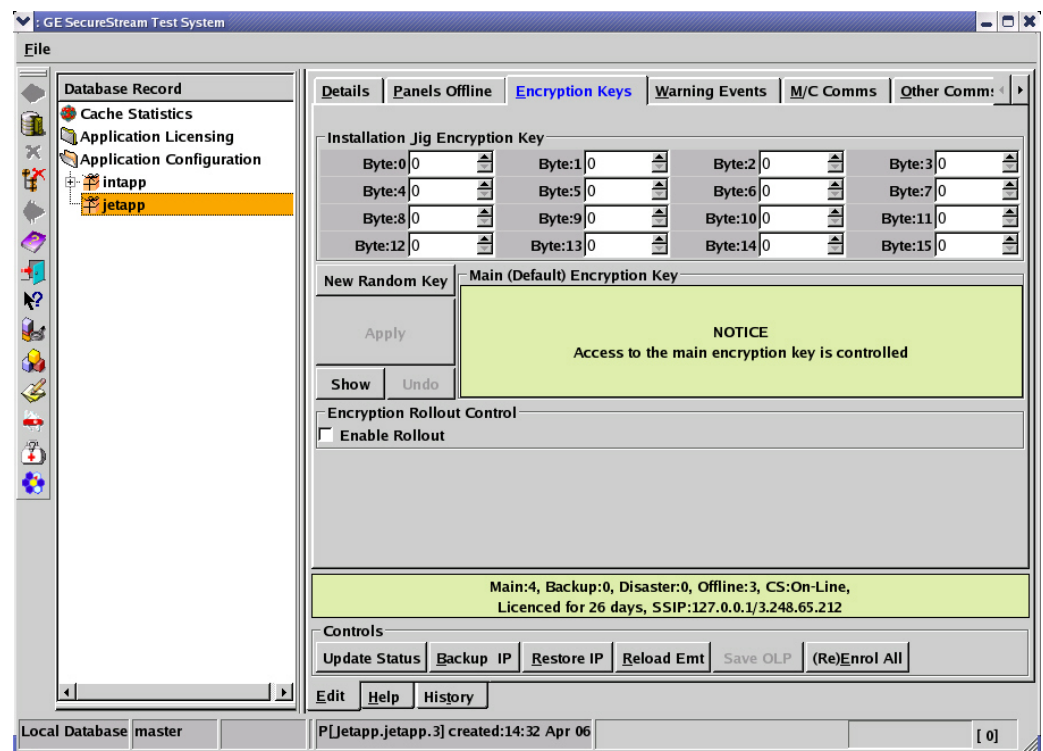
The Encryption Keys tab stores the default encryption key. This tab has no other function apart from a storage role when SecureStream IP is used in conjunction with management software. To simplify administration, all or most of the Challengers on a network can use this default encryption key as a template.

When no management software is present, the key can be copied from here to individual panels using the *Load With Default Key* button in the panel editor, panel by panel (see Figure 20 on page 34).

When management software is present, the encryption key is entered into the management software and downloaded to the panels. The key must (at least) then be typed into the **Installation Jig Encryption Key** fields for each panel to reflect the changes. Alternatively, you can create a random key.

TIP: We recommend you do not apply encryption until all panels are working and the monitoring station is receiving events. All fields should be set to 0.

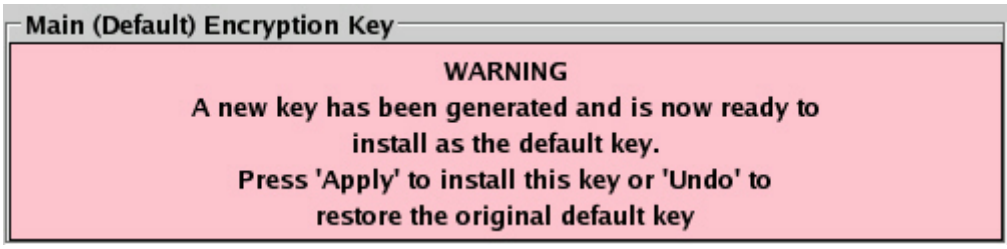
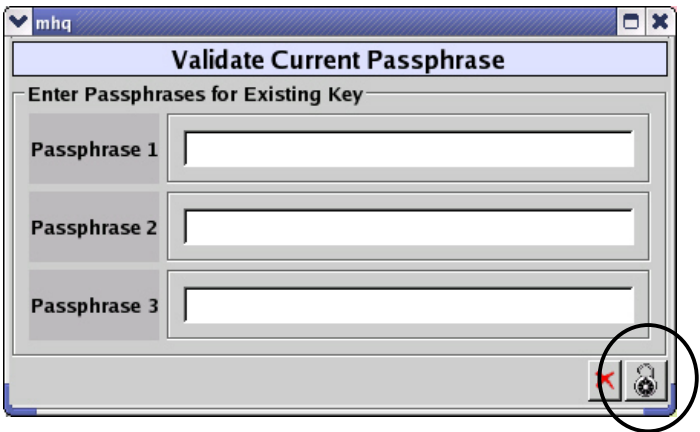
Figure 7: Jetapp configuration editor, Encryption Keys tab



Trained Installation Technicians may set up the default encryption key. The following steps assume that passphrases have not been previously programmed.

NOTE: The precise order of the steps will change depending on the choices made. The following steps are only a guide.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Select the Encryption Keys tab (see Figure 7).
3	Click the Show button to display spin boxes for the Main (Default) Encryption key. The Validate Current Passphrase dialogue box displays (see step 5).

Step	Instructions
4	Use the spin boxes to set the encryption key numbers (bytes) from 0-255. Alternatively, click New Random Key to create a random key. A warning message displays. 
5	Click Apply to install the key. The Validate Current Passphrase dialogue box displays. The order that this dialogue box appears depends on whether you used the Show button or the New Random Key button. 
6	Since passphrases have not yet been programmed, leave all fields blank, and then click the padlock button (circled).
7	The Enter New Passphrase dialogue box displays. 
8	Type at least one passphrase and then retype it in the Again field. A blue check button displays at the bottom right of the dialogue box.
9	When all passphrases have been entered (twice), click the blue check button. WARNING: Once committed, the new key will only be accessible to you using the passphrases you just entered. You will only be able to change the key using the passphrases that you just entered.
10	The Enter New Passphrase dialogue box closes. Your new Default Encryption Key can now be used as the encryption key for each panel.

Working with the Warning Events tab

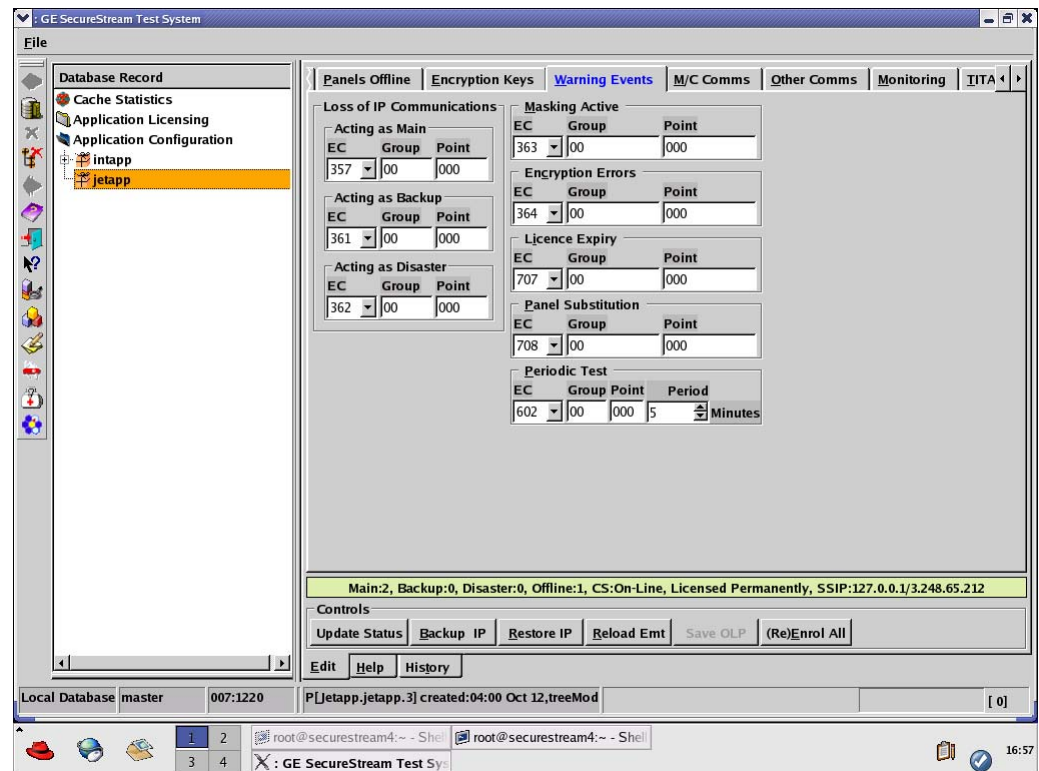
The Warning Events tab allows you to change the CID message code for different types of warning event. This is a global setting and can't be set for individual Challenger panels.

The monitoring company usually provides the CID message codes used to report these states. Codes differ between some companies. Normally there's no need to change the defaults. See *Common Ademco CID error codes* on page 57 for CID code explanations.

Each CID message code field has three parts:

- **EC** — Event Category code of the CID message
- **Group** — Group Number (the area in the Challenger)
- **Point** — Point Number (the input, DGP or RAS)

Figure 8: Jetapp configuration editor, Warning Events tab



Trained Installation Technicians may program CID message code for different types of warning events.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Select the Warning Events tab (see Figure 8).
3	Type an event code in the Loss of IP Communications field. If SecureStream IP doesn't receive any communication from a Challenger panel within the required period, SecureStream IP sends this CID alarm message to a monitoring station. SecureStream IP Receiver will send one of three event types, depending on whether it is acting as main, backup, or disaster with respect to the panel. SecureStream IP sends a 'restore' event to the monitoring station when the panel resumes communication with this SecureStream IP Receiver. The <i>Panels Offline</i> tab will list any offline Challenger panels.

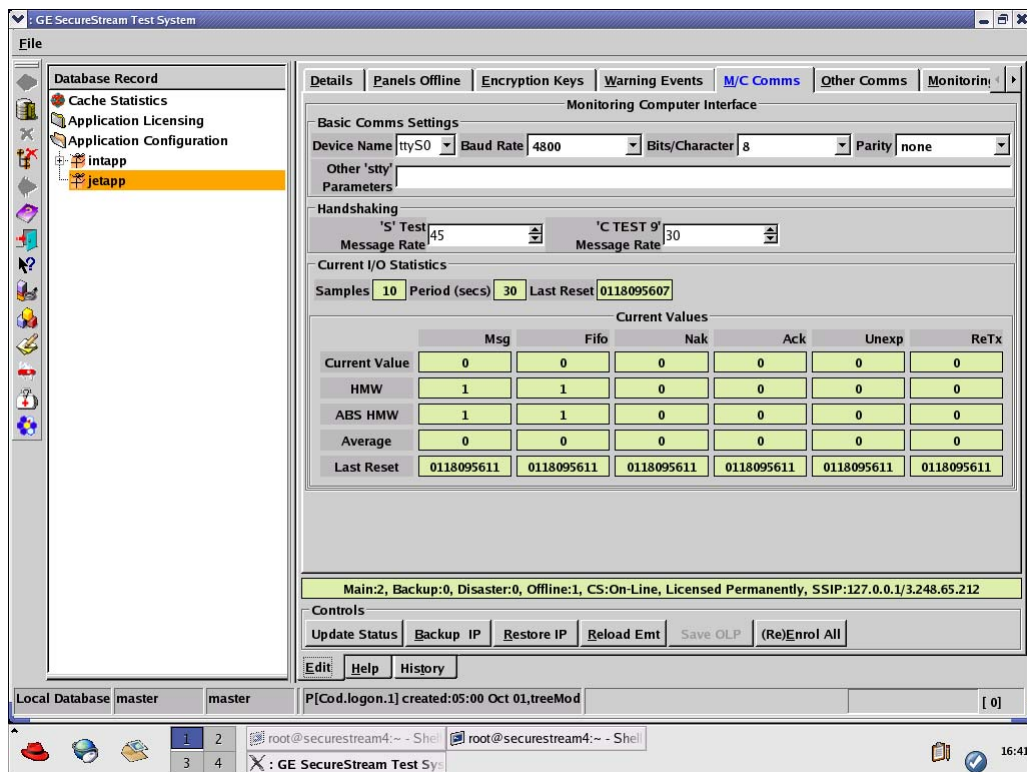
Step	Instructions
4	Type an event code in the Masking Active field. The transfer of events from a panel to the monitoring station can be disabled in the <i>Live Session Control</i> tab of the Panel Editor. Disabling the transfer of events from a panel is called 'Masking'. SecureStream IP sends a CID alarm message to the monitoring station when masking is set to 'Active'. SecureStream IP sends a 'Restore' event to the monitoring station if masking is removed or expires.
5	Type an event code in the Encryption Errors fields. If SecureStream IP receives from a panel any events that can't be decoded, it sends a CID alarm message to the monitoring station. SecureStream IP sends a 'Restore' event to the monitoring station when SecureStream IP is able to successfully decode a message from the Challenger panel.
6	Type an event code in the License Expiry field. If SecureStream IP's license is in its 30-day grace period, SecureStream IP sends a CID alarm message to the monitoring station every two hours. The CID Point number holds the unlicensed library's number. After 30 days, SecureStream IP stops sending events apart from the license expiry message.
7	Type an event code in the Panel Substitution field. If SecureStream IP detects a panel has been substituted it sends a CID alarm message to the monitoring station.
8	Click the Save icon.

Working with the Serial Comms Settings tabs

The M/C Comms (Monitoring Computer Comms) and *Other Comms* tabs are used to record the serial port communications settings for various asynchronous serial links to and from the SecureStream IP Receiver.

