S1600e
User Manual

Intelligent Security & Fire

SmartSight®

Expanding vision **beyond** wired networks

S1600e™
Firmware Release 2.60

User Manual

Intelligent Security & Fire

SmartSight™

Copyright © SmartSight Inc., 2003

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical or otherwise, without the prior written permission of SmartSight.

S1600e™ User Manual
Firmware Release 2.60

Published by:

SmartSight Networks Inc.
1800 Berlier Street
Laval (Quebec)
Canada
H7L 4S4
www.smartsightnetworks.com

Publication date: December 22, 2003

The SmartSight logo, SmartSight, and S1600e are trademarks of SmartSight Networks Inc. Any other product names mentioned herein are the trademarks or registered trademarks of their respective owners.

While every reasonable effort has been made to ensure the accuracy of this document, SmartSight makes no warranty of any kind and assumes no responsibility for errors and omissions. No liability is assumed for incidental or consequential damages in connection with or arising from the use of the information contained herein.

Intelligent Security & Fire

Table of Contents

Preface vii
- Who Should Read this Manual viii
- How to Use this Manual viii
  - Contents viii
  - Conventions ix
  - Related Documentation x
- About Us x
- Warranty xi

Chapter 1 ◆ Overview 1
- About the S1600e 2
  - Physical Characteristics 2
  - Security 2
  - Video 3
- Shipment 3
- Unit Casing Description 4

Chapter 2 ◆ Network Planning 5

Chapter 3 ◆ Configuring and Installing the Unit 7
- Configuring the Unit 8
  - Computer Requirements 8
  - Setting Unit Parameters 8
  - Performing a Point-to-Point Connection 11
- Installing the Unit 13
- Performing Serial Connections 14

Intelligent Security & Fire

Configuring the I/Os 16
Alarms 16
Audio 17
Performing a Hardware Reset 19
Status LED 20

Chapter 4 ◆ Setting Parameters with the CLI 23
Getting Started 24
Starting the CLI with Telnet 24
Using the CLI 25
Serial Port 26
Access Management 27
User Accounts 27
Security 28
System Status 30
Network 31
Advanced Menu 32
Load Default Configuration 33
Reboot System 33

Chapter 5 ◆ On-Screen Display (OSD) 35
Quadrant 2: SmartSight Logo and Video Message 36
Quadrant 3: Receiver Setup Details 37

Chapter 6 ◆ Web Interface 39
Getting Started 40
Unit Configuration 41
Serial Port 42
Access Management 44
System Status 46
Network 47
Video 48
VSIP 50
Audio 51
System Time 53
HTTP (Webserver) 54
Live Video 55
Presentation Windows 56
PTZ Controls 57

Appendix A ◆ Factory Default Configuration 59

Appendix B ◆ RS-485 Multidrop Connections 61

Appendix C ◆ DHCP Support and APIPA Service 63

Appendix D ◆ DTE and DCE Connections 65

Intelligent Security & Fire

Appendix E ◆ CLI with SConfigurator 69
Appendix F ◆ CLI with HyperTerminal 73
Appendix G ◆ Audio Pinouts 79
Appendix H ◆ Technical Specifications 81
Glossary 85
Index 91
Compliance 95

Intelligent Security & Fire

Preface

The *S1600e™ User Manual* presents the information and procedures on installing, configuring, and using the SmartSight high resolution S1600e video servers.

Intelligent Security & Fire

Who Should Read this Manual

This manual is intended for managers, IT system administrators, engineers, and technicians who will use the S1600e units. It provides conceptual information on how to configure, install, and operate the units.

This manual assumes that you are familiar with:

- Installation and manipulation of electronic equipment
- General use of computers
- Microsoft Windows operating systems
- Local area networks (LANs) and basic IP data communication concepts and practices
- Pan-tilt-zoom (PTZ) platforms (cameras and keyboards)
- Web browsers

How to Use this Manual

This manual contains all the information needed to install, configure, and use an S1600e unit.

Contents

The *S1600e User Manual* is divided into the following chapters:

1 **Overview**—Provides a brief description of the features of the S1600e and illustrations of its casing.

2 **Network Planning**—Describes planning operations relative to the IP network over which the S1600e units will work.

3 **Configuring and Installing the Unit**—Presents the configuration and installation procedures for the S1600e unit.

4 **Setting Parameters with the CLI**—Explains how to program the S1600e unit using the SmartSight command line interface (CLI).

5 **On-Screen Display (OSD)**—Presents the four quadrants on the receiver unit.

Intelligent Security & Fire

6 **Web Interface**—Explains how to use the Web interface to configure the unit and view live video.

The manual also includes the following appendixes:

A **Factory Default Configuration**—Lists the default parameter values of the S1600e unit.

B **RS-485 Multidrop Connections**—Presents the 2-wire and 4-wire RS-485 multidrop connections.

C **DHCP Support and APIPA Service**—Explains how the dynamic host configuration protocol server and the Microsoft APIPA service work.

D **DTE and DCE Connections**—Presents diagrams explaining how to differentiate and connect data terminal equipment (DTE) and data communication equipment (DCE).

E **CLI with SConfigurator**—Explains how to access the command line interface with the SConfigurator tool.

F **CLI with HyperTerminal**—Explains how to access the command line interface with the Windows HyperTerminal tool.

G **Audio Pinouts**—Presents the audio specifications.

H **Technical Specifications**—Lists the complete technical specifications of the S1600e unit.

A glossary, an index, and compliance information complete the manual.

Conventions

The following typographic conventions are used throughout this manual:

Visual cue	Meaning
Connect to	The name of a window, dialog box, field, or any other interface element. The value of an interface element.
File > **Properties**	Any sequence of steps (in the menu structure of a graphical application, in the navigation structure of a Web site, and so on).
connection_name	Text that must be replaced by a user-supplied value. Text representing variable content.
`UNIT_1`	The name of a command, file, or directory. Text that appears on the screen. Examples of user-supplied values.

Intelligent Security & Fire

Related Documentation

In addition to this manual, the following documentation is also available:

- *S1600e Quick Installation Guide*—Contains the S1600e configuration steps and the installation procedure.
- *SConfigurator User Manual*—Presents the instructions on how to use a SmartSight proprietary software to configure the S1600e unit, connect it to other units, and update its firmware.
- *Release Notes*—Contain information about S1600e upgrades and known issues still under investigation, as well as a description of features not covered in this version of the documentation.

All these documents are contained on the *SmartSight Utilities* CD shipped with the S1600e unit. Furthermore, a paper copy of the *Quick Installation Guide* is included with your order.

About Us

Positioned at the intersection of wireless and digital video streaming, SmartSight, based in Quebec (Canada), is dedicated to developing video solutions for CCTV and IP networks that deliver real-time video content over LAN, wireless LAN, WAN, Internet, and 2.5/3 G cellular networks. SmartSight's networked digital video solutions enable video management and monitoring primarily for security, surveillance, and asset protection in airports, government, municipal, and transportation facilities as well as corporate enterprises. SmartSight also offers ISPs and ASPs a tool to provide real-time video broadcast over the Internet.

Web Site

Our Web site is located at www.smartsightnetworks.com. You can use it to download the products specifications, application notes, and user documentation, as well as to request the latest versions of firmware and software (under **Support** > **Downloads**).

Intelligent Security & Fire

Support

If you encounter any type of problem after reading this manual, contact your local distributor or SmartSight representative. You can also use the **Support** section on our Web site to find the answers to your questions. Submit questions, inquiries, and comments in the **Requests** subsection, or browse our solution database (**FAQ**) holding resolved issues.

SmartSight technical support personnel is available to help you use your units and the related software.

To reach technical support	
On the Web:	**Support** section on www.smartsightnetworks.com
By phone:	1 888 494-7337 (North America) or +1 450 686-9000 Monday to Friday, from 8:30 to 18:00 EST
By fax:	+1 450 686-0198

Warranty

Each standard product manufactured by SmartSight is warranted to meet all published specifications and to be free from defects in material and workmanship for a period of one year from date of delivery as evidenced by SmartSight packing slip or other transportation receipt. Products showing damage by misuse, abnormal conditions of operation or products which have been modified by Buyer or have been repaired or altered outside SmartSight factory without a specific authorization from SmartSight shall be excluded from this warranty. SmartSight shall in no event be responsible for incidental or consequential damages including without limitation, personal injury or property damage.

SmartSight responsibility under this warranty shall be to repair or replace, at its option, defective work or parts returned to SmartSight with transportation charges to SmartSight factory paid by Buyer and return paid by SmartSight. If SmartSight determines that the Product is not defective within the terms of the warranty, Buyer shall pay all costs of handling and transportation. SmartSight may, at its option, elect to correct any warranty defects by sending

Intelligent Security & Fire

its supervisory or technical representative, at SmartSight expense, to customer's plant or location. SmartSight shall in no event be responsible for incidental or consequential damages including, without limitation, personal injury or property damage.

Since SmartSight has no control over conditions of use, no warranty is made or implied as to suitability for customer's intended use. There are no warranties, expressed or implied, except as stated herein. This limitation on warranties shall not be modified by verbal representations.

Equipment shipped ex works SmartSight factory shall become the property of Buyer, upon transfer to the common carrier. Buyer shall communicate directly with the carrier by immediately requesting carrier's inspection upon evidence of damage in shipment.

Buyer must obtain a return materials authorization (RMA) number and shipping instructions from SmartSight prior to returning any product under warranty. Do not return any SmartSight product to the factory until RMA and shipping instructions are received.

Intelligent Security & Fire

1

Overview

Designed for video monitoring and surveillance over IP networks, the S1600e video server is a self-contained solution delivering high quality MPEG-4 video at 30 frames (60 fields) per second over 10/100Base-T networks. The video server can easily be extended over local and wide area networks (LANs and WANs) or the Internet using ISDN, PSTN, or xDSL routers. It is built on open standards to provide long-term investment protection.

The S1600e enables configuration and video viewing from Web browsers. For instance, if you are using a PTZ camera, you will be able to control it directly from your Web browser.

This unit is for indoor use only.

Intelligent Security & Fire

About the S1600e

Each unit is configured to interface, right out of the box, with the most popular camera data port configuration (4800 baud, 8 data bits, no parity, 1 stop bit).

Physical Characteristics

An S1600e server can be a receiver (*-R*) or a transmitter (*-T*). You can also purchase an S1600e-T unit with the extended temperature option.

Unless otherwise specified, the word *S1600e* refers to any of these units.

The S1600e transmitter and receiver units have two independent serial ports (for RS-232 and RS-422/485 protocols) and a reset button.

You power the S1600e units with 12V DC.

Security

Every S1600e unit comes with a unique SSL (secure sockets layer) certificate for securing its IP link. SSL is a commonly used protocol for managing the security of IP message transmission. Therefore, the connections between two units or between a unit and the SConfigurator tool can be secured.

The SSL protocol secures the following data: I/O, serial port, and VSIP communication. It does not apply to audio and video transmission.

Once a unit is in secure mode, you cannot access it anymore with Telnet, you access its Web interface in secure mode only, and you cannot perform firmware updates through the IP network on it. However, you can configure it with SConfigurator.

For more information about this security feature, refer to the *SConfigurator User Manual*.

Intelligent Security & Fire

Video

The S1600e units can have the following video resolutions:

Resolution	Number of columns	Number of lines	
	NTSC/PAL	NTSC	PAL
QCIF	176	128	144
CIF	352	240	288
2CIF	352	384	448
2CIFH (*All columns*)	704	240	288
4CIF	704	480	576
All lines	352	480	576

The frame rate of the units can be:

- NTSC—1, 2, 3, 5, 10, 15, or 30 frames per second (fps)
- PAL—1, 2, 3, 5, 8, 12, or 25 fps

For more information about these video parameters, refer to the *SConfigurator User Manual*.

Shipment

Your S1600e shipment contains the following items:

- The requested transmitter and/or receiver units

Product code	Description
S1600e-R	Ethernet receiver
S1600e-T	Ethernet transmitter
S1600e-XT	Ethernet transmitter for extended temperature
ProductCode-A	Transmitter or receiver with bidirectional audio

- A 12V DC external power supply (for North America only)
- The *SmartSight Utilities* CD containing the documentation and release notes for the unit as well as the SConfigurator application
- The *S1600e Quick Installation Guide*

The shipment may also contain the following option:

- A 10-unit rack mount panel (*SRM10*)

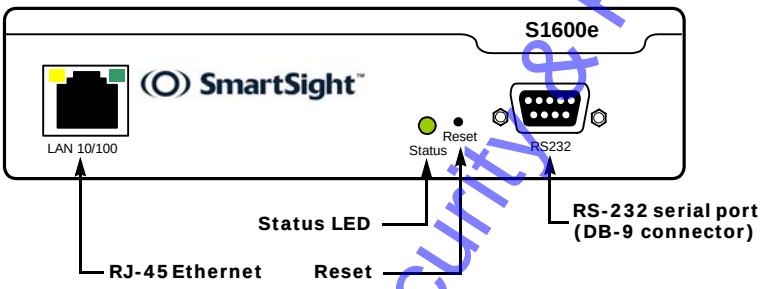
Intelligent Security & Fire

Unit Casing Description

The S1600e electronics are enclosed in a non-weatherproof extruded aluminium casing that is not meant for outdoor use.

