S3100
User Manual

SmartSight®

Expanding vision **beyond** wired networks

S3100™
Firmware Release 2.60

User Manual

For countries operating under
FCC part 15 rules and regulations

SmartSight™

S3100™ User Manual
Firmware Release 2.60

Published by:

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

Publication date: December 19, 2003

Table of Contents

Preface

The *S3100™ User Manual* presents the information and procedures on installing and configuring the SmartSight S3100 outdoor wireless bridge.

Who Should Read this Manual

This manual is intended for engineers and technicians who will install the S3100 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
- Wireless technology
- Basic IP data communication concepts and practices
- Radio frequency (RF) regulations

How to Use this Manual

This manual contains all the information needed to install and configure an S3100 unit.

Contents

The *S3100 User Manual* is divided into the following chapters:

1. **Overview**—Provides a brief description of the features of the S3100 and illustrations of its casing.
2. **Network and RF Planning**—Lists the available frequency channels and describes planning operations relative to radio frequency (RF) and system setup.
3. **Configuration and Installation**—Describes how to configure and install the S3100 unit and its antenna.
4. **Setting Parameters with the CLI**—Explains how to program the S3100 unit using the SmartSight command line interface.

The manual also includes the following appendixes:

A **Factory Default Configuration**—Lists the default parameter values of the S3100 unit.

B **RJ-45 Ethernet Cables**—Presents the pinouts of the straight-through and crossover Ethernet cables.

C **Pole Mounting of the Antennas**—Shows how to install on a pole the antennas supplied by SmartSight.

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

E **Surge Protection**—Describes how to protect the S3100 unit from voltage and current surges.

F **Technical Specifications**—Lists the complete technical specifications of the S3100 units.

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

Conventions

The following typographic conventions are used throughout this manual:

Visual cue	Meaning
Program Options	The name of a window, dialog box, field, or any other interface element. The value of an interface element.
Support > **Downloads**	Any sequence of steps (in the menu structure of a graphical application, in the navigation structure of a Web site, and so on).
`telnet`	The name of a command, file, or directory. Text that appears on the screen. Examples of user-supplied values.

Related Documentation

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

- *S3100 Quick Installation Guide*—Contains the S3100 configuration steps and the installation procedure.
- *SConfigurator User Manual*—Presents the instructions on how to use a proprietary SmartSight software to configure the S3100 unit and update its firmware.
- *Release Notes*—Contain information about S3100 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 S3100 unit. Furthermore, a paper copy of the *Quick Installation Guide* is included with your order.

Related SmartSight Products

You can use the S3100 units with the S1100w™ wireless video transmitters and with the S1500e™ series and S1600e™ video servers.

You may also use the S3100 units along with the nDVR™ software. This user-friendly video management and storage software is able to view, record, and play back video simultaneously from any location.

The S3100 and nDVR are part of the Versalis™ line of products. Versalis is the only networked digital video solution that combines distributed viewing, storage, and capture of high quality, high resolution live video, voice, and data.

For more details about any of these products, visit our Web site. For pricing information, call your dealer.

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**).

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 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.

The warranty becomes void if the product is altered in any way.

1

Overview

The S3100 is SmartSight's latest addition to its family of outdoor, wireless, digital video bridging products.

Note
The S3100 units require professional installation.

About the S3100

The S3100 license-free video bridge is used to wirelessly link SmartSight's S1100w video transmitters, or S1500e series and S1600e video servers in remote locations, to an Ethernet LAN. Several of these bridges can be used to create multiple video links covering a large geographical area (for example, citywide monitoring).

There are currently two S3100 models:

- A unit for connecting S1100w transmitters to an Ethernet LAN or for creating a wireless bridge (*S3100* product code)
- A repeater device made up of two S3100 units, a master and a slave (*S3100-RP* product code)

Every S3100 unit comes with the following security features:

- SSL—Every unit is shipped 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 VSIP communication data. It does not apply to audio and video transmission.

  Once a unit is in secure mode, you cannot access it anymore with Telnet 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*.

- SPCF/SDCF—These proprietary MAC (media access control) protocols use AES encryption (with key rotation) over the wireless link to secure communication between the units. They secure VSIP communication, audio, and video. For more information, see page 12.