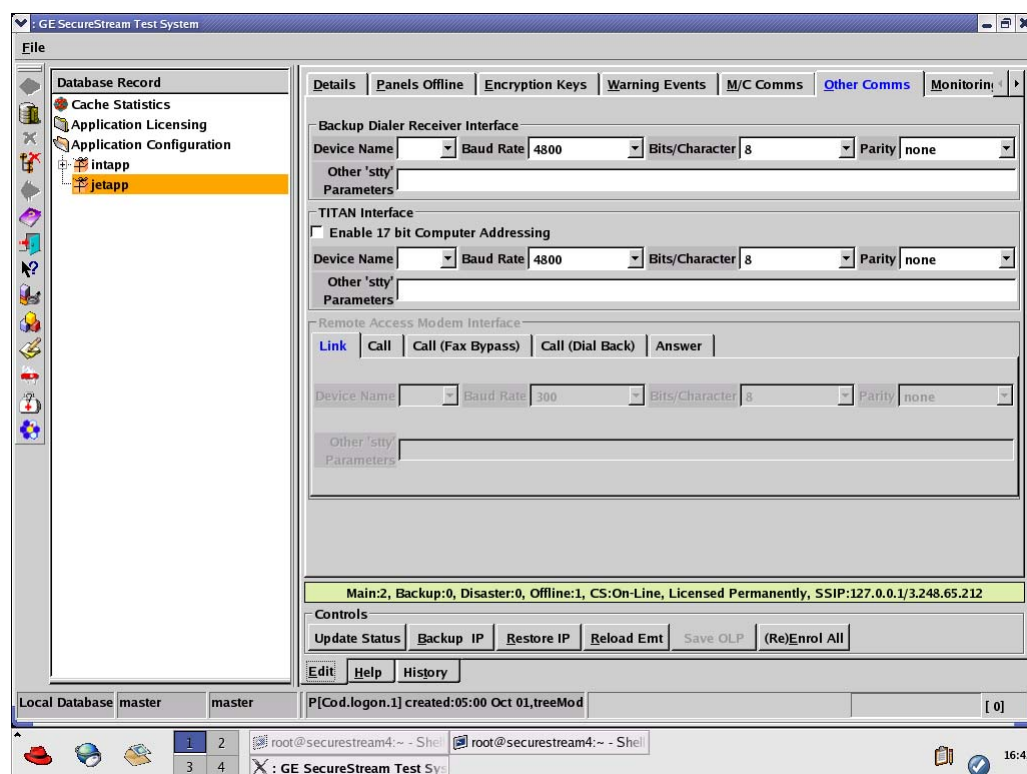
Tip: Serial ports are also referred to as serial interfaces.

Figure 9: Jetapp configuration editor, M/C Comms tab



Basic Comms Settings are used to send CID events produced by SecureStream IP to the monitoring station.

Figure 10: Jetapp configuration editor, Other Comms tab



Two other types of serial port interfaces can be set up here:

- **Backup Dialer Receiver:** Receives CID events from the Challenger network's Backup Dialer Receiver e.g., TS2000. SecureStream IP logs the events as it sends them to the monitoring computer. MasterMinder software can also be installed on the SecureStream IP Receiver, and this port can be used for the dialer backup to report its events to the monitoring station. This can only be used when MasterMinder software is installed on the same computer, and the TS2000 is connected.
- **TITAN:** Used by the TITAN software to send configuration settings to Challenger panels.

Configure each interface (or port) as described below.

Trained Installation Technicians may set up the details for serial interfaces.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Select the M/C Comms tab (see Figure 9).
3	Set the ' S Test Message Rate'. The range is 0-600 seconds. The 'S' test is a poll from the monitoring station to SecureStream IP Receiver to check line integrity. For example, select the value '1' to send one poll every second, or select the value '2' to send a one poll every two seconds.
4	Set the ' C Test 9' Message Rate'. This is the poll rate between the monitoring station and SecureStream IP. The range is 0-600 seconds. For example, select the value '1' to poll every second, or select the value '2' to poll every two seconds.
5	In the Monitoring Computer Interface section, from the dropdown list, select the device name for the monitoring computer interface. Type the Baud rate , Bits/Char and Parity as required.
6	Click the Save icon.
7	Select the Other Comms tab (see Figure 10).

Step	Instructions
8	Used only with MasterMinder monitoring software. In the Backup Dialler Receiver Interface section, from the dropdown list, select the device name for the backup dialler receiver interface. Type the Baud Rate, Bits/Character, and Parity .
9	In the TITAN Interface section, from the dropdown list select the device name for the TITAN serial port. Type the Baud rate, Bits/ Character, and Parity as required. Leave the 17 Bit Computer Addressing button unchecked.
10	Click the Save icon.

Note about “Other ‘stty’ Parameters” fields — In exceptional circumstances you may need to change other serial settings. This field accepts serial port configuration parameters in Linux stty format. Consult the Linux manual for more information on stty command options.

Working with the Monitoring tab

The Monitoring tab shows which monitoring stations are allocated as main, backup, and disaster when using MasterMinder monitoring software.

As proprietary software, (produced by DMS, Melbourne) MasterMinder supports transmission of CID events over an IP network. Consult your MasterMinder manual for further details on how to configure this tab.

Tip: The tab lists host names representing the MasterMinder server IP addresses.

Figure 11: Jetapp configuration editor, Monitoring tab

Working with the Panels Offline tab

The Panels Offline tab lists of the panels SecureStream IP has enrolled in its database but can't currently communicate with and considers offline.

No details can be entered or edited here.

Figure 12: Jetapp configuration editor, Panels Offline tab

Panels With Outstanding Issues						
IP Address	Circuit	Description	Last Rx	Role	Session	Reason Listed
203.8.124.26	009:0001	Auto-asserted (by me again)		main	IpUp	No Comms

Table 4 describes the Panels Offline tab contents.

Column title	Function
IP Address	IP address of the offline panel.
Time of Last Rx	The time and date of the last time anything was received from the listed IP address
Role	The role that this SecureStream IP Receiver fulfils for the offline panel. (Main, Backup or Disaster)
Session State:	The current state of the Challenger panel. (Challup, lpup).
Reason listed	Why the Challenger panel is listed (Unlicensed, No Comms, Clock).

Table 4: Panel Offline column headings

Users may view the Panels Offline tab.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Select the Panels Offline tab (see Figure 12).

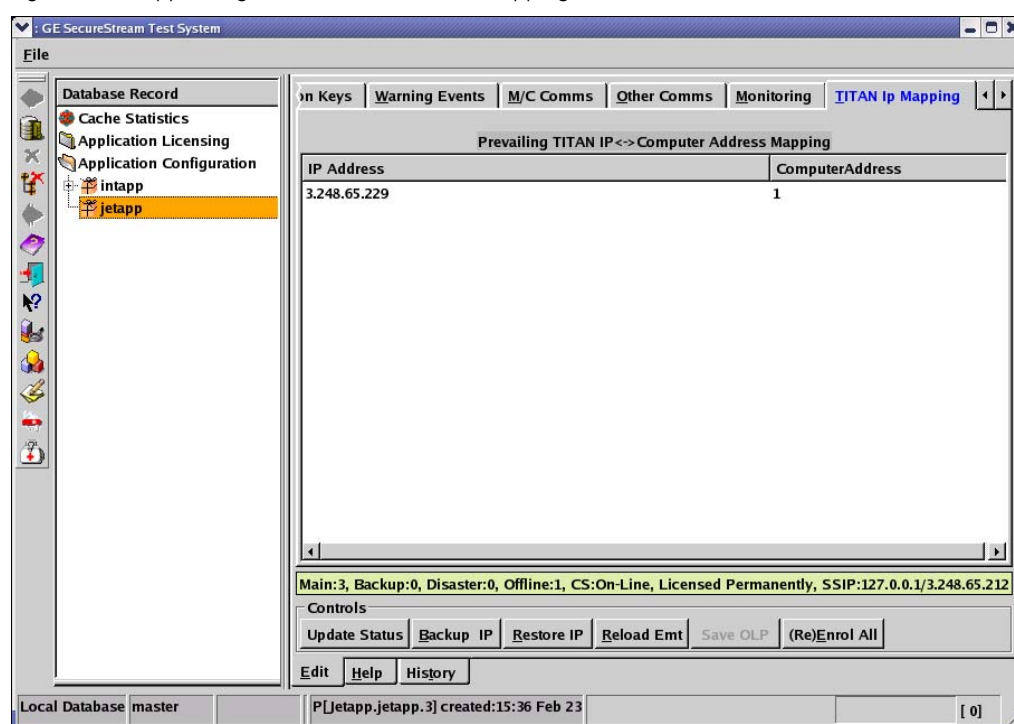
Working with the TITAN IP Mapping tab

The TITAN IP Mapping tab lists the IP addresses (e.g. 203.14.64.03) and computer addresses (e.g. 4, 10, etc.) of any active Challenger panel controlled by TITAN management software.

The TITAN computer must already be connected to the SecureStream IP Receiver for this information to appear. See *Connecting TITAN management software to SecureStream IP* on page 55 for more information.

No details can be entered here.

Figure 13: Jetapp configuration editor, TITAN IP Mapping tab



Users may view the TITAN IP Mapping tab.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Select the <i>TITAN IP Mapping</i> tab (see Figure 13).

Working with the Application Status tab

The Application Status tab in the configuration editor, gives an overview of the status of SecureStream IP. No details can be entered or edited here.

Figure 14: Jetapp configuration editor, Application Status tab

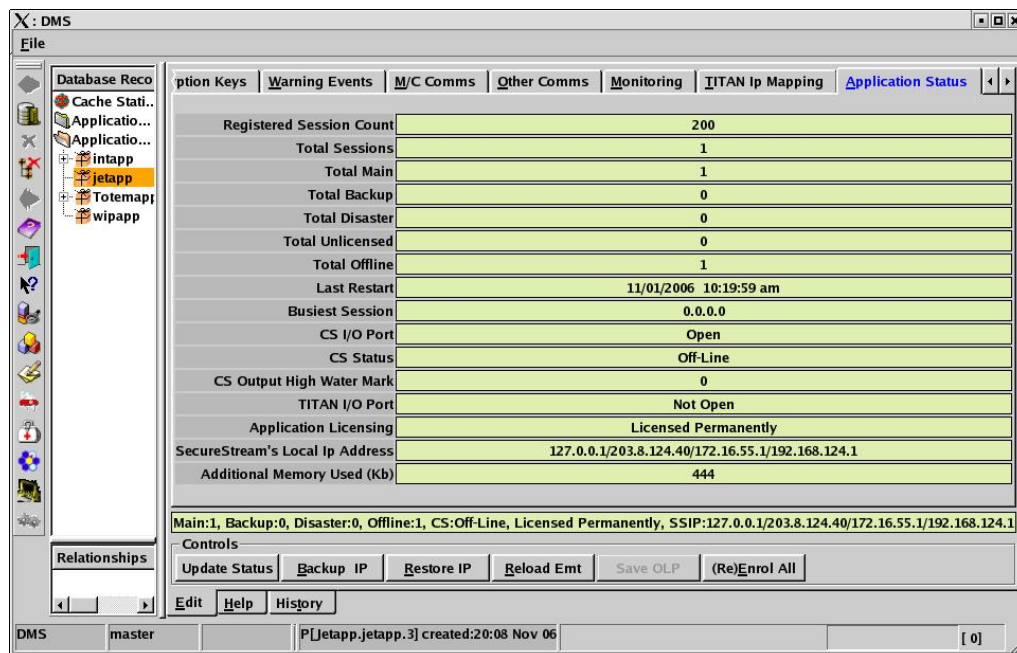


Table 5 describes the Application Status tab data.

Table 5: Application Status tab data

Field	Function
Registered Session Count	The total number of licensed Challenger sessions available.
Total Sessions	Total number of Challenger sessions in use.
Total Main	The total number of panels in the database that consider this SecureStream IP Receiver to be designated as 'main'.
Total Backup	Total number of panels in the database that consider this SecureStream IP Receiver to be designated as 'backup'.
Total Disaster	Total number of panels in the database that consider this SecureStream IP Receiver to be designated as 'disaster'.
Total Unlicensed	The total number of unlicensed panels in the database.
Total Offline	Total number of panels listed as 'Offline'.
Last Restart	Date and time of last SecureStream IP Receiver restart.
Busiest Session	IP address of the Challenger panel that created the most event traffic over the most recent ten-minute accounting period.
CS I/O port	Central Station (Computer) port status (Open/Not Open).
CS Status	Central Station link status (On/Off line)
CS Output High Water Mark	The quantity of Challenger panels waiting to remove message(s) from their buffers. Messages cannot be removed until the monitoring computer acknowledges its currently outstanding message.
TITAN I/O port	Port status. Open or closed.
Monitoring Computer	Monitoring station link status. Online or offline.
Application licensing	Licensed, unlicensed or number of days left of the 30-day grace period.
SecureStream's local IP Addresses	IP address of this SecureStream IP Receiver.

Field	Function
Additional Memory Used (KB)	Kilobytes of memory used to handle all IP sessions.

Users may view the Application Status tab.

Step	Instructions
1	Open the configuration editor as described in <i>Overview</i> on page 15.
2	Select the Application Status tab (see Figure 14).

Working with Challenger panels and the panel editor

Overview

Challenger panels and SecureStream IP

The Challenger Version 8 (V8) panel reports the state of points (an active input, DGP or RAS) and areas to an alarm monitoring station. The panel supports both IP and dialler event transmission.

The Challenger panel reports events to an Internet protocol (IP) alarm receiver (SecureStream IP Receiver) using the dialler as a backup if IP transmission fails.

The SecureStream IP Receiver and dialler receivers forward panel events in standard Ademco CID format to an alarm monitoring station.

For Challenger panels to communicate and work correctly with SecureStream IP software, the panel must be configured correctly (see the *TS0898 Ethernet Interface Installation and Programming Guide* for details).

Challenger panel auto-enrolment

When SecureStream IP Receiver is first connected, SecureStream IP automatically looks for and auto-enrols any available and correctly configured Challenger panel — unless something goes wrong. This section describes how auto-enrolment works. When the correct configuration settings are entered in Challenger or in the management software, the auto-enrolment sequence below occurs.

The auto-enrolment sequence is as follows:

Stage	Description
1	Once the installer enters the Challenger's configuration settings, the panel will try to send queued events to the SecureStream IP Receiver that is designated as 'main'.
2	SecureStream IP checks its database for the IP address of the Challenger from which it has just received the events. If the address isn't found, SecureStream IP creates a new record for that IP address using default parameters.