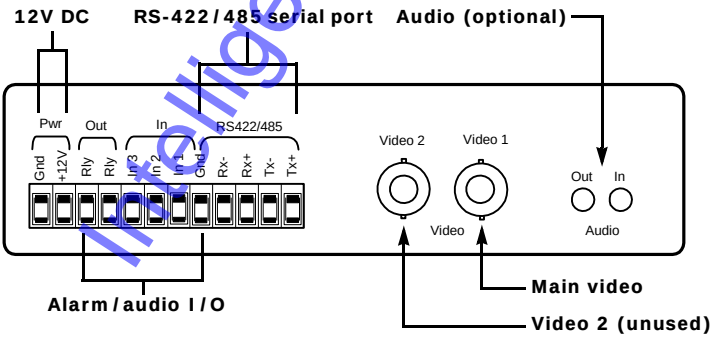
The front panel consists of:

- An RJ-45 jack
- A system status LED
- A reset button
- A female DB-9 connector for RS-232 use



The back panel consists of:

- A 12-pole connector for power, input/output, and RS-422/485
- One female BNC connector to be used as video input or output
- Optional audio connectors



Intelligent Security & Fire

2

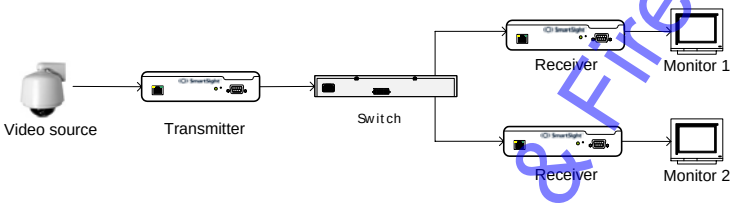
Network Planning

To allow optimal configuration, you must properly plan your network.

Intelligent Security & Fire

It is critical to ensure that no IP link of more than 300 feet (100 meters) be present in a network, unless otherwise stated by connection equipment such as 100Base-T to SC converters, which can offer a 1.25-mile (2-km) range.

The S1600e supports a streaming method called *multicast*, which permits more than one receiver unit to view a video stream at any one time. Here is a typical connection for a point-to-multipoint application.



Intelligent Security & Fire

3

Configuring and Installing the Unit

To prepare your S1600e unit for operation, you have to perform a series of steps:

- Basic configuration, mainly for communication and serial connection
- Physical installation in its final location
- Alarm and audio configuration
- Connection to the serial ports

Remember that your unit is an indoor product that cannot support an outdoor environment.

Intelligent Security & Fire

Configuring the Unit

The following configuration steps are required:

- Setting a series of parameters, including the IP address
- Performing a point-to-point connection

Computer Requirements

The minimum software and hardware requirements for the computer needed to configure the unit are:

- Windows 2000 Service Pack 2 or higher, or Windows XP
- Network card
- Serial port

Setting Unit Parameters

The first step in installing an S1600e system is to change the IP address of the unit to ensure compatibility with an existing network. The default IP addresses of all units are based on the APIPA service and will be in the range 169.254.*X*.*Y*, where *X* and *Y* are relative to the MAC address of the individual unit; for more information about the APIPA service, see page 63.

To work properly, units on the same network must have unique IP addresses. The unit will not prevent you from entering a duplicate address. However, its system status LED will turn to flashing red; then the unit will reboot with an APIPA address. If the unit is a receiver, the “Duplicate IP Detected” message will also appear in the on-screen display (for more information about this display, see Chapter 5, page 35).

You can set the IP addresses of a unit by two methods:

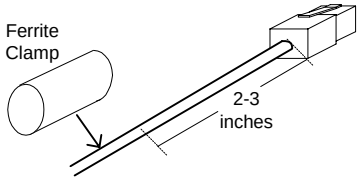
- Connecting your unit to the same LAN as the computer running SConfigurator (described next)
- Using the command line interface (see page 31)

Next, you have to set the serial port parameters of the unit.

Intelligent Security & Fire

To set the parameters of a unit:

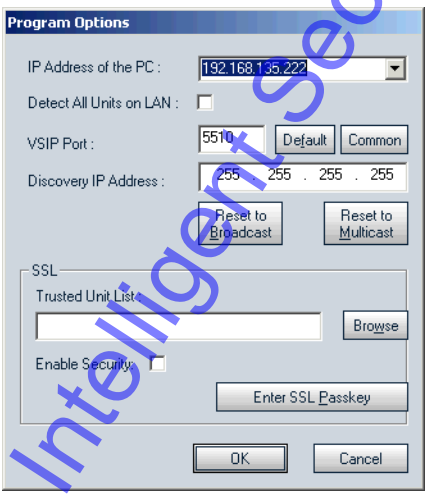
1. In a lab, unpack the unit and set it on a table.
2. Plug the S1600e IP connector directly to a computer using a crossover cable or to your LAN using a straight-through cable.
3. Install the ferrite snap-on clamp on the Ethernet cable:



4. Power the unit.
5. Start the SConfigurator software included on the *SmartSight Utilities* CD shipped with your equipment.

   The **SConfigurator** window appears.
6. From the **General** tab, click **Program Options**.

   The **Program Options** window appears.

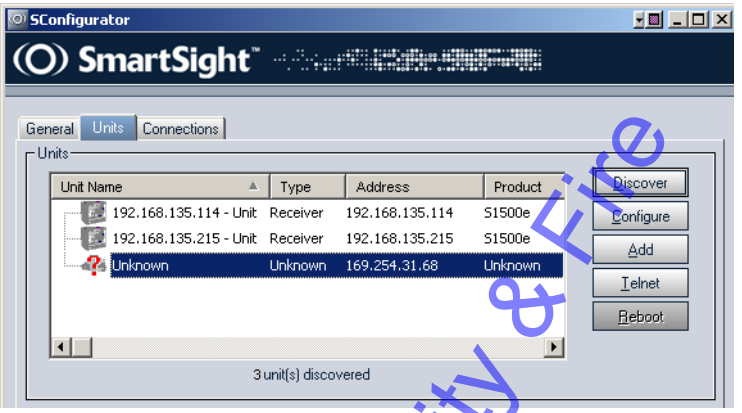


7. Ensure that the **VSIP Port** value is 5510; otherwise, click **Default**.
8. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.
9. Check **Detect All Units on LAN**, then click **OK**.

Intelligent Security & Fire

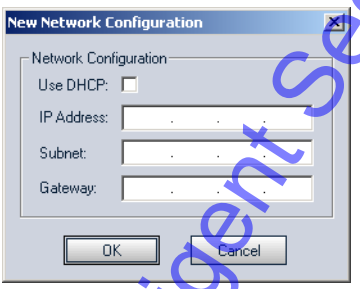
10 Choose the **Units** tab, then click **Discover**.

A unit of type “Unknown” with a 169.254.*X*.*Y* IP address appears in the list; it corresponds to your new unit.



11 Select the unknown unit, then click **Configure**. In the **Reconfigure unit?** confirmation window, click **Yes**.

The **New Network Configuration** window appears.



12 To use DHCP (dynamic host configuration protocol), check **Use DHCP**. Otherwise, enter the IP address, subnet mask, and gateway of the unit, as provided by your network administrator.

For more information about DHCP, see page 63.

13 Click **OK**.

The unit reboots with its new network configuration.

14 In the **Units** tab, click **Discover**.

The new S1600e unit appears.

15 Select the unit, then click **Configure**.

Intelligent Security & Fire

16 Configure the serial port parameters to match those of the target equipment (for instance, camera or PTZ keyboard).

For more information, refer to the *SConfigurator User Manual*.

The S1600e initial configuration is now complete. You perform further configuration with SConfigurator.

Performing a Point-to-Point Connection

To allow transfer of video, audio, I/O, and serial data, you have to create a connection between a transmitter and a receiver. Typically, both units sit on the same IP subnet as SConfigurator and have the same VSIP port; to access other units, refer to the unit discovery section in the *SConfigurator User Manual*.

Note

The two units must have the same firmware version, with the following exception: The S1504e and S1508e, both at firmware release 3.0, will work with an S1600e receiver at version 2.60.

For more information about the connection process, refer to the “Managing Connections” chapter, also in the *SConfigurator User Manual*.

To perform a point-to-point connection:

1 Start SConfigurator.

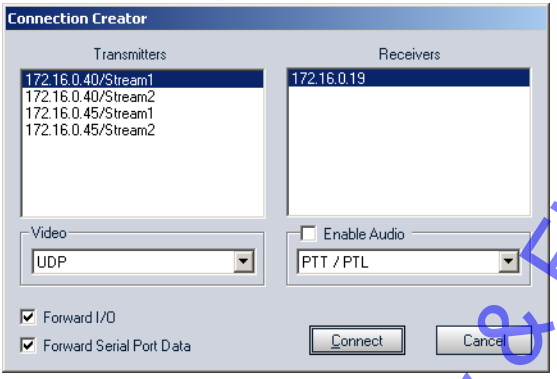
2 In the **Units** tab, discover the desired units.

The discovered units appear in the **Units** box.

Intelligent Security & Fire

3 Choose the **Connections** tab, then click **Add**.

The **Connection Creator** window appears.



4 Select a Stream2 transmitter in the left column and a receiver in the right one. On the S1600e-T units, Stream1 is reserved for Web viewing.

5 To disable I/O data transmission (for example, alarms), clear **Forward I/O**.

6 To disable serial port data transmission (like PTZ commands), clear **Forward Serial Port Data**.

7 To enable audio, check **Enable Audio**, then select the audio mode.

8 Click **Connect**.

You should now have video on the monitor connected to the receiver unit.

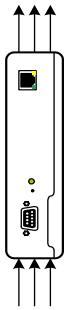
Intelligent Security & Fire

Installing the Unit

Once your system is successfully configured, it is ready to be installed in its final location.

To install the system:

1. On the transmitter, plug the video cable of the dome or camera to the video connector.
2. On the receiver, plug the video input cable of the monitor to the video connector.
3. Connect the RS-422/485 serial port of the unit to the target device (for instructions, see page 14).
4. Plug the network cable to the RJ-45 Ethernet connector on the unit.
5. When installing an S1600e-XT unit, make it stand vertically, allowing for better cooling.



Intelligent Security & Fire

Performing Serial Connections

The S1600e units hold connectors for two serial ports: RS-232 and RS-422/485.

RS-232

Use the following wiring scheme to plug a serial cable to the DB-9 connector in the back of the unit:

DB-9 pin number	Cable signal name
2	RxD
3	TxD
5	Signal ground
7	RTS
8	CTS

RS-422/485

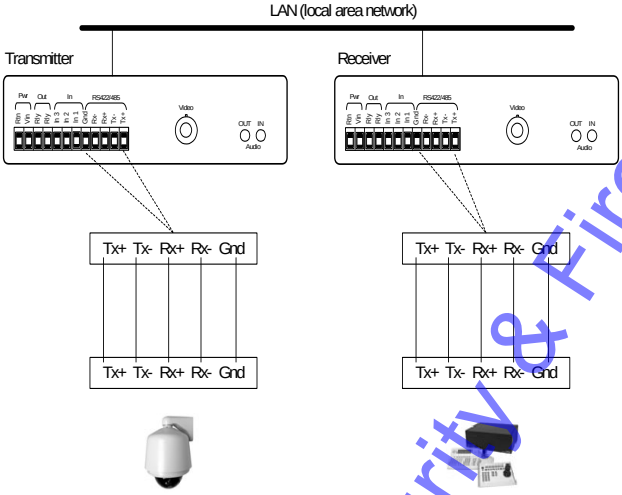
To use the RS-422/485 functionality, you have to connect a twisted pair cable to the multipole connector on the back of the unit. The connector gives access to the Tx+, Tx-, Rx+, Rx-, and Gnd signals.