Shipment

Your shipment contains the following items:

- The requested outdoor wireless bridge:
  - *S3100* for point-to-multipoint or wireless bridge applications
  - *S3100-RP* for repeater setups
- For an *S3100* unit:
  - A power-over-Ethernet kit (injector and power cord)
  - An 82-foot (25-meter) outdoor Ethernet cable (may be replaced by the optional *ECAB-50* cable)
- For an *S3100-RP* unit:
  - A 3-foot (1-meter) outdoor crossover Ethernet cable
  - Two 30-foot (10-meter) 24V AC outdoor power cords
- A wall mount bracket set, already installed on the unit
- A pole mount bracket set, including stainless steel clamps
- The *SmartSight Utilities* CD containing the documentation and release notes for the unit as well as the SConfigurator application
- The *S3100 Quick Installation Guide*

The shipment may also contain the following options:

- Antennas:

Warning

When choosing antennas, you must ensure that the combined transmission power of the unit and the antenna does not exceed the maximum value established by your country's regulations. For the regulation values in North America and the procedure to lower the unit power, see page 22.

  - A 13-dBi, 5.25–5.85 GHz, 58° beamwidth, patch antenna with a pole mount bracket and a 3-foot (1-meter) SMA-N cable (*ANT-WP13-5x/S*)
  - A 16-dBi, 5.25–5.85 GHz, 90° beamwidth, sector panel antenna with a pole mount bracket and a 3-foot (1-meter) SMA-N cable (*ANT-WP16-5x/S*)

- ❖ An 18-dBi, 5.25–5.85 GHz, 18° beamwidth, patch antenna with a pole mount bracket and a 3-foot (1-meter) SMA-N cable (*ANT-WP18-5x/S*)
- ❖ A 24-dBi, 5.25–5.85 GHz, 9° beamwidth, patch antenna with a pole mount bracket and a 3-foot (1-meter) SMA-N cable (*ANT-WP24-5x/S*)

◆ For an *S3100* unit:

- ❖ A 164-foot (50-meter) outdoor Ethernet cable (*ECAB-50*)

◆ For an *S3100-RP* unit:

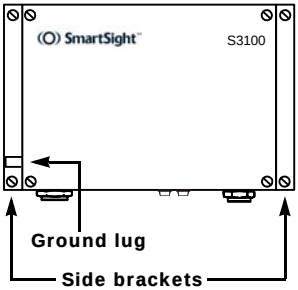
- ❖ One or two 24V AC external power supplies (*PS2440*)

Note

If you are using power supplies other than those supplied by SmartSight, you need to ensure that they have a minimum capacity of 30 VA.

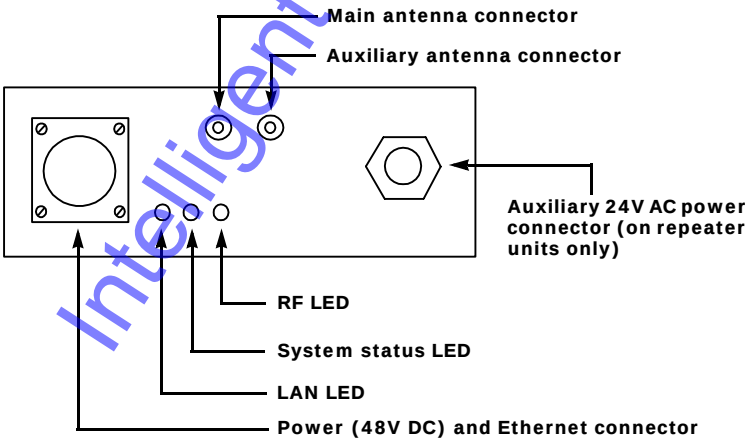
Unit Casing Description

The S3100 electronics are enclosed in a weather-tight cast aluminum module. All cable entries are mounted on the underside of the unit to maintain its weatherproof properties. Here is the S3100 casing:



The unit underside integrates:

- A power and Ethernet connector
- Three LEDs
- Two female antenna connectors (the auxiliary connector is for future development)
- An optional 2-pin auxiliary power connector (on the repeater units only)



2

Network and RF Planning

To allow optimal configuration, you must properly plan your network, especially configuration layout and RF (radio frequency).

Available Channels

The S3100 supports communications in the 2.4 GHz ISM and 5 GHz U-NII frequency bands available in North America. To know which bands are available elsewhere, refer to each country's specific legislation.

Note
The 2.4 GHz band will be supported in a future firmware release.