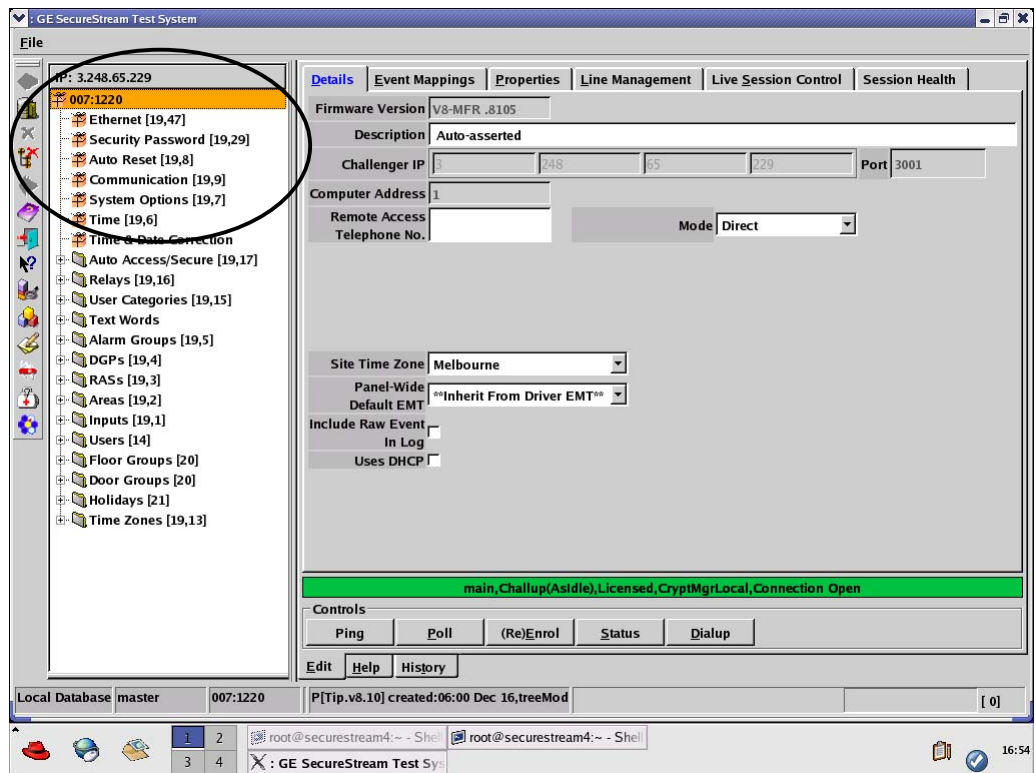
Stage	Description
3	Then, one of the following occurs: a) If the encryption set at the panel matches the encryption set at SecureStream IP, and SecureStream IP can read the events, the panel's computer address (Challenger Installer menu 9) and other parameters, are read and stored in the database. SecureStream IP sends acknowledgements to the panel for all events received. b) If no encryption is set, and SecureStream IP can read the events, the panel's computer address (Challenger Installer menu 9) and other parameters are read and stored in the database. SecureStream IP sends acknowledgements to the panel for all events received. c) If SecureStream IP <i>can't</i> read the events, e.g., when encryption key is incorrect, the computer address of the new record is set to '0000' and an error message is displayed in SecureStream IP when that Challenger's record is edited. This message displays: 
4	If SecureStream IP has successfully read the initial events from Challenger (as in points a or b), SecureStream IP immediately forwards CID events to the alarm monitoring station.

Panel Editor

The panel editor allows you to configure individual Challenger panels. SecureStream IP is designed to auto-enrol many of the details when a correctly-configured panel is added to the system.

SecureStream IP can send or receive data (upload or download data), depending on the presence or absence of management software. The options for uploading and downloading data are described in the following pages.

Figure 15: Note the parcel images on left (circled)



The panel editor has four main sections, accessed via 'parcels' (see Table 2). Each parcel's editor has one or more tabs (or screens) listed in Table 6. Click each parcel once to display its editor and associated tabs.

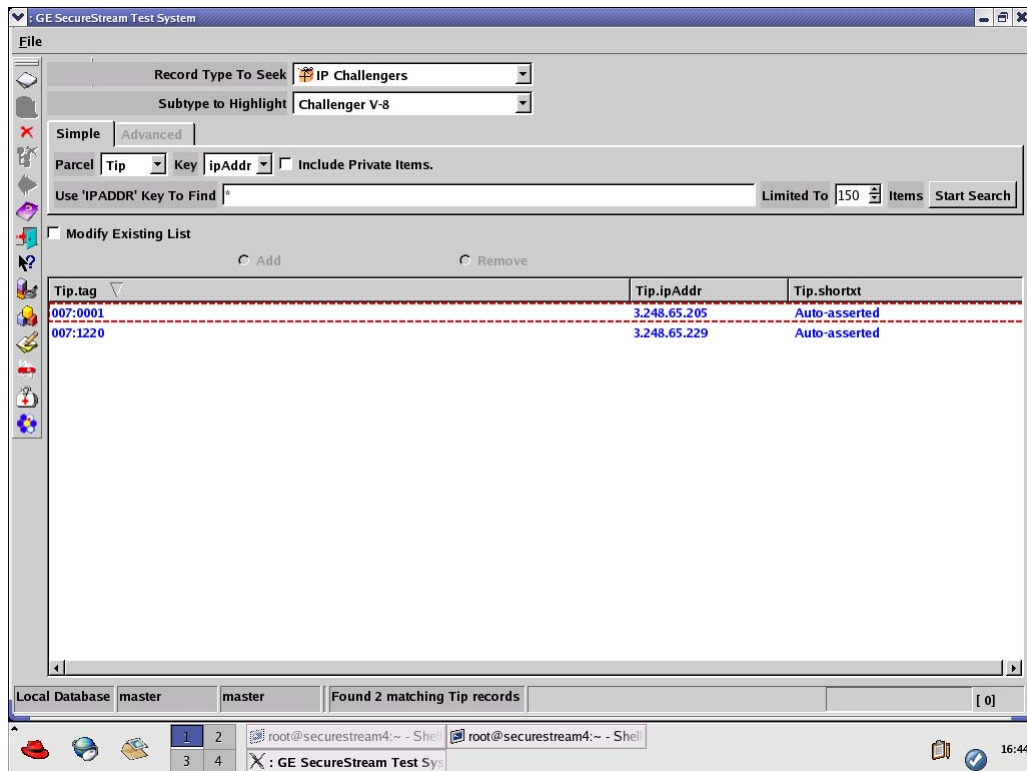
Field or Parcel name	Panel editor tabs
Panel IP Address	- Details - Event Mapping - Properties - Line Management (not used) - Live Session Control - Session Health
Ethernet (19, 47)	- IP Information - Encryption Key - IP Timeouts
Security Password (19, 29)	Remotely Programmable Device Settings
Communication (19, 9)	- Telephone Numbers - General Control - Miscellaneous - Area Reporting

Table 6: Panel Editor tabs for each selected parcel

How to find a Challenger panel record

SecureStream IP lists all Challengers panels via the Finder. To work with a specific Challenger panel, use the **Finder** to locate a panel, and then open the record for that panel.

Figure 16: Finding a Challenger panel



Use the **Finder** icon to find a Challenger panel.

Step	Instructions
1	Click the Finder icon (see Table 1).
2	Click the <i>Record Type To Seek</i> arrow and select 'IP Challengers'.
3	Click the <i>Subtype To Highlight</i> d arrow and select 'Challenger V-8'.
4	Click the <i>Key</i> arrow and select the type of data that you want to search. The example depicted in Figure 16 above uses the ipAddr key, and so will be used in the following steps.
5	Type a keyword (such as part of an IP address) for the panel in the Use 'IPADDR' Key To Find field, and then click Start Search to search for the keyword . Alternatively, type an asterisk '*' in the Use 'IPADDR' Key To Find field, and then click Start Search to search for all records. The asterisk may be added to a keyword to perform wildcard searches.
6	This will display a list of all of the IP Challengers in the database that are found by the search, highlighting all entries whose type is 'Challenger V8' by displaying them with blue text.
7	Double-click the panel you want to check or edit to display the panel editor for that panel.
8	See <i>How to set up a Challenger panel with the panel editor</i> on page 29 for further details.

How to set up a Challenger panel with the panel editor

Auto-enrolment: Once you've selected the panel you wish to work with, the panel editor allows you to edit the panel's details. Note that if newly-added Challenger panels have been properly configured, SecureStream IP auto-enrolment will automatically populate many of the panel's data fields.

Table 7 lists the details that are automatically populated. Data fields that are not automatically populated must be programmed via one of the following means, as appropriate:

- An LCD RAS keypad on the Challenger's LAN
- Management software
- SecureStream IP

Uploading and downloading: In a system where several combinations of hardware and software are possible, rules control the uploading and downloading of data between Challenger panels, management software and SecureStream IP. These are summarised further in this topic.

Table 7 summarises auto-enrolment for Challenger panels.

Panel parcel name	Parcel tab (or screen) name	Auto-enrolment?	Notes
Panel IP address (or name)	Details	Yes	Automatically populates the IP address and computer address.
	Event Mappings	No	—
	Properties	No	—
	Line Management	Yes	Not currently used.
	Live Session Control	No	—
Ethernet	Details	Yes	—
	Encryption Key (local)	No	Enter via management software and download to the panel. Without management software, enter via SecureStream IP and download to panel. The Encryption Key can only be uploaded if the device requesting the key knows the current key.
	IP Timeouts	Yes	—
Communication	Details	Yes	Enter via a RAS, management software, or via SecureStream IP if no management software is present.
	Telephone numbers	Yes	Enter via a RAS, management software, or via SecureStream IP if no management software is present.
	General control	Yes	Enter via a RAS, management software, or via SecureStream IP if no management software is present.
	Miscellaneous	Yes	Enter via a RAS, management software, or via SecureStream IP if no management software is present.
	Area Reporting	Yes	Enter via a RAS, management software, or via SecureStream IP if no management software is present.

Table 7: Challenger auto-enrolment

Working with the panel editor

Communication controls

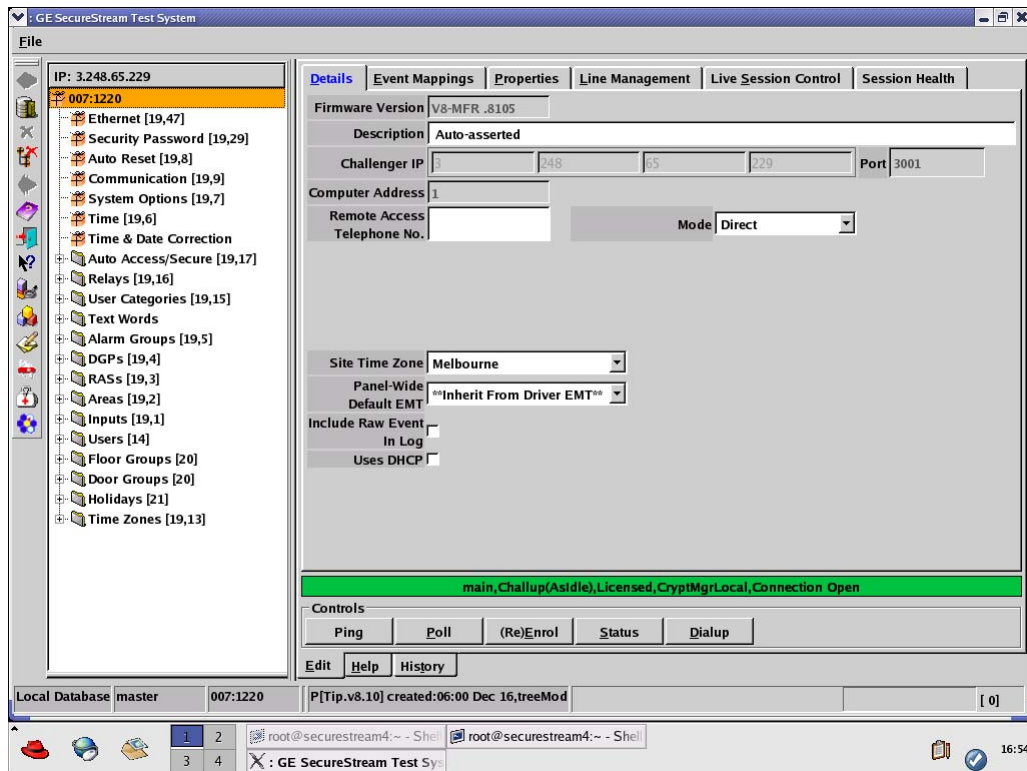
When a Challenger panel's top-level parcel is selected (refer to Figure 17 below) the following Controls buttons display:

- **Ping** — Click to send a ping (ICMP) packet from the receiver to the panel. The button label changes to indicate the result. For example, if a ping fails, the button label is Fail. Click the button again to send another ping.
- **Poll** — Click to send a poll (Challenger protocol null event) to the Challenger panel.
- **(Re)Enrol** — Click to force a re-establishment of the session that manages traffic between Challenger and SecureStream IP.
- **Status** — Click to refresh the information displayed in the current status field (the highlighted field immediately above the Controls buttons).
- **Dialup** — Click to...

Details tab

Trained Installation Technicians may edit the details of individual Challenger panels, if required. Most of the fields auto-enrol. The first field shows the version number of the Challenger firmware.

Figure 17: Editing a Challenger panel



Trained Installation Technicians may edit the details of a Challenger panel.

Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	In the Description field, enter a suitable text description of the Challenger (e.g. the premises street address) so it is easy to identify when using the finder.
3	The Challenger IP field displays a copy of the IP address of the panel as set via Installer menu 47 of the panel. This data is automatically populated when the panel first communicates (enrols) with SecureStream IP and cannot be edited here.
4	The Computer Address field is a copy of the computer address of the panel as set via Installer menu 9 on the panel. This data is automatically populated when the panel first communicates (enrols) with SecureStream IP and cannot be edited here.

Step	Instructions
5	If the panel can receive incoming calls (i.e. for remote programming of the panel via a dialup link), enter the phone number of the telephone line in the Remote Access Telephone No. field. Similarly, specify the type of line using the associated Mode selection box.
6	In Site Time Zone field, select the time zone field that matches the geographical location of the panel.
7	Leave the Panel Wide Default EMT field to its default setting.
8	If you wish to include a hexadecimal copy of the raw event data received from the panel (e.g. for diagnostic purposes), check the Include Raw Event In Log check box.
9	Click the Save icon to save the changes.

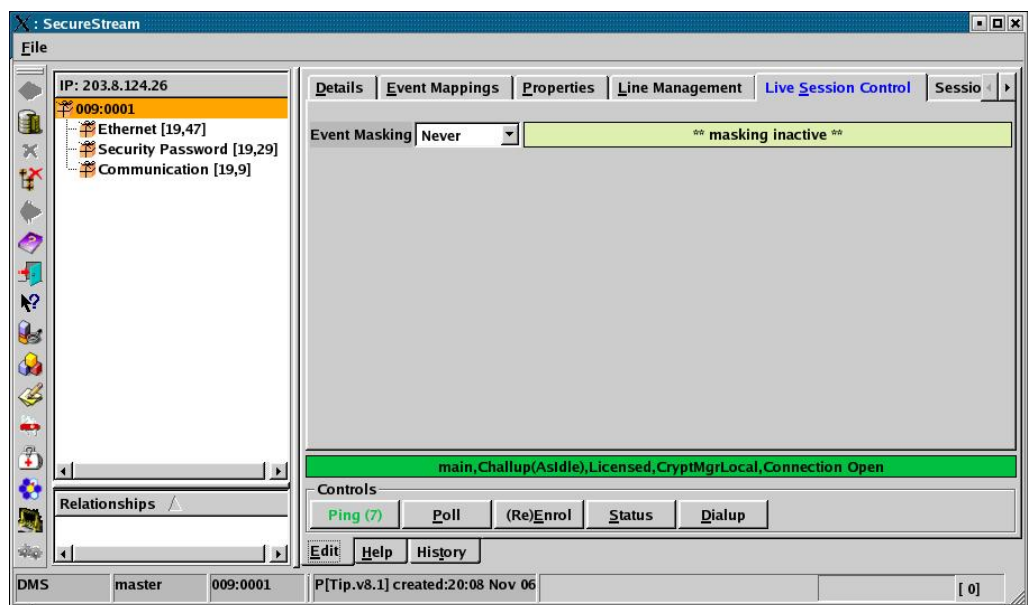
Line Management tab

Not currently used.