To properly connect an RS-422/485 serial connection using four wires, use the following wiring scheme:

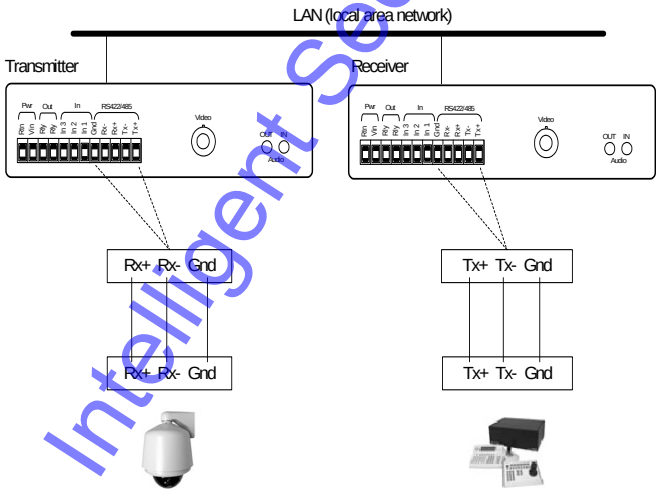
Target device connector	S1600e connector
Tx+	Tx+
Tx-	Tx-
Rx+	Rx+
Rx-	Rx-
Gnd	Gnd

Intelligent Security & Fire

For the RS-422/485 bidirectional protocols, the setup is the following:



For the RS-422/485 Pelco P or D protocols, you connect the serial port the following way:



A typical connection of a multidrop RS-485 network (a number of terminals sharing the same line) is presented in Appendix B, page 61.

Intelligent Security & Fire

Configuring the I/Os

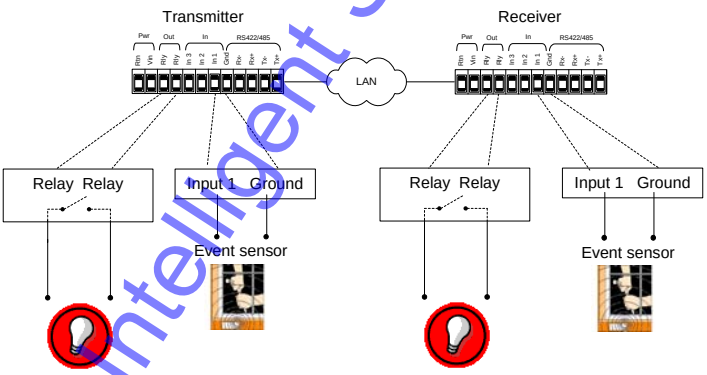
The input/output features on the multipole connector on the back of the unit are bidirectional and are used for alarm (or events) and audio. There are three input and one output terminals. Each terminal has a dedicated purpose:

- Input 1—Either transparent alarm links in a point-to-point configuration or PTL (push-to-listen) audio transmission mode.
- Input 2—PTT (push-to-talk) audio transmission mode.
- Input 3—Unused.
- Output—Relay for the input 1 signal.

You cannot program audio and alarms at the same time, since both contexts require input 1.

Alarms

All S1600e units can generate and receive alarms. To configure alarms in a point-to-point configuration, you plug the event sensor to the input 1 and ground terminals of the connector (typically on a transmitter unit), and your alarm system to the Out section of the receiver. For example:



With SConfigurator, you activate the alarm process by checking the **Forward I/O** box in the **Connection Creator** window.

Intelligent Security & Fire

Audio

If audio is supported, two 3.5 mm jacks are installed on the units. Appendix G, page 79, presents the jack pinouts for input and output.

Data Transmission

Two transmission modes for audio data are available:

- Full duplex—Data is transferred in both directions simultaneously.
- PTT/PTL—The push-to-talk/push-to-listen mode allows you to control audio communication between two units.

When creating a point-to-point connection between a receiver and a transmitter in SConfigurator, you set the transmission mode in the **Connection Creator** window.

The PTT/PTL transmission mode requires specific hardware configuration:

- To activate the audio reception circuit (for PTL) on receiver units, you have to short the input 1 and ground terminals on the multipole connector. You cannot activate PTL on transmitters.

Note

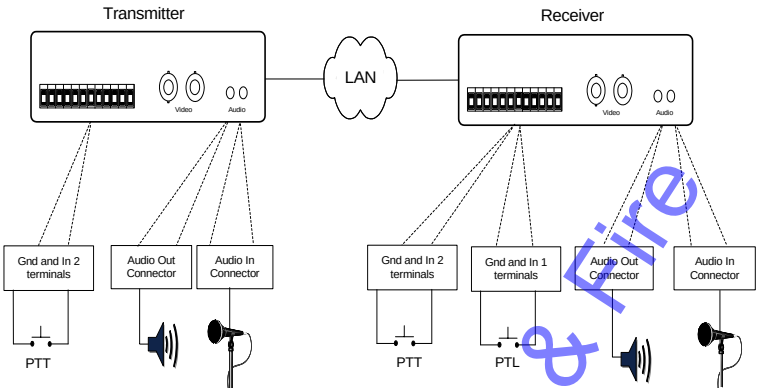
The input 1 terminal is also used for alarms. It will perform both functions if you set up the PTL mode.

- To activate the audio transmission channel (for PTT), you must trigger an activation switch (for example, a button) that is based on the shorting of the input 2 and ground terminals.

If both the transmitter's and receiver's PTT switches are activated at the same time, the receiver will have precedence. Audio will be transferred from the receiver to the transmitter. If the receiver's PTL and PTT functions are activated at the same time, PTT will be activated and PTL will be ignored.

Intelligent Security & Fire

Here is a typical PTT/PTL application:

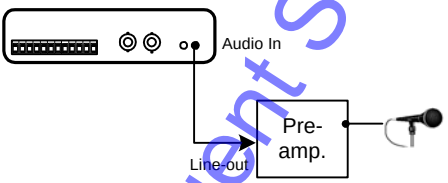


Audio Input/Output Types

The unit supports the following audio input types:

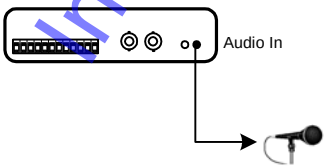
- Line-in—To use a 3.5 mm jack (default).

  In this mode, you need a pre-amplifier. You connect the audio input on the unit to the Line-out connector on the pre-amplifier.



- Mic (with pre-amp)—To use a multimedia microphone (Electret). Most multimedia microphones use a 3.5 mm jack.

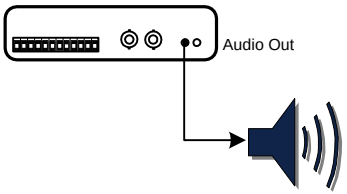
  You connect the microphone directly in the unit's audio input.



With SConfigurator, you set the input type in the **Audio** tab.

Intelligent Security & Fire

The only available output type is **speaker**: You plug a speaker directly on the audio output of the unit.



In SConfigurator's **Audio** tab, you can set one output setting, the volume.

Specifications

The audio input/output specifications are (where 0 dBV = Vrms):

Mode	Gain	Impedance	Frequency range
Mic	-38 to -21 dBV	30 Kohm	
Line-in	-20 to -3 dBV	30 Kohm	300–3600 Hz
Speaker	-45 to -3 dBV	8 ohms min.	

Performing a Hardware Reset

You can perform a hardware reset on the unit. This operation will assign the factory default settings to the parameters of the unit (listed in Appendix A, page 59). All user-defined values will be lost. To reset the parameters to their factory defaults without performing a hardware operation, see page 33.

Following a reset, you will need to reprogram the S1600e unit (for instance, its IP address and VSIP port) for proper operation within its network.

Depending on the date the unit was released from factory, it may or may not have a Reset button on the front panel.

To perform a hardware reset with the Reset button:

1. Press and hold the Reset button.

   The system status LED flashes red very rapidly.

2. Hold the button for an additional five seconds, until the LED turns off.

The unit reboots with the default parameters.

Intelligent Security & Fire

To perform a hardware reset on a unit without a Reset button:

1. Power down the unit.
2. Short the TxD and CTS wires together (pins 3 and 8 on the DB-9 connector).
3. Power up the unit and wait until the normal boot-up sequence is completed.
4. Remove the short on the TxD and CTS pins.

The unit reboots with the default parameters.

Status LED

The system status LED is a bicolor (green-red) LED providing detailed information on the current state of the system.

Condition	Indication	-T	-R
Steady red	The unit is powering up.	✓	✓
Flashing red (1 sec. intervals)	The IP address of the unit is already assigned to another unit in the network.	✓	✓
Flashing green (3 sec. intervals)	The firmware has started, but the unit is not connected to the network.	✓	✓
Flashing green (1 sec. intervals)	The firmware has started, the unit is connected to the network, but no video/audio/serial* data is transmitted.	✓	
	The firmware has started, the unit is connected to the network, but no video is received or audio/serial* data is received or transmitted.		✓
Flashing green (0.2 sec. intervals)	The firmware has started, the unit is connected to the network, and video/audio/serial* data is transmitted.	✓	
	The firmware has started, the unit is connected to the network, and video is received or audio/serial* data is received or transmitted.		✓
Three consecutive red blinks every 2 sec.	No video source is detected and no video is transmitted.	✓	
Flashing green-red (1 sec. intervals)	The unit is undergoing a firmware update.	✓	✓
Flashing red (0.1 sec. intervals)	The unit is being identified.	✓	✓
One red blink	A video packet is lost. In the worst case, it could flash at 5 Hz.		✓

Intelligent Security & Fire

* At least one of them must be transferred to obtain the LED condition.

Warning

The following power-up conditions are abnormal:

- LED not lit: Check the power supply and cabling. If power is available and the LED stays off, call SmartSight technical support for assistance.
- Steady red LED: There is an internal error that prevents the unit from starting normally. Power down and power back up the unit once. If the condition persists, proceed to a firmware update (for details, refer to the *SConfigurator User Manual*). If the update fails or the condition persists after the update, call SmartSight technical support for assistance.
- Flashing red LED (2 second intervals): There is an internal error that prevents the unit from operating normally. This situation may happen after a firmware update or after the first boot-up. Power down the unit and call SmartSight technical support for assistance.
- Flashing green-red LED not during a firmware update: The unit is in backup mode; you will need to perform a firmware update using a serial connection.

Intelligent Security & Fire

4

Setting Parameters with the CLI

The S1600e units come with a simple command line interface (CLI) for configuration purposes. The CLI is hierarchically organized, with menus, sub-menus, and individual options representing configuration parameters. Only the parameters that you are likely to change are described.

Intelligent Security & Fire

Getting Started

You can access the CLI the following ways:

- With a network connection and the Telnet command
- With a serial connection and the SConfigurator utility (see Appendix E, page 69)
- With a serial connection and a terminal emulation program such as HyperTerminal (see Appendix F, page 73)

Starting the CLI with Telnet

You can use the Telnet command to open the command line interface of the S1600e.

Note

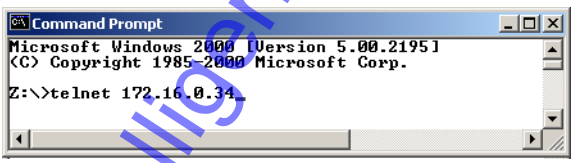
Ensure that your PC and the S1600e unit are in the same IP subnet.

To enter the CLI with Telnet:

1. Start the **Command Prompt** Windows accessory.

   A **Command Prompt** window appears.

2. At the command line, type telnet followed by the IP address of the unit, then press **Enter**.



Intelligent Security & Fire

The CLI main menu appears.

```
******************************
Main Menu
------------------------------
Menus:
1) Serial Port
2) Access Management
3) System Status
4) Network
5) Ethernet Communication
6) Advanced

Commands:
s) Save Settings
r) Reboot System
l) Load Default Configuration
q) Quit
******************************
```

The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

- The “Thank you for using the SmartSight CLI.” message appears at the command line.
- You are brought back at the **Command Prompt** command line.

3 To reactivate the CLI, re-enter the telnet command.

4 To end the CLI work session:

- Save the settings by entering **s** at the main menu, then pressing **Enter**.
- Exit the CLI by entering **q** at the main menu, then pressing **Enter**.

Using the CLI

To work through the CLI menu structure, follow these guidelines:

- To execute a command or open a menu, type in the corresponding letter or number, then press **Enter**.
- Entering **p** returns you to the previous menu, until you are back in the main menu.
- Entering **s** in the main menu saves all the changes you have made in the work session.
- To exit, enter **q** in the main menu. Depending on the changed settings, the unit may perform a soft boot.

Intelligent Security & Fire

Serial Port

The Serial Port menu enables you to establish the proper settings ensuring compatibility between the S1600e unit and your serial equipment (for example, dome, keyboard, matrix, multiplexer, or access card). For more information about the serial port settings of the specific product with which you want to interface, refer to its user manual or contact your product manufacturer.