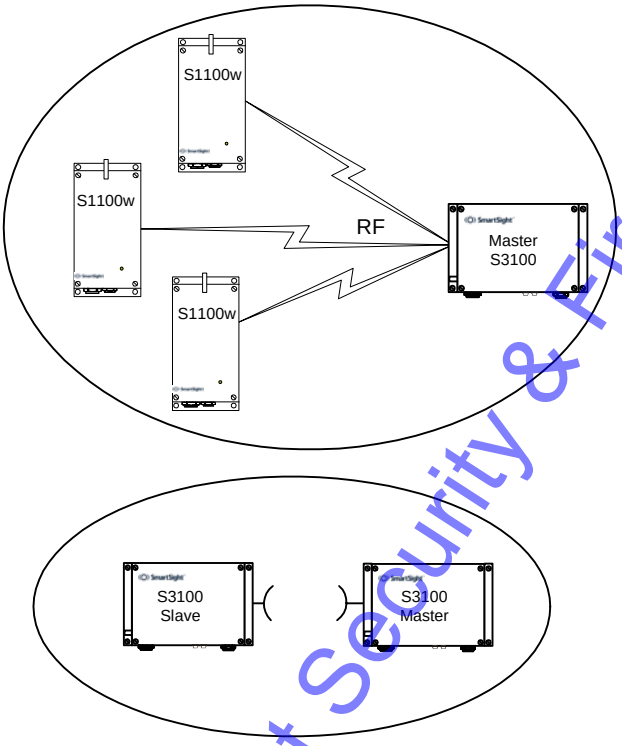
In the 5 GHz band, eight channels are available, all non-overlapping and for indoor or outdoor use. The center frequencies of these channels are:

Channel	Frequency (GHz)
52	5.26
56	5.28
60	5.30
64	5.32
149	5.745
153	5.765
157	5.785
161	5.805

Wireless Cells

A wireless network is designed such that information can travel back and forth between two points without the need for wires. Wireless devices are grouped into wireless cells (or *wireless LANs*). The devices in a cell communicate together on the same frequency channel and that share the same wireless passkey (described on page 32).

Here are examples of wireless cells:



You can collocate many wireless cells if you respect certain conditions (see page 16).

System Planning

The grouping of units in each wireless cell is determined by their respective locations with respect to one another and by the available outdoor wireless bridges. As a rule of thumb, there should be clear RF line of sight between each S1100w or slave S3100 unit and their master bridge within each cell. However, the S1100w and slave S3100 units can be completely hidden from one another. For more information about RF line of sight, see page 20.

Furthermore, when installing many wireless cells in the same area, you have to carefully plan their positions in order to prevent radio interference and select the appropriate antennas.

In a wireless cell, the order in which you configure the units (either the first time or later when they are installed in the field) is critical if you do not want to loose access to them. You should then:

1. Configure the units starting with the farthest (in terms of number of RF hops) from the computer.
2. One step at a time, get closer to the computer.

The S3100 units are used in many types of applications, namely:

- Point-to-multipoint—One S3100 bridge and multiple S1100w units
- Repeater—Two S3100 units acting as a range extender
- Wireless bridge—Two S3100 units linking two networks (wired or wireless)

Compatibility Issues

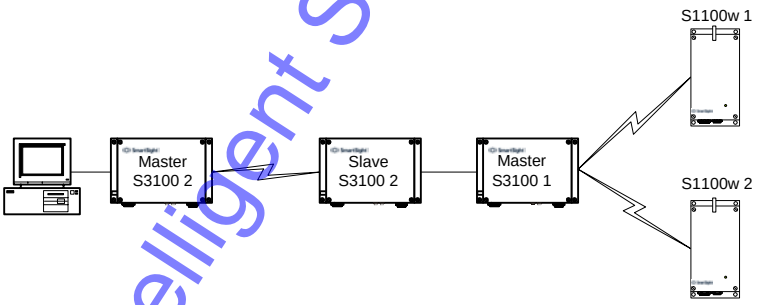
When planning your wireless systems, you have to take into account the firmware versions of the involved S1100w and S3100 units. Use the following matrix to ensure complete compatibility between your units:

		S1100w and slave S3100		
		V2.55	V2.56	V2.60
Master S3100	V2.55	Yes	No	No
	V2.56	No	Yes	No
	V2.60	No	No	Yes

To update the firmware of the units without losing them in the field, follow these guidelines:

- Update the units starting with the farthest (in terms of number of RF hops) from the computer running the upgrade procedure.
- One step at a time, get closer to the computer.

For example, consider the following setup:



You should update the units in the following order:

1. S1100w 1—You then lose contact with S1100w 1.
2. S1100w 2—You then lose contact with S1100w 2.
3. Master S3100 1—You can then reach all units.
4. Slave S3100 2—You then lose contact will all units except master S3100 2.
5. Master S3100 2—You can then reach all units.

For the complete firmware update procedure, refer to the *SConfigurator User Manual* or the nDVR online help.