Live Session Control tab (event masking)

In some circumstances, you may wish to disable (mask) the transfer of events from a panel to the monitoring station for a specified period. During the masking period, the events that are sent by the panel are discarded by SecureStream and therefore not sent to the monitoring station.

Figure 18: Editing a Challenger panel, Live Session Control tab



The dropdown menu in the *Live Session Control* tab controls the masking period. Options are:

- **Never** – Do not disable the forwarding of events received from this panel.
- **Value [1 Minute – 1 Day]** – Disable forwarding of events received from this panel for the chosen period. A message is displayed next to the drop down menu in this format: 'indicating masking until [Date, Time]'.

When the label, drop down menu, and message are read together it appears as:

Event Masking 1 Hour indicating masking until 05/01/2002 10:02:45am

TIP: Log file. While masking is enabled, events are still received from the panel but not transferred to the monitoring station. The SecureStream IP log file identifies these with the 'M' flag in the *Flags* column. SecureStream IP sends an error code to the monitoring station indicating a panel is masked.

Trained Installation Technicians may use the *Live Session Control* tab to disable the transfer of events from a panel to the monitoring station.

Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	Select the Live Session Control tab (see Figure 18).
3	Select an Event masking value from the dropdown menu.
4	Click the Save icon to save the changes.

Working with the Ethernet tabs

The Ethernet tabs are:

- IP Information
- Encryption Key
- IP Timeouts

Details for two of the three Ethernet tabs are auto-enrolled (not the Encryption Key tab). Detailed instructions for setting local encryption only, are given in the following pages.

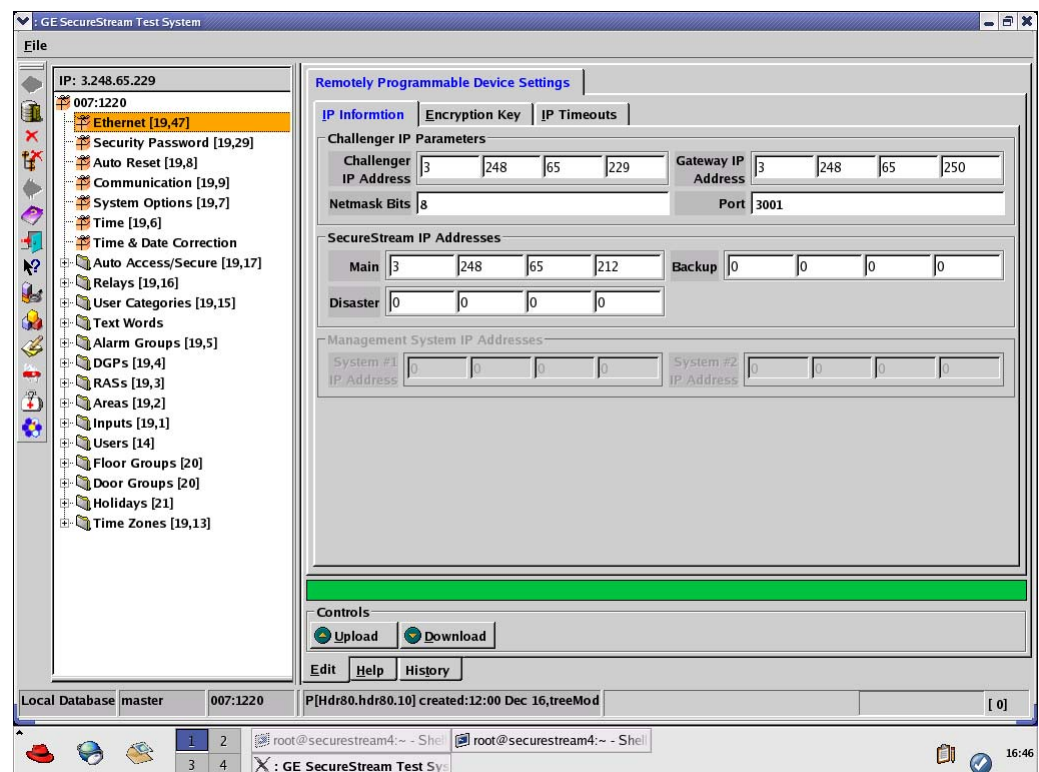
For more information on the IP Information and IP Timeout tabs, see the *TS0898 Ethernet Interface Installation and Programming Guide*.

Trained Installation Technicians may use the Challenger panel's Ethernet parcel, IP Information tab to access the Ethernet tabs for a Challenger panel.

Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	Select the Ethernet parcel.
3	The three Ethernet tabs are named IP Information, Encryption Key, and IP Timeouts (see Figure 19).

IP Information tab

Figure 19: Editing a Challenger panel's Ethernet parcel, IP Information tab



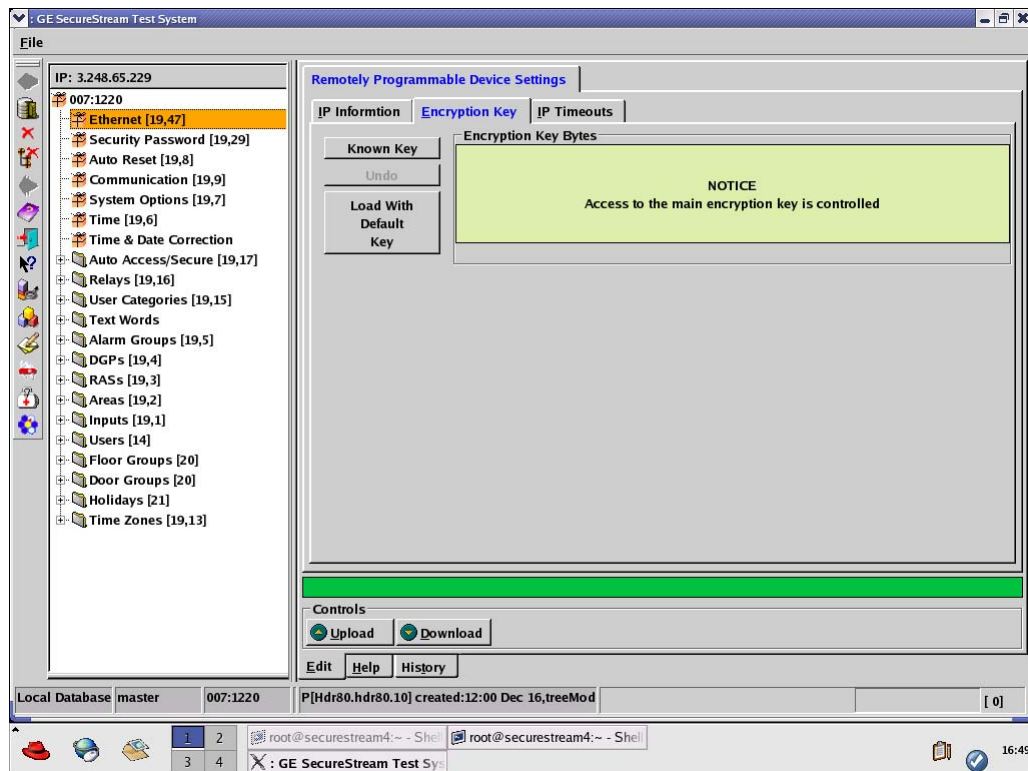
Note: If management software is connected, the **Management System IP Addresses** fields will be greyed and may not be edited.

Encryption Key tab

In SecureStream IP, encryption is set up with an encryption 'key' that is 16 bytes long. The key can be the default encryption key or an individual key. Keys can be either downloaded from SecureStream IP to the panel, or from management software to the panel (if management software is present).

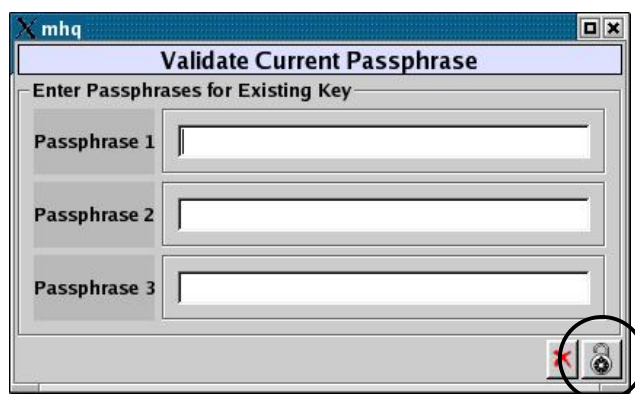
Do not confuse the SecureStream IP encryption with the Challenger panel encryption option for Tecom Direct Line format communications (Installer menu 9-Communications).

Figure 20: Editing a Challenger panel's Ethernet parcel, Encryption Key tab



Load With Default Key: This button installs the Main (Default) Encryption key for use with the current panel (see *Working with the Encryption Keys* tab on page 17). Consistent use of this button simplifies key administration by ensuring that all panels end up using the same encryption key.

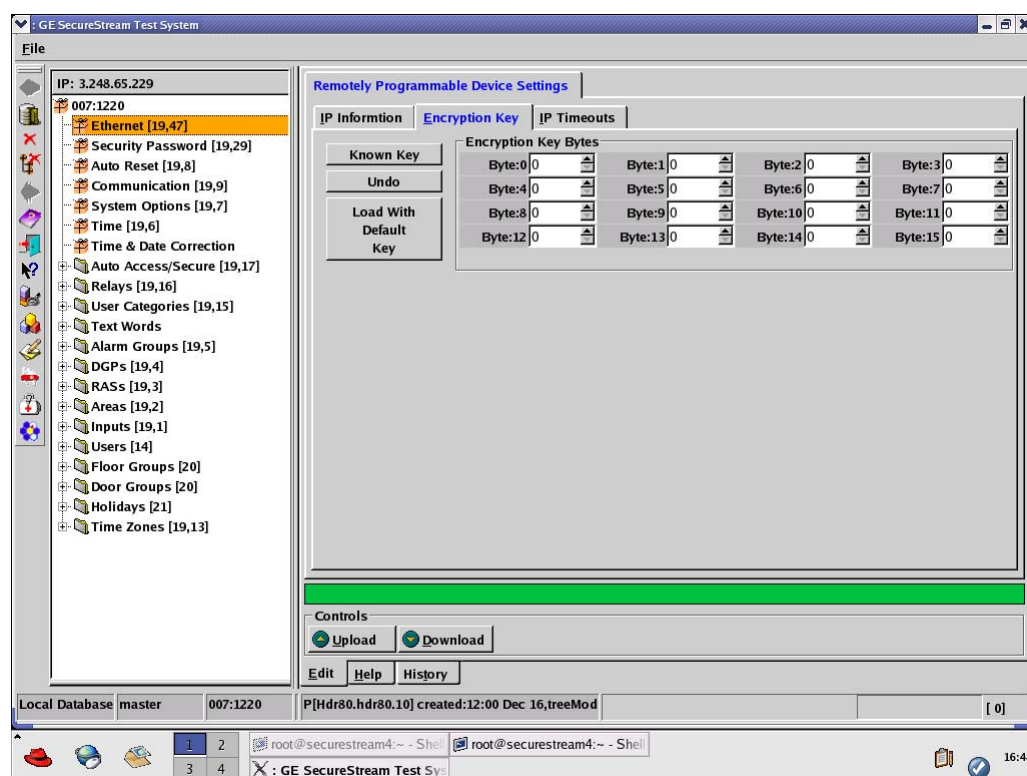
Known Key: This button allows you to set a specific encryption key for this panel. However, before entering this key, it is first necessary to provide any prevailing passphrases needed to authorize access to the encryption key.



Type the passphrase(s) for the existing key, and then click the padlock button (circled) to enter the passphrase(s).

Once the correct passphrase(s) have been entered, the key editing fields are then revealed as shown in Figure 21.

Figure 21: Editing a Challenger panel's Ethernet parcel, Encryption Key tab (after the correct passphrases have been entered)



Encryption rules

Challenger menus have no option for entering the key. So how is the Local Key loaded? The answer depends on whether a Challenger is configured to use the ARES 4.5 (or later) or Forcefield system management software. The rules for encryption key management are:

- **Challenger Configured for ARES 4.5** (or later) – If the network has a computer with ARES or Forcefield software and the IP address of this ARES or Forcefield station is recorded in the Challenger configuration settings (Installer menu 47, '**Management Sw #1:**'), the Challenger will only accept encryption keys from the ARES or Forcefield station at that address.
- **Challenger not Configured for ARES** – If no IP address is recorded for ARES or Forcefield, the Challenger panel will only allow encryption keys to be downloaded from SecureStream IP.

Encryption and ARES or Forcefield

If ARES 4.5 (or later) or Forcefield is installed, the *Encryption* tab described in this section is used only to 'tell' SecureStream IP how messages exchanged with the panel are encrypted. Making changes in this tab has no effect on the Challenger's local settings but may of course disable communication with that panel. If ARES or Forcefield is not installed however, changes made in this tab, either individual or default encryption values, are downloaded to the panel when the record is next saved.

Trained Installation Technicians may use the Challenger panel's Ethernet parcel, Encryption Key tab to set encryption for a Challenger panel.

Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	Double-click a panel record to open it. If management software is present, encryption details must have already been entered via the management software.

Step	Instructions
3	At this stage you can either: - use the default encryption key already set up in the <i>Configuration Editor</i>. Click Load With Default Key. - enter an individual encryption key for the panel. The number range for each field is 0-255. Select the numbers by either clicking the up or down arrows until the correct number displays or type the number with the keyboard. TIP: Ignore the upload and download buttons.
4	Click the Save icon to save the changes.

Tips on encryption

The one special case to consider is when all bytes of the encryption key are set to 0 — this disables encryption. In this state data exchanged with the panel is unencrypted and is observable by anybody with commonly available network monitoring tools.

If an encryption error occurs (i.e., messages from the panel cannot be processed successfully), SecureStream IP will send an error message to the monitoring computer. The exact message sent is set in the configuration editor (see *Working with the Warning Events tab* on page 19).