You have access to two independent serial ports.

```
************************
Main Menu \ Serial Port
-----------------------

Menus:
1) RS-232
2) RS-422/485

Commands:
p) Previous Menu
************************
```

For the RS-232 port, the available commands are:

```
*******************************
Main Menu \ Serial Port \ RS-232
-------------------------------

Parameters:
1) Bit rate: 4800
2) Parity  : None

Commands:
p) Previous Menu
*******************************
```

For the RS-422/485 port, you can change the following settings:

```
*********************************************
Main Menu \ Serial Port \ RS-422/485
---------------------------------------------

Parameters:
1) Bit Rate                 : 4800
2) Parity                   : None
3) RS-422/RS485 Operating Mode: RS-422 4 Wires

Commands:
p) Previous Menu
*********************************************
```

Bit Rate

The bit rate represents the data rate at which the target product operates. Possible values range from 1200 bps to 230,400 bps (for a transmitter) or to 115,200 bps (for a receiver).

Intelligent Security & Fire

Parity

The serial equipment may have a parity of *odd* or *even*. It may also not have parity check; most communication devices do not use parity.

RS-422/485 Operating Mode

The operating mode setting enables you to establish the way your RS-422/485 serial equipment will interface with the S1600e unit. The supported modes are:

- RS-422 4 Wires
- RS-485 4 Wires
- RS-485 2 Wires

Access Management

The Access Management menu takes care of user accounts (user names and passwords) and unit security.

```
********************************
Main Menu \ Access Management
--------------------------------
Menus:
1) User Accounts
2) Security

Commands:
p) Previous Menu
********************************
```

User Accounts

The User Accounts menu enables you to protect the configuration of the unit by restricting its access with a user name and a password. Once the user account mode is activated, you need the user name/password combination to access the CLI through a serial connection or a Telnet session, or to open the Web interface (described on page 39).

Intelligent Security & Fire

Two types of users are available:

- Administrator—Has all rights and is automatically available when user accounts are activated
- Web client—Only has access to live video in the Web interface

```
*********************************************
Main Menu \ Access Management \ User Accounts
---------------------------------------------
Parameters:
 1) User Accounts          : Disabled
 2) Administrator User Name: USERNAME
 3) Administrator Password : PASSWORD
 4) Web Client 1 User Name :
 5) Web Client 1 Password  :
 6) Web Client 1           : Disabled
 7) Web Client 2 User Name :
 8) Web Client 2 Password  :
 9) Web Client 2           : Disabled
10) Web Client 3 User Name :
11) Web Client 3 Password  :
12) Web Client 3           : Disabled
13) Web Client 4 User Name :
14) Web Client 4 Password  :
15) Web Client 4           : Disabled
16) Web Client 5 User Name :
17) Web Client 5 Password  :
18) Web Client 5           : Disabled

Commands:
p) Previous Menu
*********************************************
```

Security

The Security menu holds commands relative to the protection of the unit. It allows you to control:

- Firmware updates through the IP network
- Access to Telnet and to the Web interface
- SSL

```
*****************************************
Main Menu \ Access Management \ Security
-----------------------------------------
Parameters:
1) IP Firmware Update     : Enabled
2) Firmware Update Port   : 12345
3) Telnet Session         : Enabled
4) HTTP Access            : Enabled
5) Secure HTTP Access     : Disabled
6) Report Monitor         : Enabled
7) Global Security Profile: Disabled
8) SSL Passkey            :

Commands:
p) Previous Menu
*****************************************
```

Intelligent Security & Fire

IP Firmware Update

You can prevent firmware updates to be performed on your unit through the IP network. By default, this type of update is allowed.

For more information about firmware updates, refer to the *SConfigurator User Manual*.

Telnet Session

By default, you can use Telnet to access the CLI of your unit. To improve the security of your system, you may prohibit such an access. In this case, the CLI will only be accessible through a serial connection (with the SConfigurator console or HyperTerminal).

HTTP Access

By default, you can access the configuration pages of the unit through the Web interface. If you block this access, you can only set up the S1600e unit with SConfigurator, Telnet, or a serial connection.

Secure HTTP Access

By default, you access the Web interface of the unit in unsecure mode (that is, with an `http://` address prefix). You can restrict this access to SSL connections only, with `https://`, provided the unit has an SSL certificate. After you activate the secure HTTP access, the user accounts (described on page 27) are automatically activated.

Global Security Profile

This command is available if the unit has an SSL certificate. If you activate the global security profile, the unit will only accept secure SSL connections. Once this profile is activated on a unit:

- You cannot access it anymore with Telnet.
- You cannot perform firmware updates through the IP network on it.
- You access its Web interface in a secure mode (that is, the secure HTTP access mode is enabled).

Intelligent Security & Fire

SSL Passkey

To secure a unit with SSL, provided of course it has an SSL certificate, you need to provide a passkey. This passkey must be the same for all units and the software tools to allow proper secure communication between them.

It is recommended to perform this operation in SConfigurator (version 2.55 or higher for the tool and the unit). Otherwise, to build a truly secure system, you should first access the CLI through a physical serial port connection, not through Telnet, therefore avoiding eavesdropping on the network.

System Status

The system status information indicates the current values of internal S1600e parameters, including the unit's serial number and firmware version. A transmitter and a receiver connected together need to be running the same firmware version.

A value of 03-03 or later in **Unit Tested** indicates that the unit has an SSL certificate.

```
**********************************************
Main Menu \ System Status
----------------------------------------------
Parameters:
   Firmware Version    : 2.60 - build 380
   Build Date          : Nov 18 2003 at 17:07:50
   CPU Info            : Rev. 1.0
   CPU Frequency       : 206250000
   Uptime              : 3 days 06:23:38
   Serial Number       : 00079a-002da4
   CPLD Version        : 0
   Flash Size          : 4
   Internal Value 1    : 9389904 / 16
   Audio Hardware      : Absent
   Unit Tested (MM-YY) : 05-03
   Unit Firmware Size  : 3456 KB
   Backup Firmware Size: 384 KB

Commands:
p) Previous Menu
**********************************************
```

Intelligent Security & Fire

Network

The Network menu allows you to configure several parameters to ensure the compatibility between the S1600e and its IP network.

```
*******************************************
Main Menu \ Network
-------------------------------------------
Parameters:
1) DHCP Configuration        : Disabled
2) Local IP Address          : 192.168.135.92
3) Subnet Mask               : 255.255.255.0
4) Gateway                   : 192.168.135.2
5) Primary DNS Server Address: 0.0.0.0
6) Backup DNS Server Address : 0.0.0.0
7) Ping Request              : 0.0.0.0

Commands:
i) Ping Remote Address
p) Previous Menu
*******************************************
```

For more information about these settings, contact your network administrator.

DHCP Configuration

DHCP (dynamic host configuration protocol) allows devices and computers connected to a network to automatically get a valid network configuration from a server. For more information about DHCP, see Appendix C, page 63.

You can set this option only if the S1600e is connected to a network that uses a DHCP server.

Local IP Address

The IP address is the identifier of the S1600e on the network. The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number is in the 0-255 range. Each device on a network must have a unique IP address.

Subnet Mask

The subnet mask is the binary configuration specifying in which subnet the IP address of the unit belongs. A subnet is a portion of a network that shares a common address component. On TCP/IP networks, a subnet is defined as a group of devices whose IP addresses have the same prefix.

Unless otherwise specified by your network administrator, it is recommended to use a subnet mask of 255.255.255.0.

Intelligent Security & Fire

Gateway

The gateway represents a network point that acts as an entrance to another network.

Warning
Never use the IP address of the unit as the gateway value.

Ping Request

Ping is a basic Internet program that allows you to check that a particular IP address exists and can accept requests.

To ping a specific unit:

1. In the **Ping Request** parameter, enter its IP address.
2. Execute the **Ping Remote Address** command.

Advanced Menu

The Advanced menu holds a series of advanced setups mainly used by SmartSight technical support. Some of these configuration parameters are available through the SConfigurator utility software.

```
****************************************
Main Menu \ Advanced
----------------------------------------
Menus:
1) Video
2) Video Status
3) Test and Debug
4) Serial Port (IP)
5) VSIP
6) VSIP Statistics
7) Power Management
8) Audio
9) System Time
10) HTTP (Webserver)
11) License Management
12) Serial Port Status
13) Communication Status and Statistics

Commands:
i) Identify Unit
p) Previous Menu
****************************************
```

Intelligent Security & Fire

Identifying a Unit

To recognize an S1600e among a large set of units, you can make its system status LED flash red rapidly.

To identify an S1600e unit:

1. From the main menu, choose **Advanced**, then press **Enter**.
2. Enter **i** to make the LED flash red. Re-enter **i** to set the LED to its original state.
3. Enter **p** until you are in the main menu.
4. Enter **q** to exit.

Load Default Configuration

The Load Default Configuration command, located in the main menu, resets all unit parameters to their factory settings (described in Appendix A, page 59). All user-defined values will be lost. To reset the parameters to their factory defaults with a hardware operation instead, see page 19.

Following a reset, you will need to reprogram the S1600e unit (for instance, its IP address and VSIP port) for proper operation within its network.

Reboot System

The Reboot System command, located in the main menu, performs a soft boot on the S1600e. A system reboot clears all unsaved changes in the CLI and returns to your preset configuration.

Intelligent Security & Fire

5

On-Screen Display (OSD)

The S1600e receiver units display information on a video monitor.

Intelligent Security & Fire

The information displayed on the video monitor can be broken down into four quadrants as follows:

Quadrant 1	Quadrant 2
Quadrant 4	Quadrant 3

Quadrants 1 and 4 are unused.

If a video source is not plugged into a currently streaming receiver, quadrants 1 and 4 turn to red and quadrants 2 and 3 become blue/black.

Quadrant 2: SmartSight Logo and Video Message

In quadrant 2, when the unit is powering up, the SmartSight logo will be displayed during 30 seconds.

When a connection is created between two units, a message like the following is displayed:

`Video [192.168.135.56:46742]`

It contains the IP address of the transmitter to which the receiver is connected and the IP port used by the receiver.

Intelligent Security & Fire

Quadrant 3: Receiver Setup Details

Quadrant 3 displays basic S1600e-R configuration details, including serial port and network setup. This information is displayed during 45 seconds. For example:

```
S1600e ver: 2.60- build 380
Comm: 4800, 8, N, 1 232f-d
IpAddr: 192.168.135.97
SubNet: 255.255.255.0
Gateway: 192.168.135.1
```

Here is the description of the `Comm` line:

Serial port	Description
4800	Bit rate
8	Number of data bits
N	Parity: None
1	Number of stop bits
232f-d	Line driver

The “Duplicate IP Detection” message will be displayed if the IP address of the unit is already assigned to another machine on the network.

Intelligent Security & Fire

6

Web Interface

You can access the S1600e transmitters with your Web browser (Internet Explorer 5.5 or higher), for live viewing or configuration purposes. For instance, if you are using a PTZ camera, you will be able to control it directly on your Web browser.

The S1600e supports the Pelco P PTZ protocol.

Intelligent Security & Fire

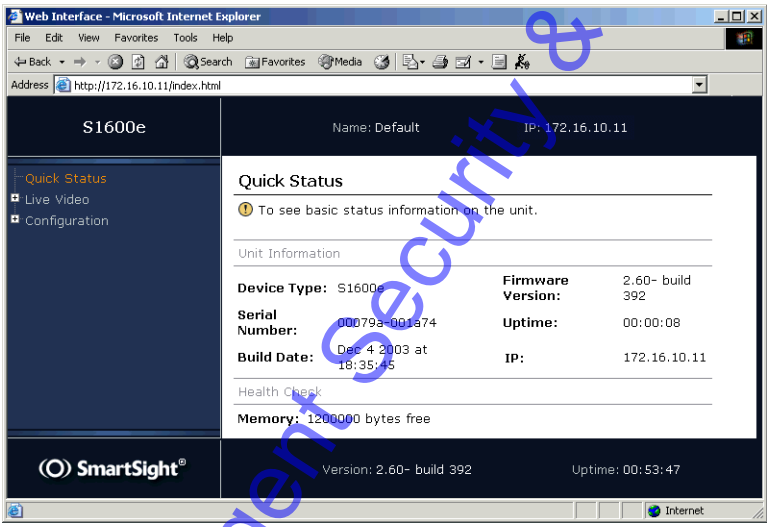
Getting Started

Depending on user account and security settings, you may have to provide a user name and password when logging into the Web interface, or access it in secure mode.

To open the Web interface the first time:

1. Start your Internet Web browser.
2. In the **Address** field, enter the IP address of the S1600e-T unit using the http://*IP_address* format.

   The Web interface window appears.



The Web interface presents three types of information:

- Quick Status—Basic information on the unit.
- Live Video—The video stream coming out of the camera connected to the S1600e transmitter.
- Configuration—A series of parameters to configure the unit.