MAC Protocols

Depending on the type of applications, an S3100 unit uses one of the two proprietary MAC protocols that solve problems inherent to 802.11 wireless networking products:

- SPCF (SmartSight point of coordination function)—This protocol is used in point-to-multipoint applications. An SPCF wireless cell contains one master S3100 and multiple S1100w transmitters.

  SPCF resolves the “hidden node,” quality of service, range, and security problems.

  With the SPCF protocol, a master S3100 has total control over the radio frequency used; therefore, in an RF line-of-sight context, you cannot install two cells sharing the same frequency channel.

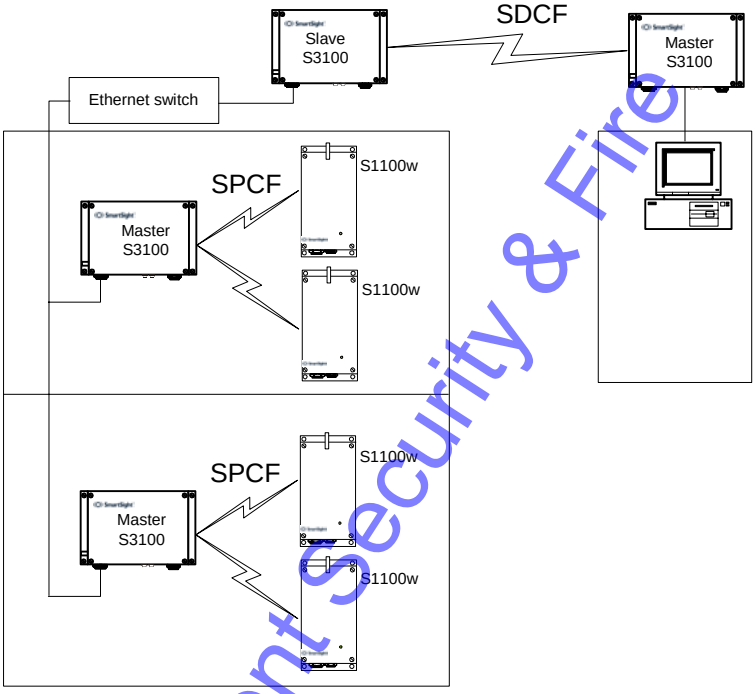
- SDCF (SmartSight distributed coordination function)—You use this protocol in point-to-point systems with a high volume of video transmission, typically over long distances or when a remote site is hard to reach. An SDCF wireless cell comprises two S3100 units, a master and a slave. You cannot use SDCF with S1100w units.

  SDCF optimizes the RF link by providing more data throughput. It also resolves the range and security problems of the 802.11 standard. However, SDCF does not manage the hidden node issue.

  Two SDCF cells can use the same frequency channel: They will share the available bandwidth.

These two protocols are optimized to work with SmartSight units; they cannot work with wireless units from other vendors.

Here is a typical context of use showing the two protocols. A point-to-multipoint system is installed on every floor of a multistorey parking building. The surveillance station is in another building. The SDCF cell acts as a wireless bridge between the two sites.



Video Bit Rate and Data Throughput

You can connect up to 16 S1100w and 7 slave S3100 units to a master bridge in a wireless cell. However, video quality, frame rate, and system layout can limit the number of units that a single master bridge can support.

Video quality and frame rate influence the required data throughput. Therefore, you need to carefully plan the number of cameras that will work on a link.

The following figures were measured in typical setup situations. They may vary depending on your configuration.

The total data throughput for the SPCF protocol is:

Bit Rate	SPCF throughput for a 3-mile (5-km) distance	SPCF throughput for a 15.5-mile (25-km) distance
6 Mbps	3 Mbps	3 Mbps
9 Mbps	4 Mbps	4 Mbps
12 Mbps	5 Mbps	5 Mbps
18 Mbps	6 Mbps	5.5 Mbps
24 Mbps	7 Mbps	6 Mbps
36 Mbps	8 Mbps	7 Mbps

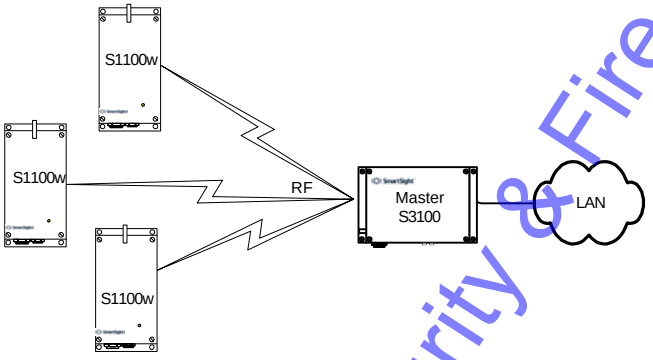
The values for the SDCF protocol, in a unidirectional UDP link setup, are:

Bit Rate	SDCF throughput for a 3-mile (5-km) distance	SDCF throughput for a 15.5-mile (25-km) distance
6 Mbps	4 Mbps	3.5 Mbps
9 Mbps	6 Mbps	5 Mbps
12 Mbps	7.5 Mbps	6 Mbps
18 Mbps	10 Mbps	7 Mbps
24 Mbps	11.5 Mbps	8 Mbps
36 Mbps	14.5 Mbps	9.5 Mbps

For the bit rate requirements of the video servers to which the cameras are connected, consult the *Bit Rate Settings for Video Servers* document located on the SmartSight Web site: **Support > Downloads > Manuals & Tools > Tools**.

Point-to-Multipoint Application

A point-to-multipoint application is a wireless cell made up of an S3100 bridge (the *S3100* product code, called the *master*) and several S1100w transmitters (the *stations*). The MAC protocol for the master S3100 is SPCF. Here is a typical point-to-multipoint system:



For example, to associate three S1100w units to one bridge, you have to:

1. Assign the same wireless passkey to the S1100w units and the S3100 bridge. The wireless passkey must be different from that of other collocated cells, if any.
2. Assign a frequency channel to the S3100 unit. The channel must be different from that of any other nearby cell. The associated S1100w units will automatically use their master's channel.
3. Install the S1100w units such that each one has a clear RF line of sight with the S3100 bridge.

For the complete configuration and installation procedure, see page 26.

Collocated Cells

You can operate many wireless cells in the same location, provided you follow guidelines relative to frequency channel, distance, and wireless passkey.

Regarding frequency channel, the guidelines vary depending on the MAC protocols:

- When at least one SPCF cell is involved, you cannot use the same frequency channel.
- Two SDCF cells can use the same frequency. They will share the available bandwidth.

The distance limitations are:

- To avoid material damages, you must never power any two units while their antennas are facing one another with a distance of less than 10 feet (3 meters).
- When using adjacent channels in the same frequency band, two antennas should be at a minimum distance of 3 feet (1 meter) from one another.
- With different frequency bands, two units can be side by side with no minimum distance between them.
- When collocating SDCF cells using the same frequency channel, you must carefully plan their maximum link distances (see page 54).

The wireless passkeys of collocated cells must be different from one another, regardless of their MAC protocols or frequency channels.

For example, to collocate three point-to-multipoint applications, each one made up of three S1100w units and one bridge (*S3100* product code), you have to:

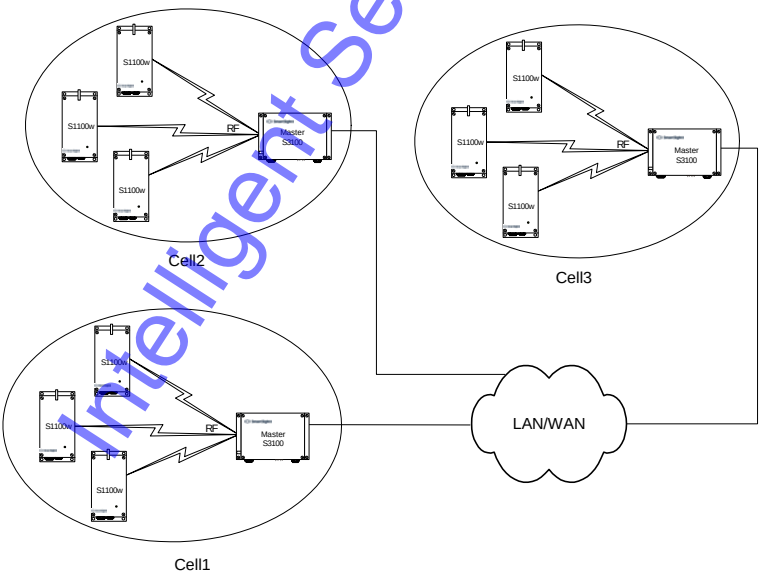
1. In each cell, assign the same wireless passkey to the S1100w units and the S3100 bridge. The wireless passkey must be different from that of the other cells.