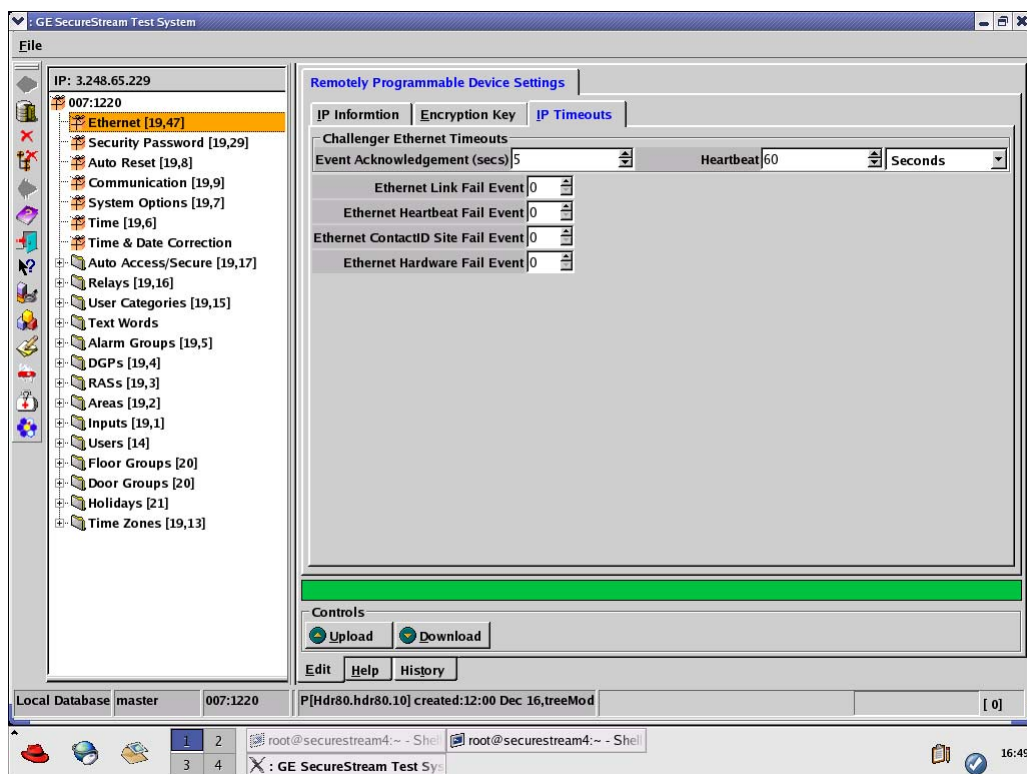
IP Timeouts tab

The IP Timeouts tab sets the event acknowledgement and heartbeat for individual panels.

Event Acknowledgement: Challenger expects an acknowledgment for every event it sends to SecureStream IP. The Event Acknowledgement is the maximum number of seconds Challenger waits before trying to send the event again. Challenger tries three times before assuming the SecureStream IP Receiver is offline.

Heartbeat: The maximum time Challenger waits for a poll from SecureStream IP before assuming the SecureStream IP Receiver is offline. If the heartbeat fails, Challenger sends an event to the monitoring station to tell it the SecureStream IP Receiver is offline. Challenger also regularly checks if SecureStream IP Receiver is back online again.

Figure 22: Editing a Challenger panel's Ethernet parcel, IP Timeouts tab



Trained Installation Technicians may use the Challenger panel's Ethernet parcel, IP Timeouts tab to set the Event Acknowledgement and Heartbeat for a Challenger panel.

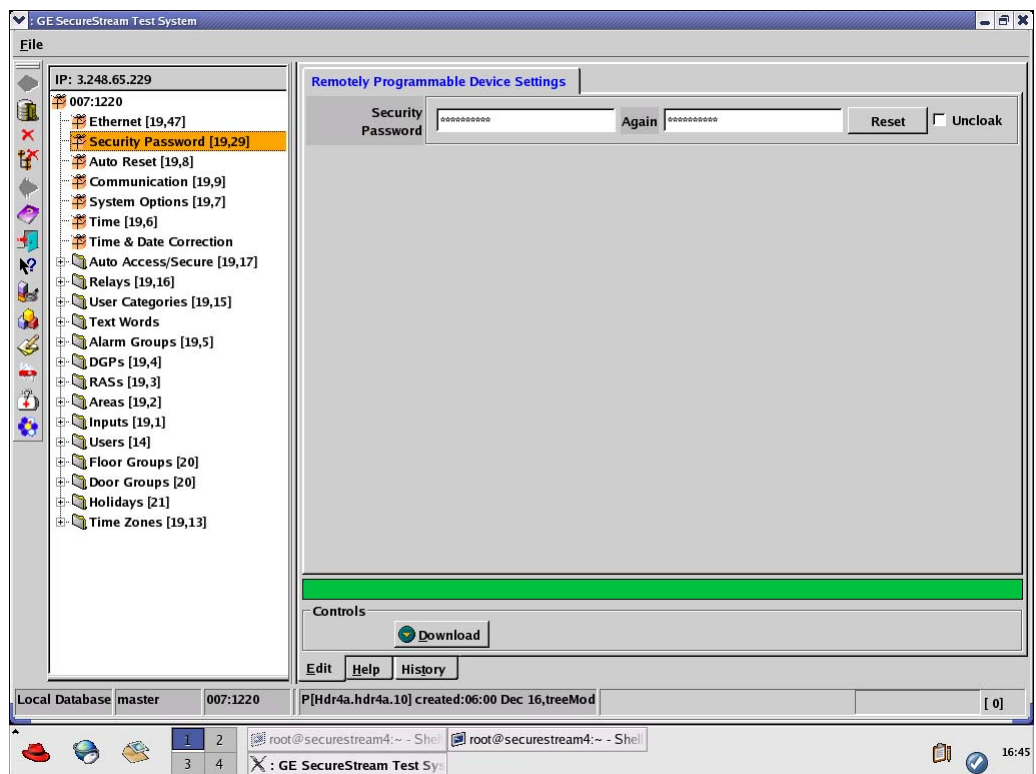
Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	Select the Ethernet parcel, and then select the IP Timeouts tab.
3	Type the value for Event Acknowledgement. See the <i>TS0898 Ethernet Interface Installation and Programming Guide</i> for allowable values.
4	Type the value for the Heartbeat, and then select the required interval (e.g. seconds). See the <i>TS0898 Ethernet Interface Installation and Programming Guide</i> for allowable values.
5	Click the Save icon to save the changes.

Working with the security password

A password can be set for each panel if required, to give access to full remote upload and download features on the Challenger panel when no management software is attached.

Important note: The 10-digit code entered in this field **must** match a code entered by the installation technician at the panel.

Figure 23: Editing a Challenger panel's Security Password parcel, Security Password fields



Trained Installation Technicians may use the Challenger panel's Security Password parcel to set the security password for a Challenger panel.

Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	Select the Security Password parcel.
3	In the Security Password field, type the 10-digit code, and retype it.

Step	Instructions
	Notes: - The 10-digit code entered in this field must match a code entered by the installation technician at the panel. - The default password in the SecureStream IP database if upload and download are disabled is '0000000000'.
4	To reveal the actual characters in the password click the Unclock button if required.
5	Click the Download button to download this password to the panel. If management software is attached, this button will be greyed-out, because it is not possible to download a security password to the panel while management software is attached.
6	Click the Save icon to save the changes.

Working with the Communication tabs

The final set of tabs in the Communication section for a Challenger panel are:

- Telephone Numbers
- General Control
- Miscellaneous
- Area Reporting

As the information displayed in these tabs is automatically populated, a description is not given here. Refer to the *Challenger V8 Programming Guide* (Installer menu 9-Communications) for details about entering data in each of these fields.

Trained Installation Technicians may use the Challenger panel's Communication parcel tabs to view a Challenger panel's communication details.

Step	Instructions
1	Select the panel using the Finder (see <i>How to find a Challenger panel</i> record on page 28).
2	Select the Communication parcel, and then select the required tab.

Working with operators, qualifications (access rights) and features

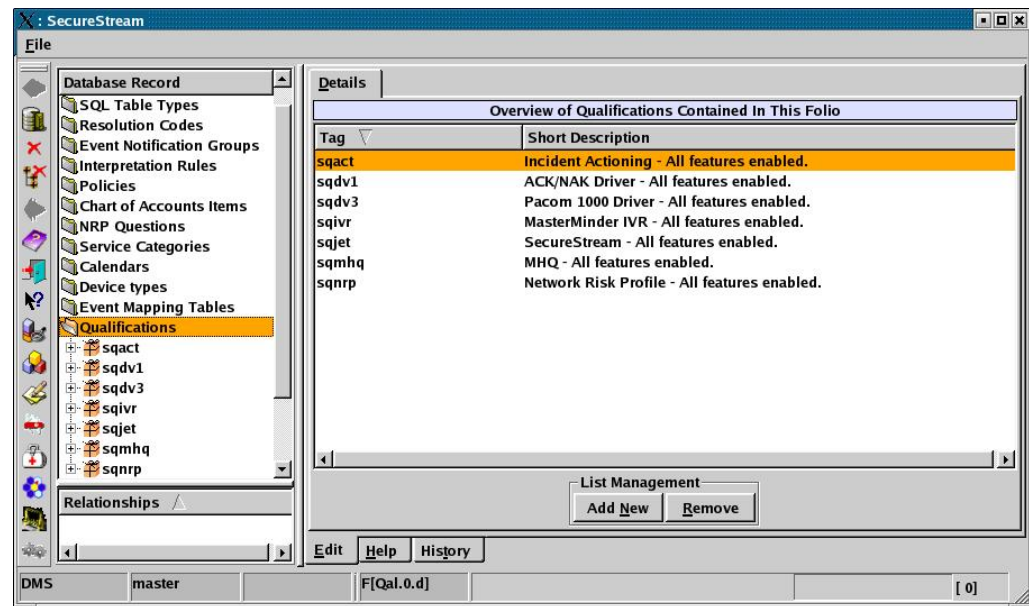
Operator qualifications and features

Overview

A qualification is a defined set of access or permission rights given to operators. A qualification's main purpose is to save time setting up new operators. Figure 24 displays a list of pre-defined qualifications on the right-hand side of the screen.

A qualification's features may be enabled or disabled to define the functions that are available to a logged-in operator who has been assigned the qualification. For example, an operator who does not have the 'access' feature enabled for the Area parcel cannot remotely access Areas on a Challenger panel. Each operator can be given one or more qualifications.

Figure 24: List of pre-defined qualifications



Parcels and features

SecureStream IP handles data in collections called parcels. For example, a premises address and the details of a Challenger Area are each stored in specific parcels. Every parcel has a predefined set of features that control what can be done with the data held in that parcel.

All parcels have four basic features: **view**, **edit**, **add**, and **delete**. Depending on their purpose, some parcels may have additional features. For example, the Challenger Area parcel also has **access**, **secure**, **query status** and **download** features.

Refer to Table 2 on page 8 to see the icon associated with parcels. See *Enabling and disabling features* on page 41.

How to create a qualification

Trained Installation Technicians or Site Managers may create a qualification.

Step	Instructions
1	Click the Resources navigation icon (see Table 1 on page 8).
2	Click the Qualifications folder in the data tree to display existing qualifications.
3	Click Add New to display a new Details tab. See Figure 24 on page 39 for the location of the Add New button. Type the details for the following fields: • Tag – A single word describing this qualification. For example, type 'trainee' for a Trainee Operator. • Short Description – Brief description of the qualification, for example 'Trainee Operator'. • General Comments – Any comments describing this qualification or the way in which it is applied.
4	Click the Save icon to save the new parcel (e.g. 'trainee').

Refer to the following sections for detailed descriptions of enabling and disabling specific Feature elements.

How to edit an existing qualification and its features

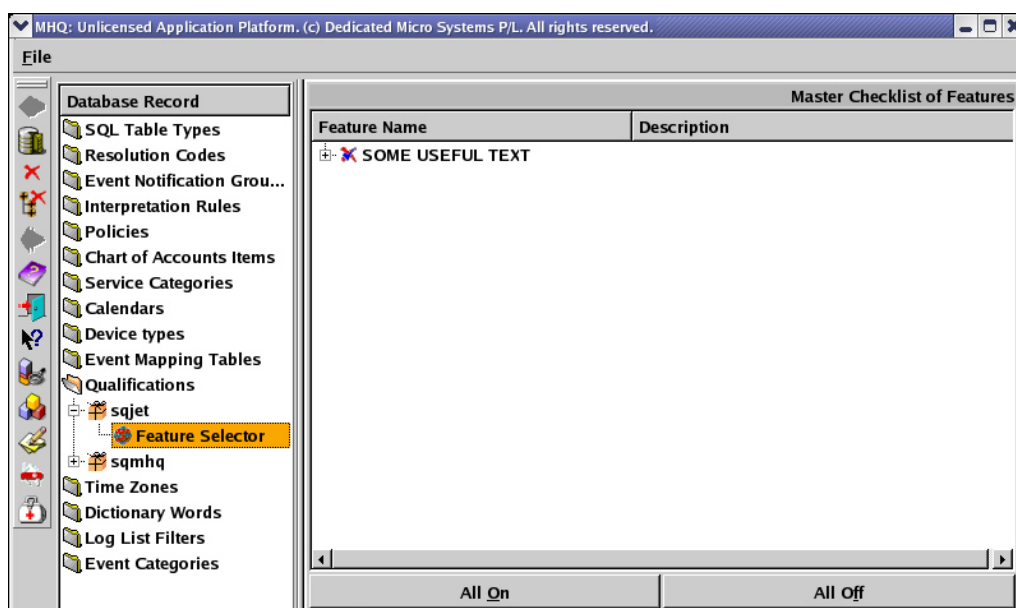
Editing an existing qualification

Changes made to an existing qualification affect all operators currently using that qualification. For example, if the administrator decides to give an individual operator a set of features different from the other operators, they will need to create a new qualification for that operator.

Selecting and deselecting features and feature sub-elements can make operator access highly specific.

NOTE: Altering an existing qualification changes access rights for all other operators sharing the same qualification.

Figure 25: Selecting features for a qualification



Trained Installation Technicians or Site Managers may change an existing qualification. This will affect all operators currently using that qualification.

Step	Instructions
1	Click the Resources navigation icon (see Table 1 on page 8).
2	Click the Qualifications folder in the data tree to display existing qualifications.
3	Double-click the qualification you want to edit to display the Feature Selector icon.
4	Click the Feature Selector icon to display the feature list for that qualification. Click the + box to expand the features tree. See Figure 25 on page 40.
5	Make the changes you require by enabling or disabling features. See <i>Enabling and disabling features</i> below.
6	Click the Save icon.

Enabling and disabling features

The check boxes next to features enable or disable the feature. Clicking the check box changes the state of a feature.

- Checked Box – enabled feature.
- Unchecked Box – disabled feature.

Icons displayed next to the headings in the features list show the state (enabled or disabled) of groups of features.