Intelligent Security & Fire

Unit Configuration

You can configure the S1600e transmitter with the Web interface, instead of using SConfigurator or the built-in command line interface (CLI). You can set the following parameter categories:

- Serial port
- Access management
- System status
- Network
- Video
- VSIP
- Audio
- System time
- HTTP

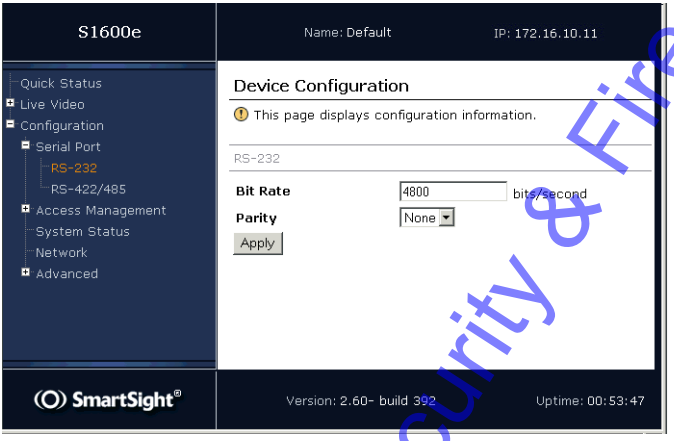
Only the parameters that you are likely to change are described.

Intelligent Security & Fire

Serial Port

The S1600e unit has two serial ports, RS-232 and RS-422/485, for communicating with serial equipment (for example, cameras or domes).

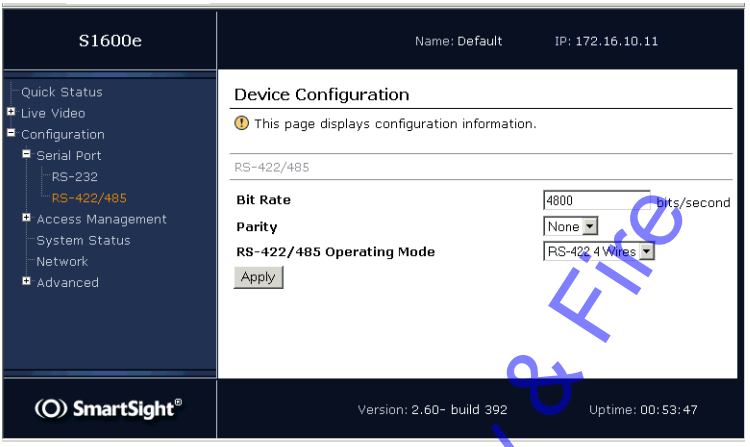
The RS-232 parameters are:



Parameter	Description
Bit rate	The data rate of the target product.
Parity	The quality of being either odd or even. There can also be no parity check.

Intelligent Security & Fire

The RS-422/485 parameters are:



Parameter	Description
Bit rate	The data rate of the target product.
Parity	The quality of being either odd or even. There can also be no parity check.
RS-422/485 Operating Mode	The way your S1600e unit will interface with the RS-422/485 serial equipment. Three modes are supported: RS-422 4 Wires, RS-485 4 Wires, and RS-485 2 Wires.

Intelligent Security & Fire

Access Management

Access management takes care of user accounts and unit security.

User Accounts

With user accounts, you can protect the configuration of the unit by restricting its access with a user name and a password. Once the user account mode is activated, you need the user name/password combination to access the CLI through a serial connection, a Telnet session, or the Web interface.

Two types of users are available:

- Administrator—Has all rights and is automatically available when user accounts are activated.
- Web client—Only has access to live video and quick status in the Web interface. Five Web clients are available.

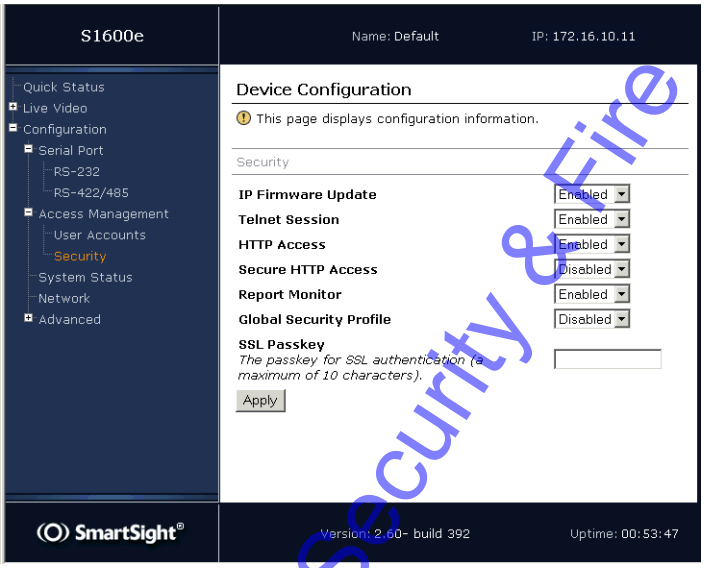
The user account parameters are:

Intelligent Security & Fire

Security

The security settings are relative to the protection of the unit. For more information, see page 28.

The parameters are:



Parameter	Description
IP Firmware Update	To enable or disable the performance of firmware updates on the unit through the IP network.
Telnet Session	To enable or disable the access to the command line interface (CLI) of the unit with Telnet.
HTTP Access	To enable or disable the access to the Web interface of the unit.
Secure HTTP Access	To enable or disable the access to the Web interface of the unit in a secure SSL context. If enabled, you access the unit with `https://` in your Web browser; furthermore, the user account mode (described on page 44) is automatically activated.
Global Security Profile	To enable or disable the complete SSL security on the unit. If enabled, you cannot access the unit with Telnet, you cannot perform firmware update over the IP network on it, and the secure HTTP access is enabled.
SSL Passkey	The passkey to secure the unit with SSL.

Intelligent Security & Fire

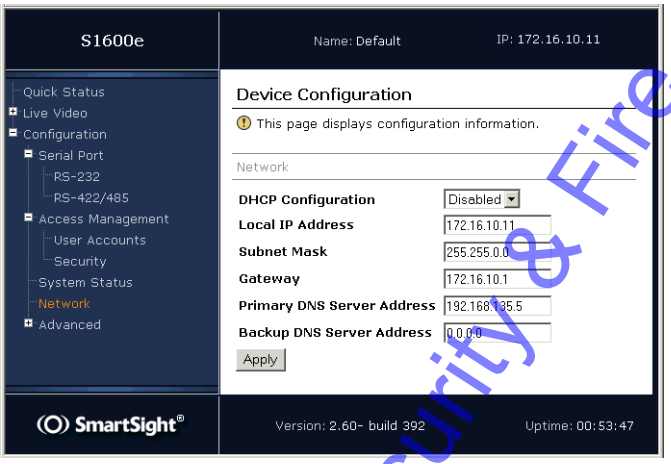
System Status

The system status information indicates the current values of internal S1600e parameters, including the unit's serial number and firmware version.

Intelligent Security & Fire

Network

The Network menu allows you to configure several parameters to ensure compatibility between the S1600e and its IP network. The parameters are:



Parameter	Description
DHCP Configuration	To enable or disable the use of DHCP (dynamic host configuration protocol) to automatically get a valid network configuration for the unit from a server.
Local IP Address	The IP address of the S1600e unit.
Subnet Mask	The binary configuration specifying in which subnet the IP address of the unit belongs.
Gateway	The IP address of the network point that acts as an entrance to another network.

Intelligent Security & Fire

Video

You can configure parameters related to the encoding of video in the unit. The parameters common to the two encoders of the S1600e unit are:

Parameter	Description
Video Standard	The analog display standard.
Brightness	The total amount of light in the color.
Contrast	The range of colors in an image.
Saturation	The vividness of a color.
Hue	The relative amounts of red, green, and blue in a color.

Intelligent Security & Fire

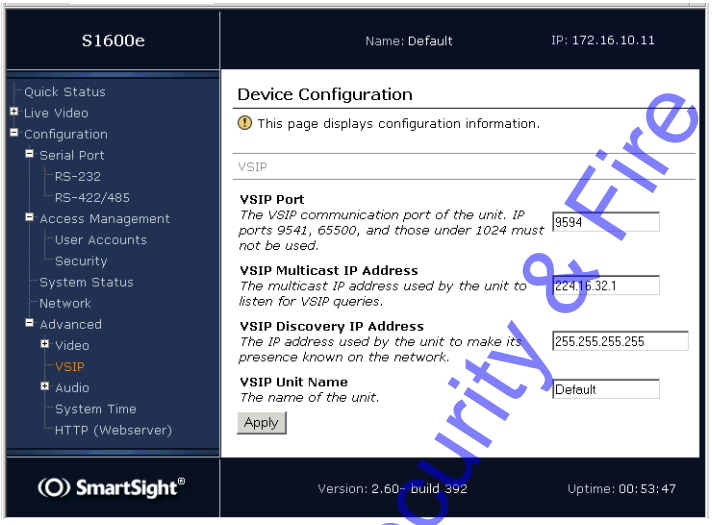
For each encoder, the video parameters are:

Parameter	Description
Transport Protocol	The protocol used to transport video.
Input Filter Mode	The level of filtering applied to the video signal before it is encoded.
Resolution	The number of pixels (columns * lines) for each picture of the video sequence.
Rate Control Mode	The mode controlling the bit rate variation.

Intelligent Security & Fire

VSIP

You can set the following parameters related to the VSIP communication protocol:



Intelligent Security & Fire

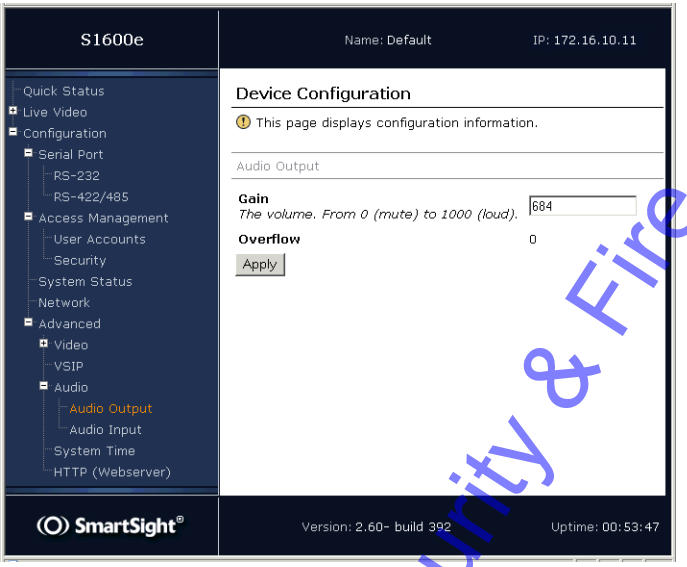
Audio

If your unit has audio capabilities, you can set general parameters, as well as specific values for the audio input and output. The general parameters are:

Parameter	Description
Audio Mode	The transmission mode for audio data.
Output Compression	The transfer mode for the audio data of the remote unit.
Input Compression	The transfer mode for the audio data of the local unit.

Intelligent Security & Fire

The audio output parameters are:



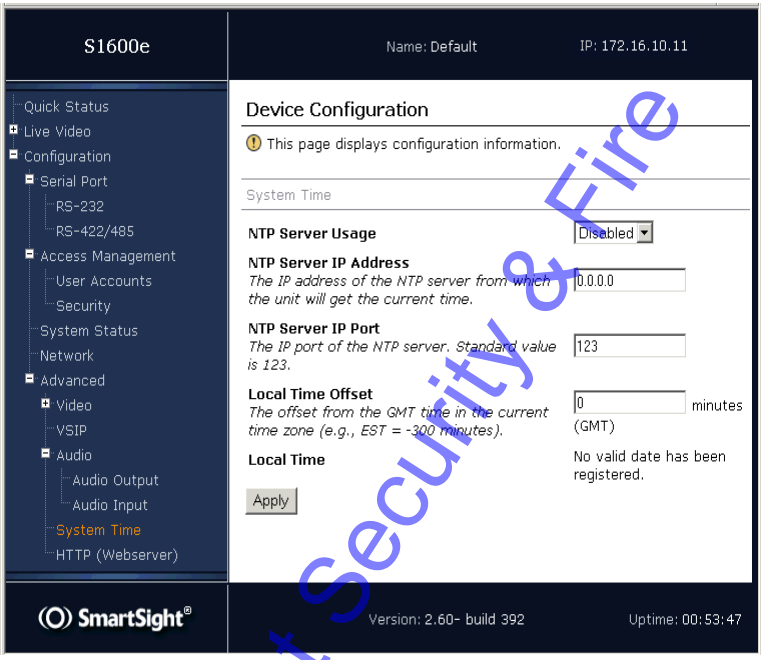
The parameters for audio input are:

Parameter	Description
Input Type	The type of your audio source.