2 Assign a different frequency channel to each S3100 unit; the associated S1100w units will automatically use their master's channel. For better isolation, use different frequency bands for adjacent cells. For example:

Unit	Cell	Channel	Wireless Passkey
S3100_1	Cell1	52	ertynmbvcxzapoiu
S1100w_11	Cell1	52	ertynmbvcxzapoiu
S1100w_12	Cell1	52	ertynmbvcxzapoiu
S1100w_13	Cell1	52	ertynmbvcxzapoiu
S3100_2	Cell2	149	PUK98rewq4123qzx
S1100w_21	Cell2	149	PUK98rewq4123qzx
S1100w_22	Cell2	149	PUK98rewq4123qzx
S1100w_23	Cell2	149	PUK98rewq4123qzx
S3100_3	Cell3	64	987123jkl456wert
S1100w_31	Cell3	64	987123jkl456wert
S1100w_32	Cell3	64	987123jkl456wert
S1100w_33	Cell3	64	987123jkl456wert

3 In each cell, install the S1100w units such that each one has a clear RF line of sight with its associated S3100 bridge.

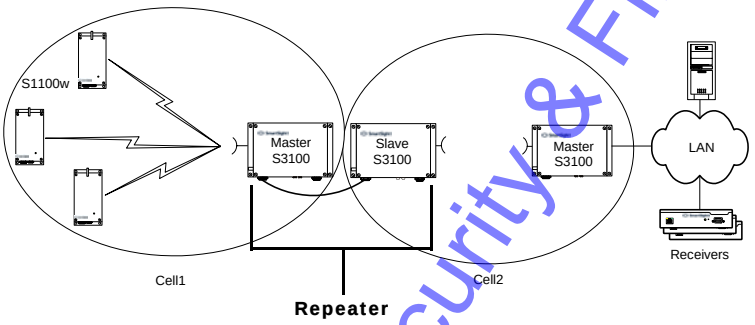
This application can be illustrated this way:



Repeater Application

A repeater is used as a range extender for wireless links, when you need a device to retransmit the signals coming from the S1100w units towards the Ethernet LAN. A typical context is when you cannot obtain RF line of sight between the transmitters and the S3100 connected to the wired LAN. A repeater device (*S3100-RP* product code) is made up of two S3100 units, a *master* and a *slave*.

A repeater application is in fact two collocated cells:



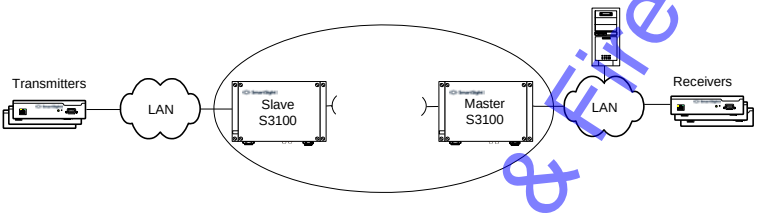
To operate the two cells forming the repeater:

1. In each cell, assign the same wireless passkey to all the units. The wireless passkey must be different from that of the other cell.
2. Always connect the S1100w units to a master S3100, never to a slave.
3. Set the MAC mode of the S3100 in Cell1 to SPCF.
4. Set the MAC mode of the two S3100 units in Cell2 to SDCF.
5. Assign a frequency channel to the master S3100 unit in each cell. For better isolation, use different frequency bands for adjacent cells.
6. Install the S1100w and slave S3100 units such that each one has a clear RF line of sight with its associated master.

For the complete configuration and installation procedure, see page 35.

Wireless Bridge Application

You can use two S3100 units (a master and a slave) to access remote or hard to reach video servers, or to send video through a long distance link. For instance, a wireless bridge application can connect remote S1500e series or S1600e video servers (the following illustration) or wireless units without RF line of sight (see page 13).



To create a wireless bridge application, you have to:

1. Assign the same wireless passkey to the two S3100 units.
2. Assign a frequency channel to the master S3100 unit.
3. Set the MAC mode of the two S3100 units to SDCF.
4. Install the S3100 units such that there is clear RF line of sight between the two antennas.

For the complete configuration and installation procedure, see page 39.

RF Planning

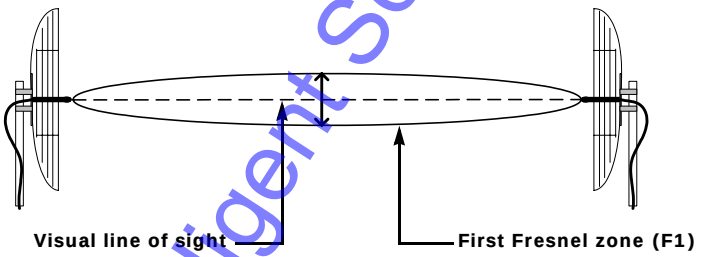
Successful operation of a wireless link depends on proper RF path planning and antenna installation. You have to install the antennas in such a way that there is clear RF line of sight between the two units.