 **(Blue) Check:** All features under this heading are **enabled**.

 **(Red) Cross:** All features under this heading are **disabled**.

 **Combination:** Some features under this heading are enabled and other features are disabled.

How to add a new operator

Overview

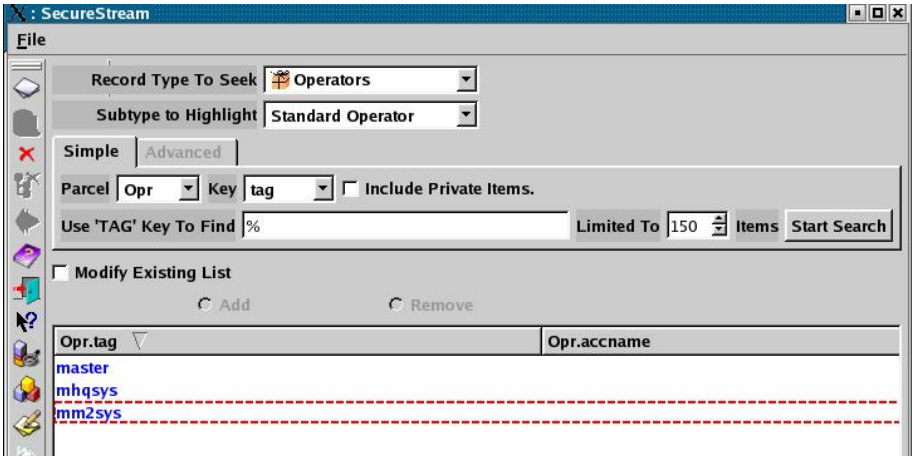
Except for the administrator, all operators (users) must be added to the SecureStream IP database. Any operator with the appropriate qualifications can add operators. The overall process of adding a new operator is as follows:

1. Ensure the operator record does not already exist. See *Search for an existing operator* on page 42.
2. Create an operator record and enter basic details. See *Create a new operator record* on page 43.
3. Create a logon password for the operator. See *Create the operator's password* on page 43.
4. Assign a qualification to the new operator (i.e., a set of access rights) to the operator. See *Assign a qualification* on page 43.

Procedures

Search for an existing operator

Trained Installation Technicians or Site Managers may use the following procedure to find an operator record.

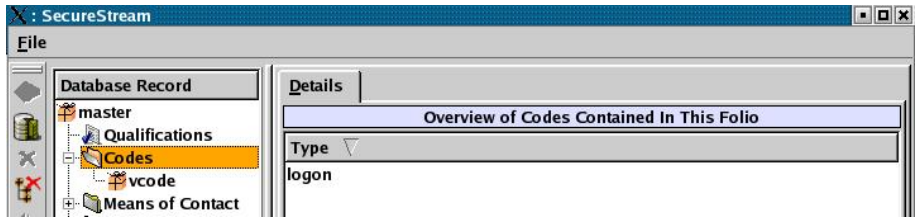
Step	Instructions
1	Log on to SecureStream IP.
2	Click the Finder navigation icon (see Table 1).
3	In the Finder, click the Record Type To Seek dropdown menu and select Operators. 
4	Click the Subtype To Highlight arrow and select the type of operator you wish to create (e.g., standard operator). If you do not have the correct qualification (access rights) a lock symbol appears.
5	Type an asterisk * in the Using 'Tag' Key To Find field, and then click the Start Search button to display a list of all the operators. Operators of the subtype selected in the Subtype To Highlight list are displayed in blue text. 
6	If an operator in the list matches or is similar to the operator you are about to create, double-click the record to check the details. If the required operator record does not exist, proceed to <i>Create a new operator record</i> on page 43.

Create a new operator record

Trained Installation Technicians or Site Managers may use the following procedure to add an operator record.

Step	Instructions (continued from previous section)
1	Ensure the operator record does not exist. See <i>Search for an existing operator</i> on page 42.
2	Click the New Record icon (see Table 1 on page 8) to display a new operator record window.
3	Click the dropdown menu and select Standard Operator.
4	Type an Operator ID (= login ID) for the new operator. Use the operator's initials and last name. This field is case-sensitive.
5	In the fields that follow, type the operator's: surname, first name, and middle name.
6	Enter any necessary comments or notes about the operator e.g., start date.
7	Click the Save icon.

Create the operator's password

Step	Instructions (continued from previous section)
1	Click the Codes folder in the data tree to display the codes overview list. 
2	Click the Add button at the bottom to display the code editor.
3	Select logon from the dropdown menu.
4	Enter the operator's password into the left password field and then retype the password in the right field. (If the two passwords do not match the Reset button displays in orange.) Tip: The Reset button resets the operator's password to the general default password for all operators, '4346'.
5	Press the Save icon to save the password.

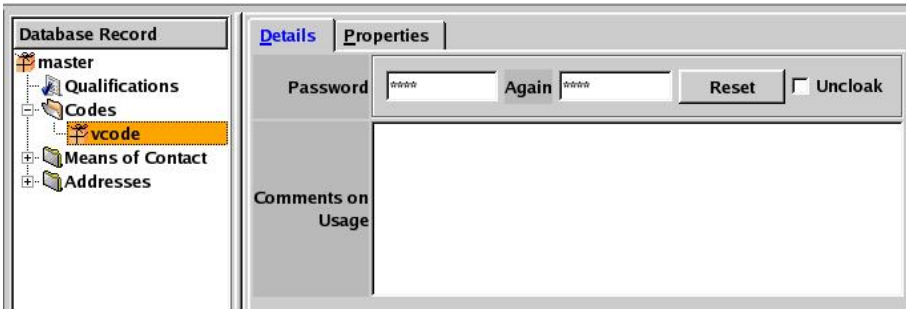
Assign a qualification

Step	Instructions (continued from previous section)
1	Click the Qualifications icon in the data tree to display the qualifications list, such as shown in Figure 24 on page 39. If you do not see appropriate qualifications for the operator, see <i>How to create a qualification</i> on page 40.
2	Highlight the qualifications that you want to assign to this operator.
3	Press the Save icon to save the qualifications. The operator will now have access to all enabled features contained in the selected qualifications.

How to change an operator password

This section describes how to change an operator's password in SecureStream IP.

Use the following procedure to change an operator's password.

Step	Instructions
1	Find the operator record. See <i>Search for an existing operator</i> on page 42.
2	Double-click the operator's record to open it.
3	Click the Codes folder in the data tree and the vcode parcel will display with the operators password information on the right. 
4	Enter the operator's password into the left password field and then retype the password in the right field. If the two passwords do not match the Reset button displays in orange. The Reset button resets the operator's password to the general default password for all operators i.e., '4346'.
5	To show the characters in the password click Uncloak .
6	Press the Save icon to save the new password.

Upgrading and re-installing SecureStream IP licenses

SecureStream IP license options

Each SecureStream IP license covers a certain number of Challenger panels, i.e. one license covers 2, 5 or 20 panels, depending on the model of SecureStream IP Receiver (see example 1 and the list below).

Each SecureStream IP Receiver is supplied with included licenses pre-installed.

If the number of Challenger panels increases to beyond the number allowed for a SecureStream IP Receiver, (see example 2 and the table below) a new SecureStream IP Receiver will need to be purchased from GE within the 30-day grace period.

Example 1: A site has a TS9080 SecureStream IP Receiver with a license for 2 panels. To increase the number of panels from 2 to 6, you'll need to buy 2 extra licenses (TS9083), as each license covers 2 panels.

Example 2: A TS9081 SecureStream IP Receiver has a license for 5 panels, but now there are 160 panels. As the TS9081 covers a maximum 100 panels, you'll need to buy and install a new TS9082 SecureStream IP Receiver (with its basic license for 20 panels), and 7 license upgrades (TS9085) to cover the 160 panels.

Example 3: A TS9081 SecureStream IP Receiver with a license for 5 Challenger panels is installed on a site with 15 Challenger panels. SecureStream IP auto-enrols the first 5 panels but the remaining 10 panels remain unlicensed. SecureStream IP won't pass events from the 10 unlicensed panels to the monitoring station until 2 licenses (TS9084) are purchased and installed.

The following is a list of licensing options (part numbers) for SecureStream IP Receiver.

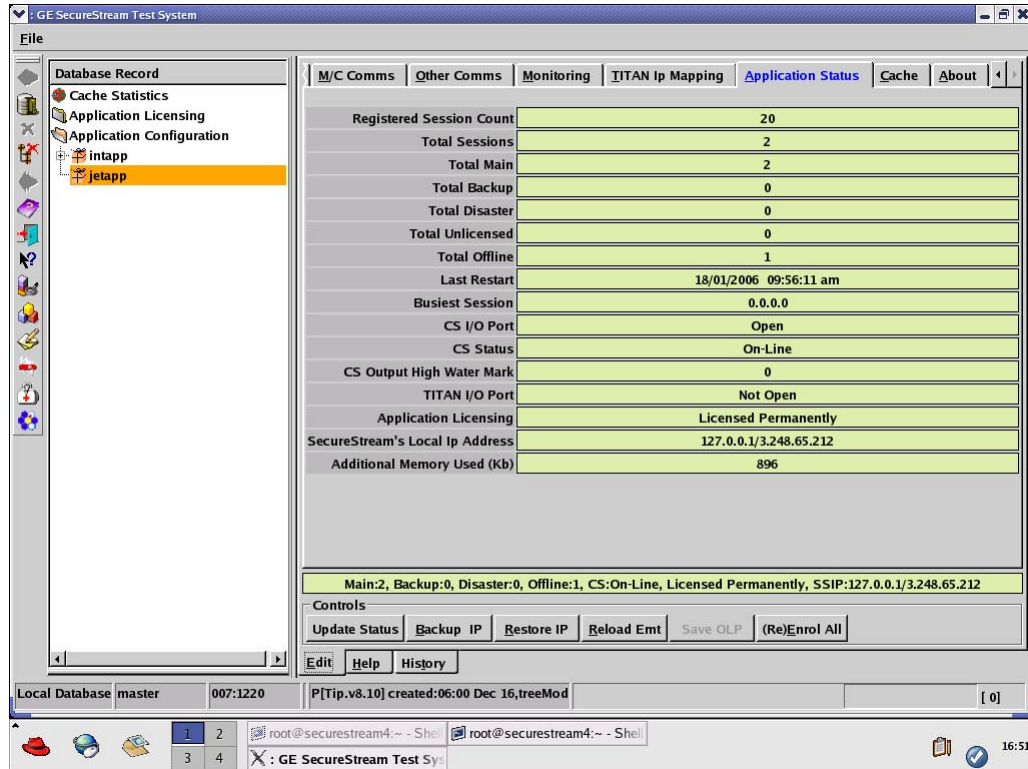
- **TS9080** — Small to medium installations (site maximum 20 panels) on a single SecureStream IP Receiver. Includes license for 2 panels. Expand with part number **TS9083** for each 2 additional panels.
- **TS9081** — Small to medium installations (site maximum 100 panels) on a single SecureStream IP Receiver. Includes license for 5 panels. Expand with part number **TS9084** for each 5 additional panels.
- **TS9082** — Medium to large installations (site maximum 300 panels) on a single SecureStream IP Receiver. Includes license for 20 panels. Expand with part number **TS9085** for each 20 additional panels.
- **TS9082B** — Medium to large installations (site maximum 300 panels) on multiple SecureStream IP Receivers. Includes license for 20 panels. Minimum order quantities apply.
- **TS9082E** — Enterprise installations (site maximum 4000 panels) on multiple SecureStream IP Receivers. Includes license for 20 panels. Minimum order quantities apply.

Checking your SecureStream IP license status

In some cases, the operator will need to check how many licenses the SecureStream IP Receiver has, i.e. how many Challenger panels it can run.

Example: The installer needs to add more Challenger panels to a system. The procedure below explains how to check the SecureStream IP for the number of licenses or Challenger panels it is already licensed for.

Figure 26: Jetapp configuration editor, Application Status tab



If you need to increase the number of licenses, read the section *Upgrading or re-installing a SecureStream IP* on page 47. There is a 30-day grace period to allow you time to increase your license after adding an unlicensed Challenger panel.

Trained Installation Technicians or Site Managers may use the following procedure to check how many licenses SecureStream IP has.

Step	Instructions
1	Log on to SecureStream IP.
2	Click the Configuration editor navigation icon (see Table 1).
3	Double-click the Application Status folder.
4	Double-click Jetapp parcel.
5	Select the Application Status tab to view the total numbers of licensed and unlicensed panels, listed as the Registered Session Count. Subtract the number of unlicensed panels.

Upgrading or re-installing a SecureStream IP license

Use this procedure if you are:

- Upgrading a SecureStream IP license when more Challengers have been added to a system.
- Re-installing SecureStream IP and re-installing the SecureStream IP license.

There are three steps involved in library registration:

1. The installer generates a License Request File (LRF).
2. The LRF is emailed to GE who use it to create a unique license file. The email address is **customerservice@gesecurity.com.au**.
3. The license file is emailed back to the installer where it is used to complete the registration process.

License grace period: There is a 30-day grace period to allow for the return by email of license requests.

Before you start

You will need a formatted floppy diskette.

Important note about the Ethernet Card MAC address

The Ethernet card MAC address is used to identify the server to MHQ. If you need to replace the card for any reason (as might occur if the card is faulty or the entire server needs to be replaced) all libraries must be reregistered within 30-days or the application will stop functioning. This 30-day grace period allows users to replace faulty Ethernet cards or servers without losing use of SecureStream IP.

Explanation of file names

Registering the 'libmhq' and 'libjet' libraries involves six files:

libmhq.ser and **libjet.ser**: the serialisation files on the floppy disk supplied with SecureStream IP when purchased.

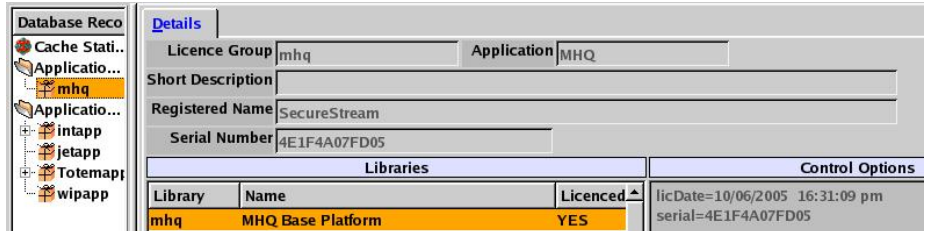
libmhq.lrf and **libjet.lrf**: the license request files sent to GE by email.

libmhq.lic and **libjet.lic**: the license files emailed back added to the floppy disk and used to install the library licenses.

Procedure

Part 1: Making the library license request files

Trained Installation Technicians or Site Managers may use the following procedure to register SecureStream IP.

Step	Instructions
1	Log on to SecureStream IP.
2	Insert the formatted floppy disk into the SecureStream IP Receiver's floppy drive.
3	Click the Configuration editor navigation icon (see Table 1).
4	Double-click the Application Licensing folder to expand the tree and select the 'mhq' parcel. 