Intelligent Security & Fire

System Time

You can set the following parameters relative to system time:

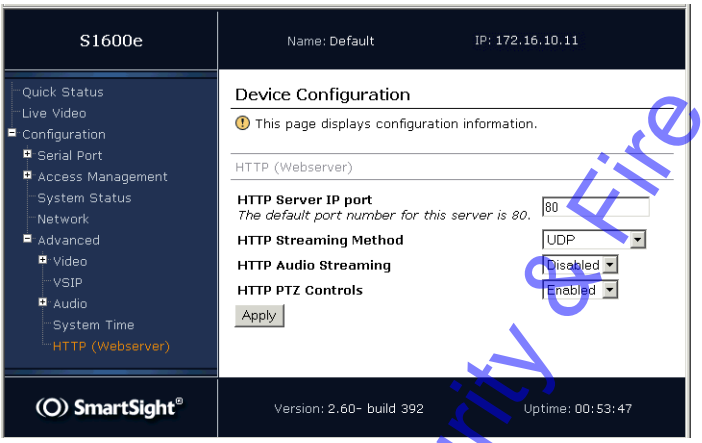


Parameter	Description
NTP Server Usage	To enable or disable the network time protocol (NTP) to get the current time. NTP uses GMT (Greenwich Mean Time) to synchronize device clock time.

Intelligent Security & Fire

HTTP (Webserver)

A series of configuration parameters are relative to the Web interface itself:



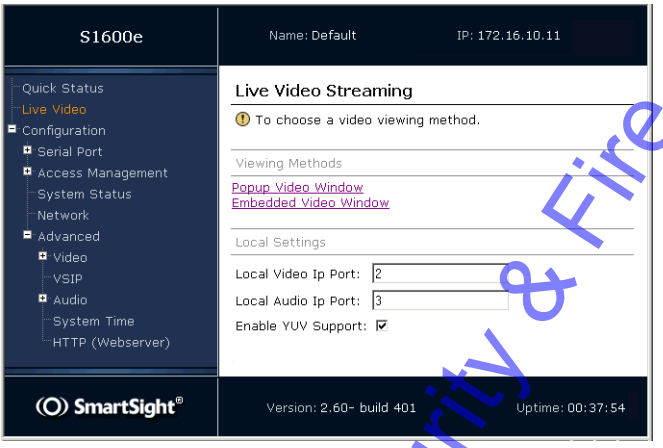
Parameter	Description
Streaming Method	The protocol used for transmitting video.
Audio Streaming	To enable or disable the transmission of audio data.
PTZ Controls	To enable or disable the transmission of PTZ data.

If you enable audio on your computer, you may experience a click every 10 seconds. To stop it, remove the sound in **Control Panel** > **Sounds and Multimedia** > **Sounds** > **Windows Explorer** > **Start Navigation**.

Intelligent Security & Fire

Live Video

You can view the stream coming out of the video source.



When you choose any of the two viewing methods, another Internet Explorer window appears, with the IP address of the unit in its title bar; you can minimize it.

The local settings are:

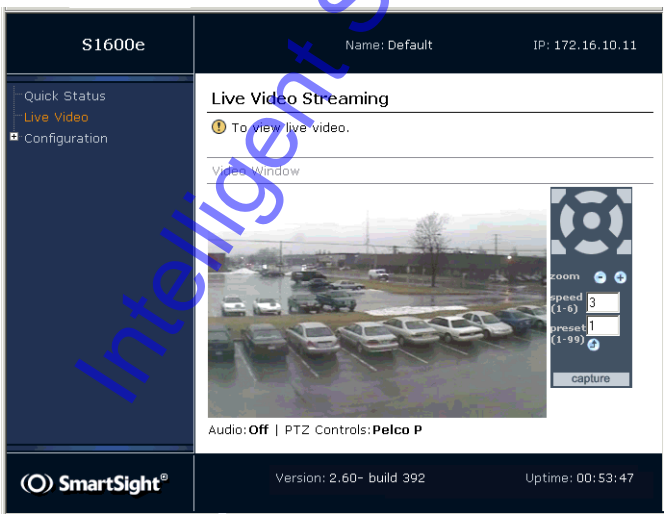
Parameter	Description
Local Video IP Port	The port number on your computer that will receive video.
Local Audio IP Port	The port number on your computer that will receive audio.
Enable YUV Support	The indicator of whether YUV video conversion will be used. Most graphics video cards support YUV.

Intelligent Security & Fire

Presentation Windows

If you choose **Popup Video Window**, the video will be displayed in a separate window:

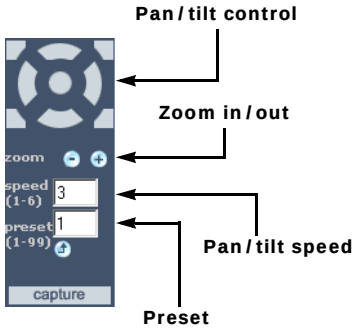
With an embedded window, the video will be displayed directly on the Web page. For example:



Intelligent Security & Fire

PTZ Controls

The PTZ controls allow you to manage the movements of the active camera and to specify zoom values:



The control buttons allow you to pan (left or right) or tilt (up or down) the camera.

The + and - buttons allow you to zoom in or out respectively. You can also determine the camera pan-tilt speed by entering a number between 1 (slower) and 6 (faster).

The Preset advanced function of automated dome is also supported.

Intelligent Security & Fire

A

Factory Default Configuration

This appendix lists the factory default configuration of the S1600e units.

Intelligent Security & Fire

The S1600e is programmed at the factory with the following configuration:

Type	Configuration
Serial port	◆ Bit rate: 4800 bauds ◆ Parity: none ◆ RS-422/485 operating mode: RS-422 4-wire
Access management	◆ Administrator user name: USERNAME ◆ Administrator password: PASSWORD ◆ User accounts: Disabled ◆ Telnet sessions: Enabled ◆ IP firmware update: Enabled ◆ Global security profile: Disabled ◆ SSL passkey: <empty>
Network	◆ DHCP configuration: Disabled ◆ IP address: 169.254.*.* (MAC address of the unit) ◆ Subnet mask: 255.255.0.0 ◆ Gateway: 169.254.*.* (MAC address of the unit) ◆ Primary DNS server address: 0.0.0.0 ◆ Backup DNS server address: 0.0.0.0 ◆ Ping request: Target IP address not specified
Video settings	◆ Target frame rate: 30 fps ◆ Target bit rate: 3200 kbps ◆ Maximum quantizer: 10 ◆ Resolution: All lines (352 x 480) ◆ Video standard: NTSC
VSIP	◆ VSIP Port: 5510 ◆ VSIP Multicast IP Address: 224.16.32.1 ◆ VSIP Discovery IP Address: 255.255.255.255

Intelligent Security & Fire

B

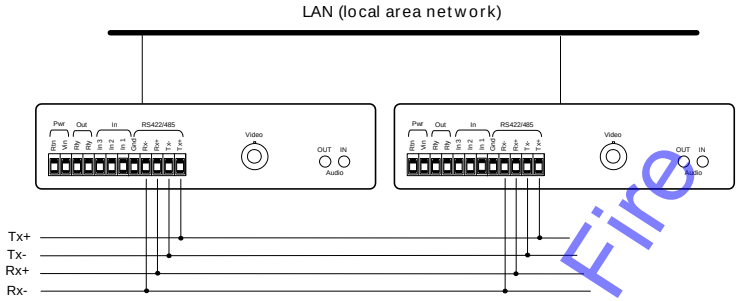
RS-485 Multidrop Connections

Two multidrop configurations are available:

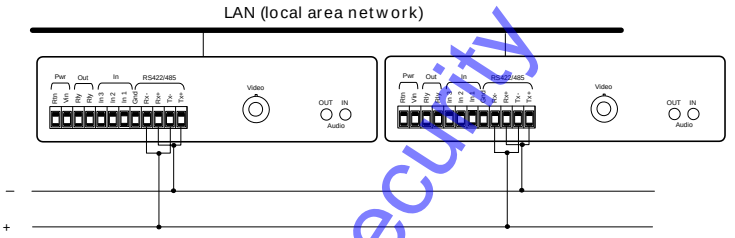
- Four-wire
- Two-wire

Intelligent Security & Fire

The four-wire configuration, which can be used for both RS-422 and RS-485, is:



The two-wire configuration, for RS-485 only, is:



Intelligent Security & Fire

C

DHCP Support and APIPA Service

DHCP (dynamic host configuration protocol) allows devices and computers connected to a network to automatically get a valid IP configuration from a dedicated server.

The APIPA (automatic private IP addressing) service, available on the Windows operating systems, enables a device to assign itself a temporary IP address.

Intelligent Security & Fire

At startup, a unit searches for a valid IP network configuration. The unit requires this configuration prior to starting its functions. The network configuration for SmartSight units consists of:

- An IP address
- A subnet mask
- A gateway
- One or two IP addresses of DNS servers (optional)

The unit first looks in its local memory. If no configuration is found, it tries to contact a DHCP server. If DHCP configuration fails—if the unit does not find a server or if it cannot get a configuration from it within one minute—the unit assigns itself temporary network settings based on the APIPA service. This service allows a unit to find a unique IP address until it receives a complete network configuration, either from a DHCP server or manually through SConfigurator or the CLI.

A unit in APIPA mode does not reside on the same subnet as the other devices on the IP network; therefore, it may not be able to see them or be visible to them. Units use the following temporary APIPA configuration:

- IP address: 169.254. * . *
- Subnet mask: 255.255.0.0
- Gateway: 169.254. * . *

The *. * portion is based on the MAC address of the unit.

A unit is in APIPA mode:

- The first time it boots up
- After receiving a duplicate IP address
- After a factory reset
- When the DHCP server does not have any available IP addresses

DHCP configuration is disabled:

- After a firmware upgrade
- After a factory reset

Intelligent Security & Fire

D

DTE and DCE Connections

Before connecting a SmartSight unit to other serial equipment, you need to determine if they are DTE (data terminal equipment) or DCE (data communication equipment).

Here are examples of both equipment types:

- DCE—SmartSight units, modems
- DTE—Computers, switches, multiplexers, cameras, keyboards

Intelligent Security & Fire

You need to know which equipment type your other serial device is in order to connect it correctly to the S1600e unit, which is a DCE.

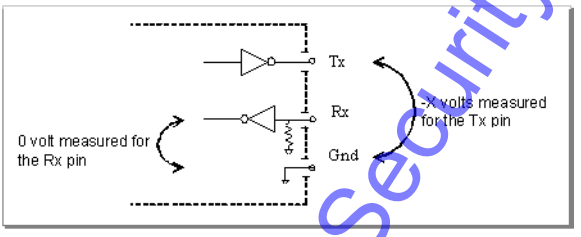
In the following descriptions:

- Voltage is measured when no data is transferred on the Rx and Tx pins.
- *-X volts* represents a negative voltage value.

Data Terminal Equipment

DTE modules have the following electrical-level setup:

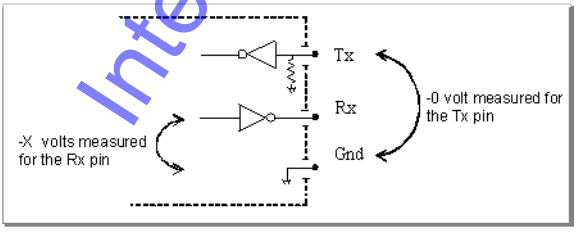
Pin number	Signal	Measured voltage
3	Tx	-X volts
2	Rx	0 volt



Data Communication Equipment

DCE modules have the following electrical-level setup:

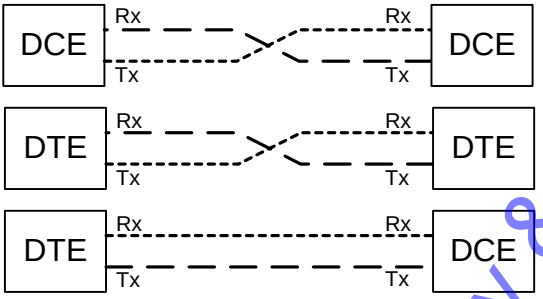
Pin number	Signal	Measured voltage
3	Tx	0 volt
2	Rx	-X volts



Intelligent Security & Fire

Connecting DTE and DCE

When connecting two modules of the same type, you have to cross the data wires to create proper communication. On the other hand, when connecting a DTE with a DCE, a straight cable is required.



Intelligent Security & Fire

E

CLI with SConfigurator

The SConfigurator console enables you to easily access the CLI (command line interface) tool to configure and customize your S1600e unit.

Intelligent Security & Fire

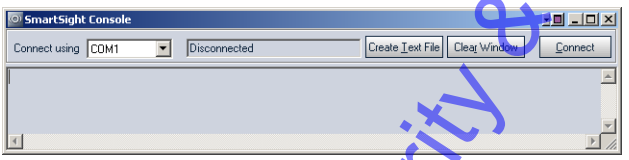
You find the SConfigurator program and its user manual on the *SmartSight Utilities* CD shipped with your unit. You can either launch SConfigurator directly from the CD or copy the executable file first on your hard disk.