Location Evaluation

The path between the two antennas must be free of obstacles that could disturb propagation. For very short link distances (less than 500 feet), you may be able to establish a working link despite partial path obstruction. However, radio waves will be in part absorbed and in part diffracted by the obstacles, therefore affecting link reliability. Because the reliability of such an installation is highly unpredictable, SmartSight does not recommend it. A path free of any obstacle is called an *RF line-of-sight path*.

To establish an RF line-of-sight path, you must take into account the beamwidth of the radio signal transmitted between the two antennas. This beamwidth is an elliptical area immediately surrounding the visual line of sight. It varies in thickness depending on the length of the signal line of sight; the longer the length, the thicker the beamwidth becomes.

The region outlined by the signal beamwidth is known as the *first Fresnel zone*. The Fresnel zone is always thicker at the mid-point between the two antennas. Therefore what appears to be a perfect line-of-sight path between the base and a remote station may not be adequate for a radio signal; this is the difference between "visual" and "RF" line of sight.



In practice, it has been determined that a radio path can be considered an RF line-of-sight path if it has a clear opening through 60% of the first Fresnel zone (or *0.6 F1*). Here are values for 0.6 F1 for various signal path distances and frequency bands:

Distance (miles/km)	2.45 GHz (feet/meter)	5.3 GHz (feet/meter)	5.8 GHz (feet/meter)	Earth curvature effect (feet/meter)
1 / 1.6	14 / 4.2	9.5 / 2.9	8.9 / 2.7	0
4 / 6.5	27 / 8.4	18.7 / 5.7	18 / 5.5	2 / 0.6
7 / 11.3	37 / 11	25 / 7.6	23.6 / 7.2	6 / 1.8
15 / 24	53 / 16	36.4 / 11.1	35 / 10.6	29 / 8.8

For distances under seven miles, the earth curvature effect is negligible. However, for greater distances, you need to consider it in your calculations; for instance, for a 15-mile link in the 2.4 GHz band, the two antennas must be located 82 feet higher than the highest obstacle in the RF line of sight between them (that is, 53 feet for the Fresnel zone plus 29 feet for the earth curvature effect). For help, consult the SmartSight project engineering group.

A common problem encountered in the field and related to the 0.6 F1 clearance rule is building obstruction. The proposed visual path may just barely clear a building but the RF line of sight will not. In such a case, the signal will be partially absorbed and diffracted. Increasing the height of the two antennas or the gain of the antennas are the only alternatives to improve the link quality.

Note

At 2.4 and 5 GHz, radio waves are highly attenuated by dense foliage. A link established in the fall or winter season may be adversely affected in the spring and summertime, if it is established below tree level.

Antenna Requirements

SmartSight offers many types of antennas for the S3100 to meet various distance requirements.

The factors to consider when choosing an antenna are the range to cover, the bandwidth requirement, and the frequency band used. For detailed values, consult the *Wireless Distance Calculations Table* located on the SmartSight Web site: **Support** > **Downloads** > **Manuals & Tools** > **Tools**.

Note

The values presented in the table were calculated with a 10-dB margin; they can be used directly for distances less than 7 miles (11.25 km). For greater distances, you might want to consider a higher security margin; therefore, the achievable distances will be shorter than those presented in the table.

Power Transmission

When choosing antennas, you must ensure that the combined transmission power of the unit and the antenna does not exceed the maximum value established by your country's regulations.

The transmission power of the unit and the maximum radiated power allowed by the FCC and IC regulations in North America vary depending on the frequency band used:

Frequency band	Channels	Transmitted power	Radiated power (EIRP)
2.4 GHz	1 to 11	17 dBm	36 dBm
5.25–5.35 GHz	52, 56, 60, 64	17 dBm	30 dBm
5.725–5.825 GHz	149, 153, 157, 161	17 dBm	53 dBm

Therefore, when choosing an antenna for your unit, you must take into account the "available" power. For instance, in the 5.25–5.35 GHz band, there is 13 dB available for the antenna. If you require a more powerful antenna, you have to lower the transmission power of the unit, using the **Tx Power Scale** parameter available in the **Wireless Communication** menu of the CLI.

Interference

In most countries, the 2.4 GHz license-free band is not regulated by a government agency; this absence of frequency coordination can result in interference between various systems. For instance, if a link with an RF line of sight is subject to excessive video delay and very low frame rate (or possibly breakdown of video images), it could be due to interference. Fortunately, there are existing tools that can be used to avert interference:

- RF channel selection—In the 2.4 GHz band, the S3100 offers 11 channels to choose from. In case of interference, it is recommended to change channel until a clean one is found.
- Antenna selection—Using a 16-dBi gain antenna instead of an 8.5-dBi one can significantly lower interference from other radio systems. Replace the antenna if switching channels does not correct the problem or if all channels must be used to collocate several systems.