Step	Instructions
5	Click the Make LRF button at the bottom of the screen. The system will create the (encrypted) License Request File (mhq.lrf) on the floppy disk.

Part 2: Email the License Request File to GE

Step	Instructions (continued from previous section)
1	Create an email with the subject heading 'SecureStream IP License Request for XX Challengers', (where XX is the required number of Challenger panels). Attach the mhq.lrf file to the email message.
2	Send the message to GE at customerservice@gesecurity.com.au .

GE will authenticate the details and, if correct, add them to their database. GE will then email a SecureStream IP license to you as an encrypted email attachment (mhq.lic).

Part 3: Complete the registration process

Step	Instructions (continued from previous section)
1	Once you receive the mhq.lic attachment by email, save the file to a formatted floppy disk.
2	Insert this floppy disk into the SecureStream IP Receiver floppy drive.
3	Click the Configuration editor navigation icon (see Table 1).
4	Select Application Licensing at the top left, and then select the mhq parcel.
5	Click the Install License From Floppy button at the bottom of the editor page on the right. The program will read and decode the license file. A message 'License for mhq has been installed successfully' displays.

Troubleshooting license installation

Errors may occur during the registration process. Each error displays an error message. The cause and the remedy of some common errors are detailed below.

Problem	Cause and remedy
Registered name must not be blank.	Enter the name of the entity the application is to be registered to in the 'Registered Name' field (e.g., Asset Banking Corporation).
Can't access public key file.	The Public Key cannot be found. The public key is installed with the original software and is used to decrypt all registration files. This error is unlikely but if it occurs, the solution is to reinstall the public key and repeat the procedure. The public key file (mhqpub.pem) can be found on the MHQ License Management Diskette and is also freely available from DMS. It should be copied to the directory /usr/local/mhq/data/misc.
Invalid Ethernet Card MAC address.	The Ethernet card either does not have a valid MAC address or is not installed. Software registration uses the MAC address of the Ethernet card to verify the identity of the server when the license file (.lic) is installed. Install the same Ethernet card that was used when the LRF was created and try again.
Can't create LRF.	The application cannot create the License Request File. There is a problem writing to the floppy disk. Likely causes are: the diskette is not in the floppy drive, or the diskette in the drive is set to 'Read Only'. Check the diskette and/or floppy drive and try again.

Problem**Cause and remedy**

Can't encrypt LRF.

The public key is corrupt. This error is unlikely but if you see it, the best solution is to reinstall the public key as described above and attempt to remake the License Request File.

Serial # in the license file is incompatible with the selected library. Are you using the correct diskette?

The serial number in the license file does not match the serial number displayed in the library overview list. This error is most likely to occur if you are licensing multiple systems and have inserted the wrong diskette by mistake. Insert the correct disk or repeat the entire registration procedure.

Reference topics

How to set up SecureStream IP Receiver

GE Security Pty. Ltd. (GE) provides SecureStream IP Receivers with SecureStream IP and Linux pre-installed. The process of setting up a SecureStream IP Receiver is described here to assist in case reinstallation is required (for example after a hardware failure).

SecureStream IP Receiver comes in various configurations, depending on the requirements (small, medium, or enterprise installations), and may vary depending on other factors (e.g. improvements in processor speed).

This procedure describes one configuration. Contact GE Technical Support if you need assistance with other configurations.

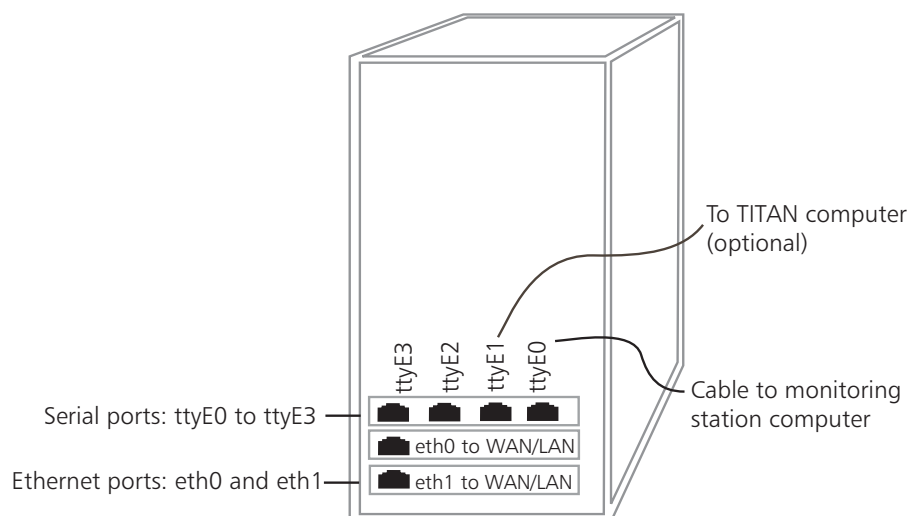
Before you start

We recommend that the installation technician setting up SecureStream IP Receiver verifies with the customer that the equipment and software supplied matches the equipment and software ordered.

Installing SecureStream IP Receiver

Step	Instructions
1	Unpack and assemble the SecureStream IP Receiver computer, keyboard, monitor, and mouse.
2	Power up the SecureStream IP Receiver.
3	Follow the instructions in the sections: • <i>Setting up SecureStream IP software</i> on page 12 • <i>Adding the SecureStream IP Receiver IP address to the network</i> on page 13
4	Connect a LAN/WAN cable to SecureStream IP Receiver port eth0 (see Figure 27 below) and connect to the LAN/WAN network (with help from your network administrator).
5	Test the connection by pinging the TS0898 Ethernet Interface(s). If you cannot successfully ping the TS0898, refer to <i>Troubleshooting connections</i> on page 51.

Figure 27: Rear view of SecureStream IP Receiver



Troubleshooting connections

If you cannot ping the TS0898s, or any other device on the same network, do the following:

- Check with your network administrator.
- Check that all the settings in SecureStream IP, especially those for the network configuration, are correct.
- Check all the hardware settings and connections.

Connecting SecureStream IP to a central monitoring station

Depending on your LAN and WAN setup, the SecureStream IP Receiver could be at the Challenger panel end, the monitoring station end, or at another network location altogether. Wherever the SecureStream IP Receiver is located, the monitoring station software will need to be set up to receive CID data from the SecureStream IP Receiver.

Step	Instructions
1	Connect the SecureStream IP Receiver to the monitoring station computer. Use serial port tttyE0 . The serial tty ports are labelled (see Figure 27 on page 50).
2	At the very minimum, at the SecureStream IP Receiver, configure the serial comms settings for baud rate, etc. in SecureStream IP in the M/C Comms tab. Refer to <i>Working with the Serial Comms Settings</i> tabs on page 20 for details.
3	In the monitoring station software set up the connection to SecureStream IP. Ensure the serial port settings are the same in the SecureStream IP software and the monitoring station software. If the installation is successful, the monitoring station should start receiving events immediately. If events aren't received at the monitoring station end, see <i>Troubleshooting central monitoring stations</i> below.

Troubleshooting central monitoring stations

We recommend that you first check with your network administrator.

If the your network administrator cannot resolve the problem, use the following procedure to check connectivity between SecureStream IP Receiver and the monitoring station by using a serial crossover cable and an application such as HyperTerminal or VT100.

Step	Instructions
1	Disconnect SecureStream IP Receiver from the monitoring station software.
2	Change the device name to tttyE0 in SecureStream IP in the M/C Comms tab. Refer to <i>Working with the Serial Comms Settings</i> tabs on page 20 for details.
3	Connect the crossover cable between tttyE0 and HyperTerminal or VT100 to enable CID events to be seen.
4	Use HyperTerminal or VT100 to verify that CID events are occurring.
5	Once working, re-connect SecureStream IP Receiver to the monitoring station software.

How to install SecureStream IP from the installation DVD

Introduction

SecureStream IP and the Linux operating system are pre-installed when supplied, but in some cases you may need to reinstall them on the SecureStream IP Receiver (e.g. after a hardware failure).

Pre-requisites

In addition to the GE SecureStream IP DVD, you need to know the following details about the network configuration before you can proceed:

- IP address
- Host name
- Net mask
- Gateway IP address
- IP addresses for primary, secondary and tertiary DNS servers. These addresses are optional for some networks.

You will need these details during the installation process.

Procedure

Part 1: Prepare the SecureStream IP computer

Step	Instructions
1	Power up the SecureStream IP Receiver, and insert the GE SecureStream IP DVD into the DVD drive during power up.
2	Press DEL during start-up to access the BIOS programming.
3	In the BIOS menu Standard CMOS Features , set the system time to the current time in the location where the SecureStream IP Receiver will be used.
4	Save the BIOS programming and exit.
5	The SecureStream IP Receiver will boot from the GE SecureStream IP DVD, and the initial installation screen will appear. Press ENTER to select Install or upgrade this platform in graphical mode .
6	Select English for the installation process, and then click Next.
7	Select US English Keyboard , and then click Next .
8	Click the Server button to select the server installation type.
9	In Disk Partitioning, select the following: • Automatically Partition • Remove all partitions on this system And then click Next .
10	A warning box will appear asking if you are sure that you wish to delete all data. Click Yes .
11	When finished, click Next to continue.
12	Ensure that a checkmark appears next to Ethernet Interface eth0 to indicate that it will be activated on boot.
13	In the "Network Devices" dialog, highlight the eth0 line and click Edit . A new dialog box will appear.

Step	Instructions
14	Clear the checkbox Configure using DHCP.
15	Type the details for the IP address and net mask.
16	Close the dialog box.
17	In the host name dialog, select manually , and then type the host name .
18	Type the gateway IP address, and the optional DNS server IP address (if applicable), and then click Next . If a DNS server IP address is not programmed, then an error message displays "Error with Data". If no DNS IP address is required, ignore the message and press Continue .
19	The Firewall is enabled by default, and the checkboxes for the services listed below must be selected: • Remote Login (SSH) • Web Server (HTTP, HTTPS) • File Transfer (FTP) • Mail Server (SMTP) Click Next .
20	In Additional Language Support , select English (Australia) and deselect English (USA).
21	In Time Zone Selection , click the yellow dot on the map that has the same time zone as the location where the SecureStream IP Receiver will be used.
22	Type a root password and then confirm it. By default, the root password is tecom4346 . Click Next .
23	Skip Package Group Selection. Click Next .
24	The About To Install screen displays. Click Next . Dialog boxes will show the file system formatting, the install image being copied to the hard disk drive, and then progress bars display the progress of individual packages and the overall progress of the installation.
25	The Installation installed successfully screen displays. Click Reboot . The installation DVD should be ejected automatically. Remove it while the machine is shutting down.

Part 2: Post-install configuration

Step	Instructions (continued from previous part)
1	After rebooting, the Welcome to post-install configuration screen displays. Click Next .
2	The License Agreement screen displays. Read the License Agreement. If you agree, select Yes, I agree to the License Agreement , and then click Next .
3	The Date and Time screen displays. Set the date and time to the current date and time in the location where the SecureStream IP Receiver will be used.
4	The Display screen displays. Configure the correct monitor resolution. Do not modify the default settings if SecureStream IP Receiver is shipped without a monitor.
5	Skip System User. Click Next . Progress messages display.

Step	Instructions (continued from previous part)
6	Log in via the process described in <i>Logging in to SecureStream IP</i> on page 11. If you see the message “no sound card”, select Do not show this message again , and then click OK .

Part 3: Install the license

Refer to *Upgrading and re-installing SecureStream IP licenses* on page 47 for details.

Part 4: Configure the firewall

Step	Instructions (continued from previous part)
1	Click the Red Hat icon at the bottom left corner of the screen (see Figure 5 on page 12), and select System Settings > Security Level . The Security Level Configuration dialog displays.
2	At the end of the Other Ports field, type “, 3001 : udp” to allow UDP packets on port 3001. Please note that the leading “, ” is only required if there are other entries in this field. Click OK .
3	The following warning displays: Clicking the ‘Yes’ button will set the security level of the system and override any existing firewall configuration. Are you sure that you want to do this? Click Yes . The Security Level Configuration dialog closes.

Connecting TITAN management software to SecureStream IP

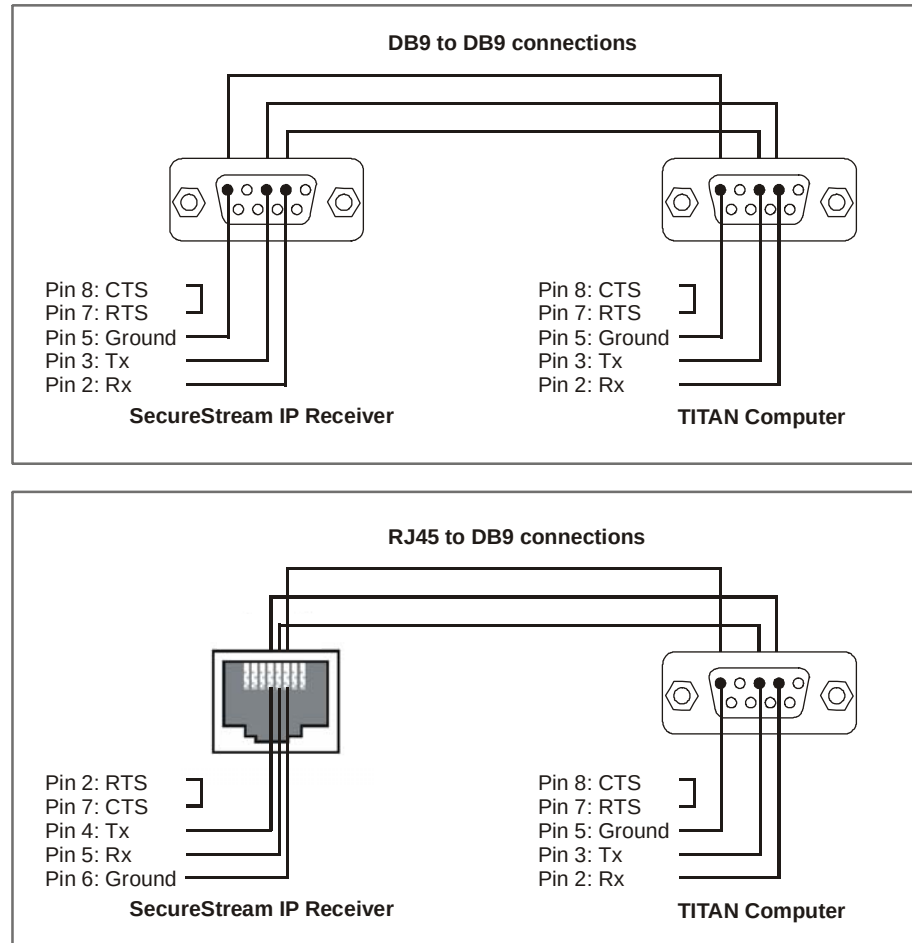
A serial cable using a null modem connection is used to connect the SecureStream IP Receiver to the TITAN computer.