To access the CLI with the SConfigurator console:

1. Connect the S1600e unit to a COM port of the computer using a serial cable.
2. Start SConfigurator.

   The **SConfigurator** window appears.
3. From the **General** tab, click **Console**.

   The **SmartSight Console** window appears.



4. In the **Connect using** list, select the COM port used to communicate with the unit.
5. Click **Connect**.

   The CLI main menu appears.

   The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

   - You loose access to the command line.
   - The “Thank you for using the SmartSight CLI” message appears at the command line.
   - The **SmartSight Console** window becomes disabled.
   - The **Disconnect** button switches to **Connect**.
6. To reactivate the CLI after a timeout, click **Connect**.
7. To end the CLI work session:

   - Save the settings by entering **s** at the main menu, then pressing **Enter**.
   - Exit the CLI by entering **q** at the main menu, then pressing **Enter**.

Intelligent Security & Fire

❖ Close the **SmartSight Console** window.

Warning

The **Disconnect** button is used to terminate the connection to the SConfigurator console, not to exit from the CLI. Clicking it does not free the RS-232 connection and does not save your settings.

Intelligent Security & Fire

F

CLI with HyperTerminal

HyperTerminal is the Windows system tool for connecting to other computers, Internet Telnet sites, bulletin board systems (BBSs), online services, and host computers. You can use it to access the CLI (command line interface) of your unit.

Intelligent Security & Fire

You have to perform the following operations before being able to use HyperTerminal to access the CLI:

1. Connecting the S1600e unit to a COM port of the computer using a CAB9P serial cable with a DB-9 end
2. Powering the S1600e unit
3. Establishing a connection
4. Setting the parameters of the computer's serial port
5. Activating the connection

Notes

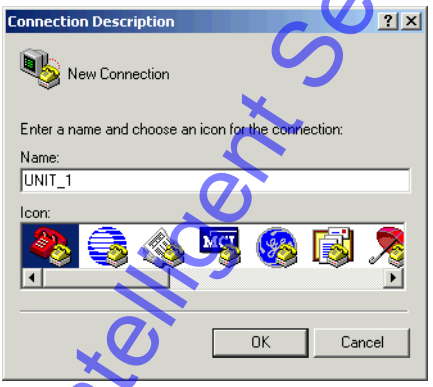
A COM port is required to perform unit configuration. You need to disable any program using this port prior to starting this procedure.

Turn off the **Scroll Lock** key on your keyboard before entering HyperTerminal.

To establish a connection:

1. From the **Start** menu, choose **Programs** > **Accessories** > **Communications** > **HyperTerminal**.

   The **Connection Description** window appears.



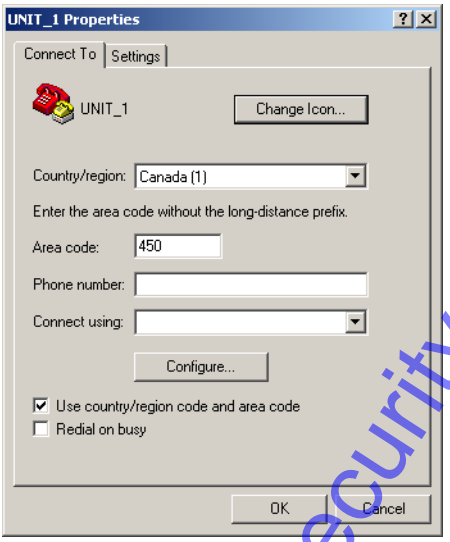
2. In the **Name** field, enter a description for the connection; for example, UNIT_1.
3. Click **OK**.
4. In the **Connect To** window, click **Cancel**.

Intelligent Security & Fire

To set the parameters of the serial port:

1 From the main HyperTerminal window, choose **File** > **Properties**.

The ***connection_name*** **Properties** window appears.

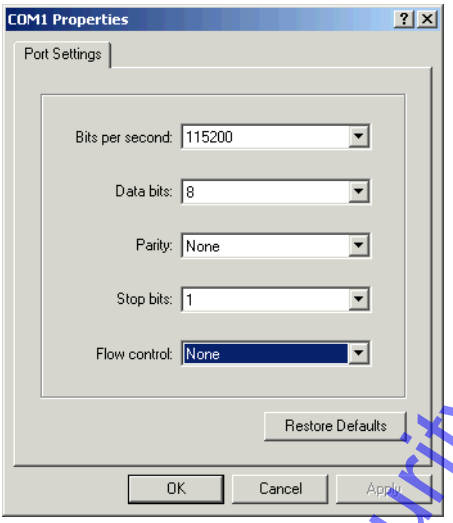


2 In the **Connect using** field, select the COM port you are using for the connection.

Intelligent Security & Fire

3 Click **Configure**.

A **Properties** window appears.



4 Set the parameters with the values indicated in the illustration.

5 Click **OK**.

6 In the ***connection_name*** **Properties** window, click **OK**.

To activate the connection:

◆ From the main HyperTerminal window, choose **Call** > **Call**.

You can now use the CLI to configure your S1600e unit.

To access the CLI with HyperTerminal:

1 Press **Ctrl**+**Break**, then the space bar for a few seconds.

The CLI main menu appears.

The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

- ❖ You loose access to the command line.
- ❖ The “Thank you for using the SmartSight CLI.” message appears at the command line.
- ❖ The **HyperTerminal** window becomes disabled.

2 To reactivate the CLI after a timeout, press **Ctrl**+**Break**, then the space bar for a few seconds.

Intelligent Security & Fire

3 To end the CLI work session:

- Save the settings by entering **s** at the main menu, then pressing **Enter**.
- Exit the CLI by entering **q** at the main menu, then pressing **Enter**.
- Close the **HyperTerminal** window.

Intelligent Security & Fire

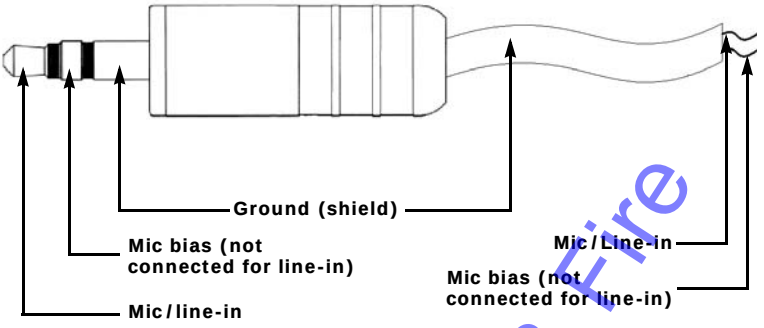
G

Audio Pinouts

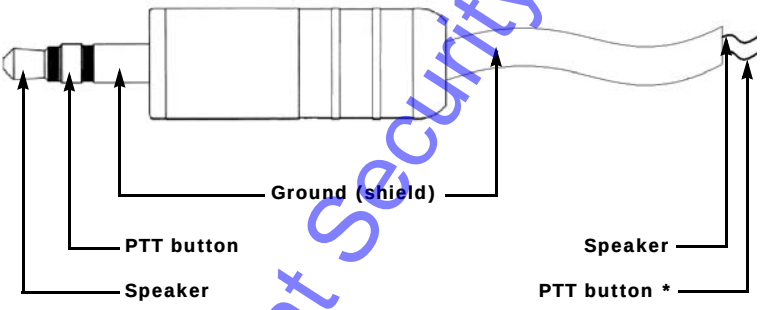
This appendix presents information relative to the 3.5 mm stereo plugs used for audio on the units.

Intelligent Security & Fire

Here is the pinout of the stereo jacks for audio input:



For audio output, the jacks are configured the following way:



* PTT is a normally open switch —⊥— .

Intelligent Security & Fire

H

Technical Specifications

Intelligent Security & Fire

Here are the S1600e technical specifications:

Video	Compression	MPEG-4-based
	Frame rate	Up to 30 fps (60 fields) programmable (full motion)
	Input	1 composite, 1 Vpp into 75 ohms
	Output	1 composite, 1 Vpp into 75 ohms
	Resolution	Scalable from 176 x 128 to 704 x 480 NTSC pixels (176 x 144 to 704 x 576 PAL pixels)
	Standard	NTSC or PAL
	Connectors	BNC female
	Bandwidth	Configurable between 30 kbps and 4 Mbps
Serial Port	Electrical levels	Port 1: RS-232 (230 kbps max.) Port 2: RS-422/485 2/4 wires (230 kbps max.)
	Connectors	Port 1: DB-9 female Port 2: pluggable screw-terminal strip
	Operating mode	Transparent serial port supporting any asynchronous serial protocol (Specific protocol emulation may be supported on request)
Alarm and audio	Alarm input	3 dry contacts
	Alarm output	1 relay contact (48V AC/DC at 100 mA max.)
	Bidirectional audio	Input: -46 to -3 dBV into 1 kOhm Output: -46 to -3 dBV into 16 ohms min.
	Audio connectors	One set of 0.14 inch (3.5 mm) input and output stereo jacks
Network	Interface	Ethernet 10/100Base-T
	Connector	RJ-45 jack
	Protocols	Transport: RTP/IP, UDP/IP, TCP/IP, multicast IP Others: DNS and DHCP client
	Security	SSL-based authentication
Power	Supply voltage	12V DC ±10%
	Consumption	6W max. (500 mA max. at 12V DC)
Physical	Enclosure	Metal case with flange mount (black color)
	Size	4.52L x 5.6W x 1.25H inches (115L x 142W x 32H millimeters)
	Weight	0.84 lbs (0.38 kg)

Intelligent Security & Fire

	Environment	S1600e: 32°F to 122°F (0°C to 50°C) S1600e-XT: -22°F to 140°F (-30°C to 60°C)
	Humidity	95% non condensing at 122°F (50°C)
Certification and Regulation	USA	FCC part 15 (subpart B, class A)
	Canada	ICES-003/NMB-003
	Europe	CE mark, EN 55022:1998 Class A, EN 55024:1998
Management	Configuration	Local via the serial port using any ASCII terminal Remote using SConfigurator, Internet Explorer 5.5, or Telnet

Intelligent Security & Fire

Glossary

This glossary is common to all SmartSight products.

Intelligent Security & Fire

Access Point A device acting as a communication switch for connecting wireless units to a wired LAN. Access points are mainly used with wireless transmitter units to transfer wireless content onto the wired IP network.

APIPA (Automatic Private IP Addressing) A feature of Windows-based operating systems that enables a device to automatically assign itself an IP address when there is no dynamic host configuration protocol (DHCP) server available to perform that function. APIPA serves as a DHCP server failover mechanism and makes it easier to configure and support small local area networks (LANs). Also known as *AutoIP*.

Bridge A unit linking a wireless network to a wired Ethernet network. The newest SmartSight bridge is the S3100.

CCTV (Closed Circuit Television) A television system in which signals are not publicly distributed; cameras are connected to television monitors in a limited area such as a store, an office building, or on a college campus. CCTV is commonly used in surveillance systems.

CIF (Common Image Format) A video format that easily supports both NTSC and PAL signals. Many CIF flavors are available, namely CIF, QCIF, 2CIF, and 4CIF. Each flavor corresponds to a specific number of lines and columns per video frame.

CLI (Command Line Interface) A textual user interface in which the user responds to a prompt by typing a command. All SmartSight units have a built-in CLI allowing their configuration.

Codec (Coder/Decoder) A device that encodes or decodes a signal.

DCE (Data Communication Equipment) In an RS-232 communication channel, a device that connects to the RS-232 interface. SmartSight units and modems are DCE.

Decoder See *Receiver*.

DHCP (Dynamic Host Configuration Protocol) A communication protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in a network.

DTE (Data Terminal Equipment) In an RS-232 communication channel, the device to which the RS-232 interface connects. Computers, switches, multiplexers, cameras, and keyboards are DTE.

Intelligent Security & Fire

DVR (Digital Video Recorder) A device (usually a computer) that acts like a VCR in that it has the ability to record and play back video images. The DVR takes the feed from a camera and records it into a digital format on a storage device which is most commonly the hard drive.

Encoder See *Transmitter*.

Ethernet A local-area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10 Mbps. It is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100Base-T (or fast Ethernet), supports data transfer rates of 100 Mbps. The 802.11a and 802.11b protocols are often referred to as "wireless Ethernet."

Firmware Software stored in read-only memory (ROM) or programmable ROM (PROM), therefore becoming a permanent part of a computing device.

IP (Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

LAN (Local Area Network) A computer network that spans a relatively small area. A LAN can connect workstations, personal computers, and surveillance equipment (like video servers). See also *WAN*.

Master An S3100 unit controlling S1100w transmitter stations and slave S3100 units.