The SecureStream IP Receiver may have either a DB9 or an RJ45 serial port. The TITAN computer is expected to have a DB9 serial port. As a result, you will need to construct one of two types of cable:

- DB9 serial to DB9 serial
- DB9 serial to RJ45 serial

The cable pin outs are described in Figure 28.

Figure 28: SecureStream IP Receiver to TITAN serial cable pin outs

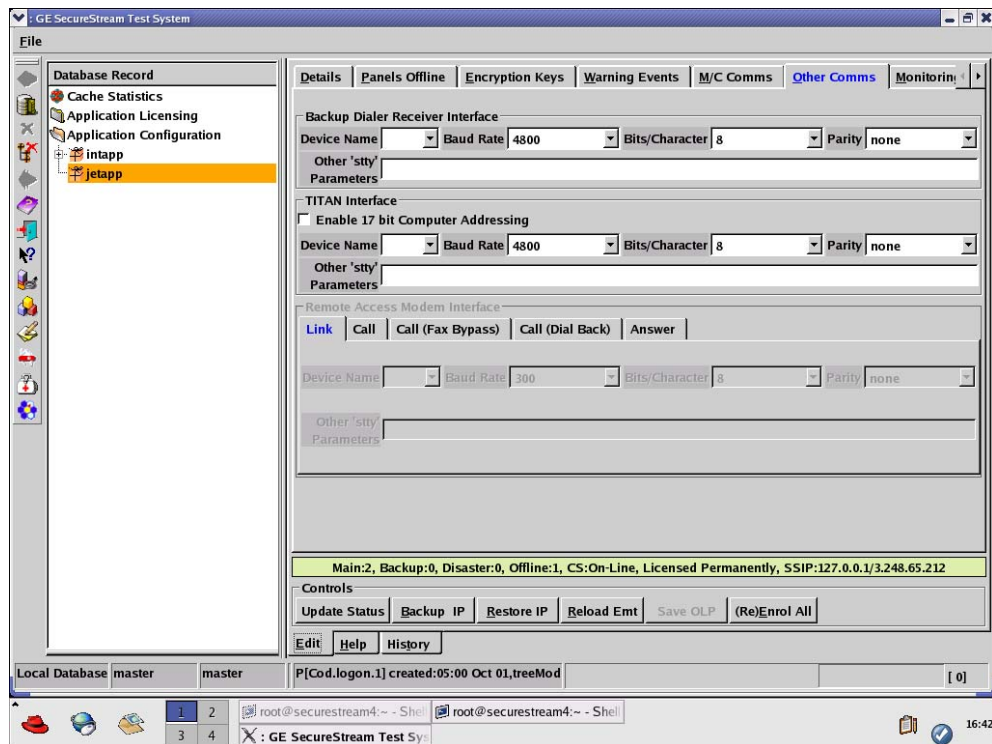


When TITAN is connected to SecureStream IP Receiver, TITAN can be used to:

- Upload and store the database for various clients.
- Modify and download the database
- Control areas and check the status of a particular panel

Note: TITAN will not receive events from Challenger when TITAN is connected to SecureStream IP Receiver.

Figure 29: Jetapp configuration editor, Other Comms tab



Trained Installation Technicians may use the following procedure to connect TITAN to SecureStream IP Receiver.

Step	Instructions
1	Log on to SecureStream IP.
2	Click the Configuration editor navigation icon (see Table 1).
3	Click the Application Configuration folder.
4	Click the Jetapp parcel.
5	Click the Other Comms tab on the right.
6	Select the serial port for TITAN interface (can be ttyE0 ... ttyE3). Leave the other options as the default settings.
7	Click the Save icon.
8	In TITAN, select Admin > Challenger , and select the SecureStream enabled check box. Click the Save button to save the record.
9	In TITAN, select Admin > Ports , and open (or create) the record for the port you are using to connect to the SecureStream IP Receiver. In the Baud Rate section, select 4800 ; and in the Comms Mode section, select Direct . Click the Save button to save the record.
10	In TITAN, select Admin > SecureStream IP Configuration . In the IP configuration screen, type the Challenger number you wish to connect to. Click the Save button to save the record.
11	In TITAN, select File > Open system , and check the SecureStream enabled check box. Click the Save button to save the record.

Step	Instructions
12	Now check that TITAN is connected. In SecureStream IP Receiver, select the TITAN IP Mapping tab. As the TITAN IP mapping is automatic, the panel's IP address and the computer address should be listed (see Figure 13 on page 23).

Common Ademco CID error codes

CID codes

The following table list the common default CID codes sent to the monitoring station by SecureStream IP.

SecureStream IP CID errors

CID code	Explanation
E357	Loss of IP communication between main SecureStream IP Receiver and Challenger
E361	Loss of IP communication between backup SecureStream IP Receiver and Challenger
E362	Loss of IP communication between Disaster SecureStream IP Receiver and Challenger
E363	When a panel has its events Masked for a defined period
E364	Encryption Key error mismatch.
E707	License expiry.
E708	Panel substitution.

TS0898 Ethernet Interface CID errors

CID code	Explanation
E703	Ethernet link failed
E704	Ethernet heartbeat failed
E705	Ethernet CID site failed (SecureStream IP Receiver)
E706	Ethernet hardware init failed (TS0898)

Troubleshooting and technical support topics

SecureStream IP

Problem	Cause and remedy
Can't log on – attempt returns dialog box containing message 'Logon Incorrect. Please try again.'	Either the Operator ID or Password has been entered incorrectly when attempting to log on. Check the Operator ID and Password in the Operator Record and retry. Remember both the Operator ID and Password fields are case-sensitive.
Can't log on – attempt returns dialog box containing message 'Logon Failed!'	The application will fail a logon after two incorrect tries and exit the application.

Linux operating system

You may need to reinstall the Linux operating system. The full procedure is described in the Linux handbook supplied with the SecureStream IP Receiver. See Chapter 3, 'Installing Red Hat Linux'.

See also

- Troubleshooting license installation on page 48
- Troubleshooting connections on page 51
- Troubleshooting central monitoring stations on page 51

How to request technical support

When technical problems occur, contact GE Technical Support at techsupport@indsys.ge.com

Glossary

Term	Definition
ARES	See <i>Management software</i>
Auto-Enrol	Automatically add a new Challenger panel to SecureStream IP and populate many of the data fields for the panel.
Backup	The (optional) second SecureStream IP Receiver to which Challenger sends events, if the main SecureStream IP Receiver fails. (CID # 002 in the Challenger Installer programming.)
CID	Standard Ademco Contact ID event code format. Support for specific CID event codes may differ between monitoring companies.
Computer address	Computer address of the panel.
Computer link queue depth	Buffer size for incoming computer messages.
Disaster	The (optional) third SecureStream IP Receiver to which Challenger sends events, if the main and backup SecureStream IP Receivers fail. (CID # 003 in the Challenger Installer programming.)
Download	Send data from the SecureStream IP Receiver to one or more Challenger panels.
Encryption	Encoding data so it is unreadable without the correct key. Without encryption, a site's data is available to those with the knowledge and tools. We strongly recommend encryption is enabled, and the encryption keys only be made known to trusted personnel.
Event log	Running log of all received and sent events.
Forcefield	See <i>Management software</i>
Heartbeat period	Rate at which SecureStream IP polls the Challenger. Also referred to as 'Max Silence'.
Host name	The IP address of the computer on which SecureStream IP software is installed. Also called the Network Interface IP address.
IP Address	Internet Protocol address. A unique identifier assigned to each panel and computer in a network.
SecureStream IP	Refers to the SecureStream IP Receiver (software only).
SecureStream IP Receiver	Refers to the entire SecureStream IP Receiver (software and hardware).
KDE	The Graphical User Interface (GUI) desktop environment that runs on the Linux operating system.
libjet	See <i>Library</i>
Library	SecureStream IP software library. Each library holds a set of licensed features. For example the 'libmhq' and 'libjet' libraries.
Linux	The pre-installed operating system on the SecureStream IP Receiver, chosen for its stability and flexibility.
Live session control	The length of time SecureStream IP stops sending CID events from a Challenger to the monitoring station. Also called 'masking'.
Main	The first SecureStream IP Receiver to which Challenger sends events. (CID # 001 in the Challenger Installer programming.)
Management software	ARES 4.5 (or later), Forcefield, or TITAN software engineered by GE to monitor and administer Challenger security systems.
MasterMinder	An example of proprietary software for monitoring stations.
Maximum Silence	Equivalent to heartbeat.
MHQ	Monitoring HeadQuarters. Software application that forms the foundation platform for SecureStream IP.
Monitoring station	Central location that monitors alarm events. Usually manages more than one site.
Panel editor	Allows you to edit the details for individual Challenger panels as well as upload and download selected Challenger panel settings.

Term	Definition
Passphrase	Passwords to authorise access to the Encryption Key. SecureStream IP uses one, two or three passphrases that should ideally be held by separate people. This ensures that keys can only be changed with the knowledge of more than one person.
Receiver number	The central monitoring station computer uses the receiver number to identify individual SecureStream IP Receivers. The number precedes the error code.
Security	This allows you to add a security password to a Challenger panel. Depending on operator permissions, this password can also be 'uncloaked' so the password is visible (i.e. instead of seeing asterisks).
TITAN	See <i>Management software</i>
TITAN IP mapping	Maps the TITAN computer addresses to the Challenger IP addresses.
Upload	Fetches or collects data from Challenger to SecureStream IP or TITAN.
Watchdog	When one SecureStream IP fails (this could be the main or backup) the next SecureStream IP takes its place. The replacement changes its poll rate to match the poll rate of the SecureStream IP Receiver it replaces.

Index

A

Ademco CID, 25
application status, 24
ARES, 8, 35

B

backup functions, 16

C

Challenger events, 8
Challenger panel
 programming, 29
Challenger port, 16
Checking your SecureStream IP license status, 46
CID data, 51
CID error codes, 57
 SecureStream IP, 57
 TS0898, 57
CID events, 20
CID message code, 19
circuit number, 16
compatible hardware and software, 5
configuration editor, 15
 application status tab, 24
 details tab, 16
 encryption keys tab, 17
 M/C comms tab, 20
 monitoring tab, 22
 panels offline tab, 22
 TITAN IP mapping tab, 23
 warning events tab, 19
connecting SecureStream IP to a central monitoring station, 51
connecting TITAN management software, 23, 55

D

Dedicated Micro Systems, 5
default password, 43
dialler backup, 21
download, 10, 26

E

encryption, 8, 13
encryption key, 17
event acknowledgement, 9
event masking, 31
event retry, 9
event-driven mode, 12

F

Finder, 28
firewall, 54
Forcefield, 8, 35

G

Glossary, 59

H

heartbeat, 9
how to find a Challenger panel, 28, 30, 32, 33, 35, 37, 38
how to install SecureStream IP, 52
how to set up a Challenger panel, 28, 29
how to set up SecureStream IP Receiver, 50

I

installing SecureStream IP licenses, 45
installing SecureStream IP Receiver, 50

GE Security Pty Ltd

IP address, 13
IP port, 16
IP timeouts, 36

J

Jetapp configuration editor, 15

L

language support, 53
library, 59
license
 30-day grace, 20, 45, 47
 installing, 45, 47
 options, 45
 status, 46
 troubleshooting, 48
live session control, 31
logging in to SecureStream IP, 11

M

management software
 ARES, 5
 Forcefield, 5
 TITAN, 6
MasterMinder, 5, 21, 22
monitor resolution, 53

N

navigation icons, 7

O

operator
 adding new, 41
operators, 12, 39
out-of-sequence event, 16

P

panel
 computer address, 30
 encryption, 33
 event acknowledgement, 36
 heartbeat, 36
 IP address, 30
 IP information, 33
 maximum number, 45
 ping, 30
 security password, 37
 time zone, 31
panel editor, 26
 area reporting tab, 38
 details tab, 30
 encryption key tab, 33
 general control tab, 38
 IP information tab, 33
 IP timeouts tab, 36
 line management tab, 31
 live session control tab, 31
 miscellaneous tab, 38
 security password, 37
 telephone numbers tab, 38
panels offline, 22
parcels, 39
password
 default, 43
password
 add new, 43
 change, 44
permissions. *See* qualifications

- programming
 - Challenger panel, 29
 - SecureStream IP, 15

Q

- qualification
 - adding new, 40
 - assigning, 43
 - editing, 40
- qualifications, 12, 39

R

- raw event data, 31
- receiver number, 16
- re-installing SecureStream IP licenses, 45

S

- SecureStream IP, 5
 - functionality, 5
 - icons, 7
 - installing, 52
 - logging in, 11
 - overview, 5
 - programming, 15
 - system layout, 5
- SecureStream IP license options, 45
- SecureStream IP Receiver, 5
 - designated 'backup', 9, 10, 22
 - designated 'disaster', 9, 10, 22
 - designated 'main', 9, 10, 22
 - installing, 50
 - troubleshooting, 51, 58
- serial communications, 20, 51

T

- technical support, 58
- third-party software, 9
- time zone, 52, 53
- TITAN, 5, 9, 21, 23, 55
 - connecting, 55

- TITAN IP mapping, 23
- troubleshooting, 48, 51, 58
- troubleshooting central monitoring stations, 51
- TS0894, 6
- TS0898, 6, 9, 12, 25
- TS2000, 5, 6, 8
- TS9080, 45
- TS9081, 45
- TS9082, 45
- TS9082B, 45
- TS9082E, 45
- TS9083, 45
- TS9084, 45
- TS9085, 45
- typical system layout, 5

U

- UDP/IP mode, 12
- upgrading SecureStream IP licenses, 45
- upload, 10, 26

W

- warning event, 19
- working with Challenger panels, 25
- working with operators, 39
- working with qualifications, 39
- working with the Application Status tab, 24
- working with the Communication tabs, 38
- working with the Details tab, 16
- working with the Encryption Keys tab, 17
- working with the Ethernet tabs, 33
- working with the Monitoring tab, 22
- working with the panel editor, 30
- working with the Panels Offline tab, 22
- working with the security password, 37
- working with the Serial Comms, 20, 51
- working with the TITAN IP Mapping tab, 23
- working with the Warning Events tab, 19

GE Security Pty Ltd
646 Whitehorse Rd
Mitcham, Victoria 3132
Australia

A.B.N. 84 086 771 404
Phone +61 3 9259 4700
Fax +61 3 9259 4799
E-mail: techsupport@indsys.ge.com

Copyright © GE Security Pty Ltd 2002
All Rights Reserved



imagination at work

Part number: MAPRG-JETSTREAM
Issue: 2.0