MPEG-4 A graphics and video lossy compression algorithm standard that is derived from MPEG-1, MPEG-2, and H.263. MPEG-4 extends these earlier algorithms with synthesis of speech and video, fractal compression, computer visualization, and artificial intelligence-based image processing techniques.

Multicast Communication between a single sender and multiple receivers on a network; the devices can be located accross multiple subnets, but not through the Internet. Multicast is a set of protocols using UDP/IP for transport.

nDVR The SmartSight video management and storage software. This graphical product is used in conjunction with Ethernet and wireless video servers.

Intelligent Security & Fire

NTSC (National Television Standards Committee) The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of television signals. In addition to North America, the NTSC standard is used in Central America, a number of South American countries, and some Asian countries, including Japan. Compare with *PAL*.

NTP (Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network.

OSD (On-Screen Display) Status information displayed on the video monitor connected to a receiver unit.

Outdoor Wireless Bridge See *Bridge*.

PAL (Phase Alternation by Line) A television signal standard (625 lines, 50 Hz, 220V primary power) used in the United Kingdom, much of western Europe, several South American countries, some Middle East and Asian countries, several African countries, Australia, New Zealand, and other Pacific island countries. Compare with *NTSC*.

PTL (Push-to-Listen) In a two-way system, the communication mode in which the listener must push a button while listening.

PTT (Push-to-Talk) In a two-way system, the communication mode in which the talker must push a button while talking.

PTZ Camera (Pan-Tilt-Zoom) An electronic camera that can be rotated left, right, up, or down as well as zoomed in to get a magnified view of an object or area. A PTZ camera monitors a larger area than a fixed camera.

Receiver A device converting a digital video signal into an analog form. Also called *decoder*.

Repeater A range extender for wireless links. The SmartSight repeater is made up of two S3100 bridges (a master and a slave).

RF (Radio Frequency) Any frequency within the electromagnetic spectrum associated with radio wave propagation. When a modulated signal is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. Many wireless technologies are based on RF field propagation.

RS-232 A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices.

Intelligent Security & Fire

RS-422 A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices, designed to replace the older RS-232 standard because it supports higher data rates and greater immunity to electrical interference.

RS-485 An Electronics Industry Alliance (EIA) standard for multipoint communications.

S1000 Series The SmartSight series of secure outdoor wireless video systems. The series includes the S1000 unit (for the 2.4 GHz frequency band in North America), the S1000-CE unit (for the 2.4 GHz frequency band in Europe), and the S1005 unit (for the 5 GHz band in North America).

S1000w The SmartSight outdoor wireless video transmitter operating on the 2.4 GHz frequency band.

S1100w The SmartSight outdoor wireless video transmitter operating on the 5 GHz frequency band.

S1500e Series The SmartSight series of Ethernet video servers (receiver and transmitter) designed for video monitoring and surveillance over IP networks.

S1600e The SmartSight high-resolution Ethernet video server (receiver and transmitter) providing point-to-point analog extension with Web access.

S3100 The outdoor, wireless, digital SmartSight video bridging unit. The S3100 bridge is used to wirelessly link S1100w wireless video servers, or S1500e series/S1600e video servers in remote locations, to an Ethernet LAN.

SConfigurator (SmartSight Configurator) A proprietary graphical program used to configure and update the firmware of video server and outdoor wireless bridge units.

Serial Port An interface that can be used for serial communication, in which only one bit is transmitted at a time. A serial port is a general-purpose interface that can be used for almost any type of device.

Slave An S3100 unit controlled by a master unit, typically in a repeater application.

SMI (SmartSight Management Interface) A proprietary graphical program used to access the command line interface of the S1000 series units and to perform firmware updates.

SSID (Service Set Identifier) A name identifying a pair of SmartSight units (transmitter and receiver) working together.

Intelligent Security & Fire

SSL (Secure Sockets Layer) A commonly used protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port, and VSIP communication; it does not apply to audio and video transmission.

Station An S1100w unit connected to a master S3100 bridge.

Transceiver (Transmitter/Receiver) A device that both transmits and receives analog or digital signals.

Transmitter A device sending video signals captured with a connected camera or dome to a receiver. The transmitter converts the analog signal into a digital form before transmitting it. Also called *encoder*.

Video Server A unit transmitting or receiving video signals. The SmartSight wireless servers are the S1000w and S1100w units; the Ethernet servers are the S1500e series and S1600e units.

VSIP (Video Services over IP) A proprietary communication protocol for sending messages between a computer and a SmartSight unit, or between two units.

WAN (Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

WEP (Wired Equivalent Privacy) A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. It is designed to afford wireless networks the same level of protection as a comparable wired network.

Wireless Cell A group of wireless devices that communicate together on the same radio frequency channel. Also called *wireless LAN*.

Wireless Transmission A technology in which electronic devices send information to receivers using radio waves rather than wiring.

Intelligent Security & Fire

Index

Numerics

3.5 mm plug *17*

A

abnormal power-up condition *21*
access
  HTTP *29*, *45*
  Web interface *2*, *29*, *45*
access management
  menu in the CLI *27*
  settings in the Web interface *44*
account, user *27*, *44*
address, IP. *See* IP address.
administrator account *27*, *44*
Advanced menu *32*
alarm configuration *16*
APIPA service *8*, *63*
audio
  connectors *80*
  input/output *17–19*
  PTL *17*
  PTT *17*
  settings in the Web interface *51*
  specifications *19*

B

bidirectional audio *17*
bit rate, serial port *26*
boot, soft *33*

C

camera control *57*
camera data port configuration *2*
casing of the unit *4*
CD, Utilities *x*
certificate, SSL *2*, *30*
characteristics of the unit *2*
checking for the SSL feature *30*
CIF resolution *3*
CLI (command line interface)
  access with HyperTerminal *73–77*
  access with SConfigurator *69–71*
  access with Telnet *24–25*
  main menu *25*
  menus *26–33*
  timeout *25*
COM port *70*, *74*
command line interface. *See* CLI (command line interface).
computer requirements *8*

Intelligent Security & Fire

configuration
  alarm *16*
  audio *17–19*
  camera data port *2*
  default *19*, *33*, *59*
  I/O *17–19*
  unit *8–11*
  Web interface *41–54*
connection
  DCE/DTE *65*
  HyperTerminal and unit *74*
  multidrop *61*
  point-to-point *11*
  RS-232 *14*
  RS-422/485 *14*, *61*
  SConfigurator and unit *70*
connector
  audio *17*
  DB-9 *14*
  for serial port *14*
console, SConfigurator *69*

D

DB-9 connector pinout *14*
DCE (data communication equipment) *65*
default configuration *19*, *33*, *59*
DHCP (dynamic host configuration protocol) *10*, *63*
differences between the units *2*
display on receiver units. *See* OSD (on-screen display).
distance between units *6*
DTE (data terminal equipment) *65*
duplex audio *17*
duplicate IP address *8*, *37*

E

EIA-232. *See* RS-232.
EIA-422. *See* RS-422/485.
enclosure, unit *4*
equipment list *3*
event, alarm *16*

F

factory default configuration *19*, *33*, *59*
features of the unit *2*
firmware update, preventing *2*, *29*, *45*
firmware version *11*, *30*
frame rate *3*
full duplex audio *17*

G

gateway *32*
global security profile *29*, *45*
GMT (Greenwich mean time) *53*

H

hardware reset *19*, *59*
HTTP access *29*, *45*
HTTP settings *54*
HyperTerminal *73*

I

I/O, alarm or audio *16–19*
identifying a unit *33*
independent serial port *2*
input, alarm or audio *16–19*
installation *13*
IP address
  APIPA *63*
  duplicate *8*, *37*
  setting *8*, *31*
  temporary *63*
IP firmware update, preventing *2*, *29*, *45*
IP link *2*, *6*

L

LED, status *20*
list of equipment *3*
live video *55–57*
loading default configuration *33*, *59*
login name. *See* user name.

M

main menu of the CLI *25*
mask, subnet *31*
menus in the CLI *26–33*
microphone, multimedia *18*
mono plug. *See* 3.5 mm plug.
multicast streaming method *6*
multidrop connection *61*
multimedia microphone *18*

Intelligent Security & Fire

N

network
- menu in the CLI *31*
- planning *5–6*
- settings in the Web interface *47*

NTP (network time protocol) *53*

O

operating mode, RS-422/485 *27*
options, when ordering a unit *3*
OSD (on-screen display) *35–37*
output, alarm or audio *16–19*

P

panel of unit *4*
pan-tilt-zoom (PTZ) *39*, *57*
parity *27*
passkey, SSL *30*, *45*
password
- for serial connection *27*, *44*
- SSL *30*, *45*
- for Telnet connection *27*, *44*
- for Web interface *27*, *44*

Pelco protocol pinout *15*
ping request *32*
pinout
- Pelco protocol *15*
- serial port *14*

plug. *See* connector.
point-to-point connection *11*
port
- COM. *See* COM port.
- serial. *See* serial port.

power requirement *2*
power-up condition, abnormal *21*
preventing
- firmware update *2*, *29*, *45*
- Telnet access *2*, *29*, *45*
- Web interface access *29*, *45*

protecting unit configuration *27*
protocol, VSIP *50*
PTL (push-to-listen) *17*, *80*
PTT (push-to-talk) *17*, *80*
PTT/PTL mode *17*, *80*
PTZ (pan-tilt-zoom) *39*, *57*

Q

quadrant, OSD *35–37*

R

reboot, soft *33*
receiver display. *See* OSD (on-screen display).
recognizing a unit *33*
requirements
- computer *8*
- power *2*

Reset button *19*
reset to factory default *19*, *33*, *59*
resolution, video *3*, *48*
RS-232
- menu in the CLI *26*
- pinout *14*
- settings in the Web interface *42*

RS-422/485
- menu in the CLI *26*
- multidrop connection *61*
- pinout *14*
- settings in the Web interface *43*

S

SConfigurator console *69*
secure HTTP access *29*, *45*
security profile *29*, *45*
security settings *28*, *45*
serial number of the unit *30*
serial port
- menu in the CLI *26*
- pinout *14*
- settings displayed on the OSD *37*
- settings in the Web interface *42*

shipment list *3*
SmartSight Utilities CD *x*
SmartSight Web site *x*
soft reboot *33*
software reset *33*
specifications
- audio *19*
- technical *81–83*

Intelligent Security & Fire

SSL (secure sockets layer)
certificate *2*, *30*
checking for the feature *30*
creating a secure connection *29*, *45*
defined *2*
passkey *30*, *45*
status LED *20*
status of the unit *30*, *46*
stereo plug. *See* 3.5 mm plug.
streaming method, multicast *6*
subnet mask *31*
support, technical *xi*
system configuration *8–11*
system reboot *33*
system status *30*, *46*
system time *53*

T

technical specifications *81–83*
technical support *xi*
Telnet
accessing the CLI *24*
preventing access *2*, *29*, *45*
temporary IP address *63*
terminal emulation tool *73*
tilt control *57*
time, system *53*
timeout, CLI *25*

U

updating firmware, preventing *2*, *29*, *45*
user account *27*, *44*
user name *27*, *44*
Utilities CD *x*

V

version of firmware *11*, *30*
video settings *3*, *48*
video, live *55–57*
VSIP protocol *50*

W

Web client account *28*
Web interface
accessing with a password *27*, *44*
configuring *41–54*
HTTP settings *54*
opening *40*
preventing access *29*, *45*
secure access *2*
Web server settings *54*
Web site, SmartSight *x*

Z

zoom control *57*

Intelligent Security & Fire

Compliance

Intelligent Security & Fire

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

EN 55022 Statement

This is to certify that the SmartSight Model S1600e Ethernet video servers are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/ECC, Article 4a. Conformity is declared by the application of EN55022 Class A (CISPR 22).

Warning

It is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take appropriate measures.

Intelligent Security & Fire

Declaration of Conformity

Manufacturer:

SmartSight Networks Inc.
1800 Berlier
Laval, Québec
H7L 4S4
Canada

Declares under sole responsibility that the product:

Product name: Ethernet video server

Model number: S1600e

To which this declaration relates is in conformity with the following standards or other documents:

EMC Directive 89/336/EEC:

EN55022:1998 class A

EN55024:1998

EN 61000-4-3:1996 3V/m

EN 61000-4-6:1996 3Vrms

EN 61000-4-2:1995 4kV CD, 8 kV AD

EN 61000-4-4:1995 1kV (power), 500V (signal)

EN 61000-4-11:1994

ENV50204:1995

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

May 6th, 2003
Laval, Canada

Willie Kouncar
Vice President, Engineering
SmartSight Networks Inc.

Intelligent Security & Fire

Intelligent Security & Fire

SmartSight Networks Inc.
1800, Berlier Street
Laval (Quebec)
H7L 4S4
Canada

www.smartsightnetworks.com