The 5.3 and 5.8 GHz bands are less cluttered than the 2.4 GHz band, resulting in less potential interference from other wireless systems.

RF Exposure Considerations

In order to comply with the RF exposure requirements of CFR 47 part 15, the units must be installed in such a way as to allow a minimum separation distance of 12 inches (30 cm) between antennas and persons nearby.

3

Configuring and Installing the Unit

Depending on the S3100 model purchased, you can set up point-to-multipoint, repeater, or wireless bridge applications.

Computer Requirements

The minimum software and hardware requirements for the computer needed to configure the S3100 units are:

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

Point-to-Multipoint Application

A point-to-multipoint application is a wireless system made up of an S3100 bridge (the *S3100* product code) using the SPCF MAC protocol and several S1100w stations.

To set up such an application, you have to follow a series of steps:

1. Configuring the S1100w transmitters
2. Connecting power and Ethernet
3. Configuring the S3100 unit
4. Installing the S3100 unit

Configuration of the S1100w

You start by configuring the S1100w units associated to the S3100 bridge. For the procedure, refer to the *S1100w Quick Installation Guide*.

Power and Ethernet Connections

Before configuring the S3100 unit, you need to assemble components and plug cables. It is strongly recommended to execute these pre-installation tasks in a lab.

Use the supplied power-over-Ethernet (PoE) kit to power the S3100 unit and establish the Ethernet connection. In addition to the kit, your shipment includes an Ethernet cable with a weatherproof connector at one end that will go directly on the unit.

The PoE kit contains two items:

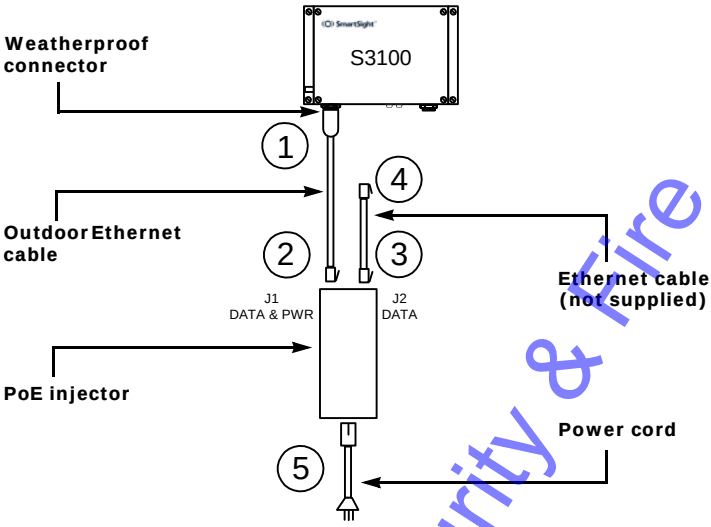
- Injector
- Power cord

Depending on your setup, you need to provide a straight-through or crossover Ethernet cable. The straight-through cable is to integrate the S3100 on a network; the crossover cable is to directly connect the unit to a computer. For their detailed pinouts, see page 59.

Note

The combined length of the two Ethernet cables (the supplied outdoor cable and the straight-through or crossover one) must not exceed 245 feet (75 meters).

To assemble the PoE kit:



1 Plug the supplied outdoor Ethernet cable (the end with the weatherproof connector) into the PoE receptacle of the S3100 unit. Lock the weatherproof connector by pushing forward the locking ring.

You unlock the connector by pulling back the locking ring, then withdrawing the plug.

2 Plug the other end of the outdoor Ethernet cable into the DATA & PWR port of the injector.

3 Connect one end of your Ethernet cable (straight-through or crossover, depending on your installation) into the DATA port of the injector.

4 Connect the other end of your Ethernet cable into an Ethernet device or your computer.

Warning

To avoid damaging your Ethernet equipment, ensure that your Ethernet cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

5 Power the S3100 unit by connecting the electric plug of the power cord into the outlet.

Configuration of the S3100

Before installing the S3100 unit, you need to change its default IP address to ensure compatibility with an existing network. You also have to set basic wireless parameters. For any other configuration task (including enabling SSL security) or for more information about the parameters, refer to the *SConfigurator User Manual*.

The MAC protocol in point-to-multipoint applications is always SPCF.

Write down the final values of the configuration parameters (especially the IP address and VSIP port) in the form located at the end of the *S3100 Quick Installation Guide*.

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.

To set the IP parameters:

1 Plug the external antenna on the main antenna connector of the unit.

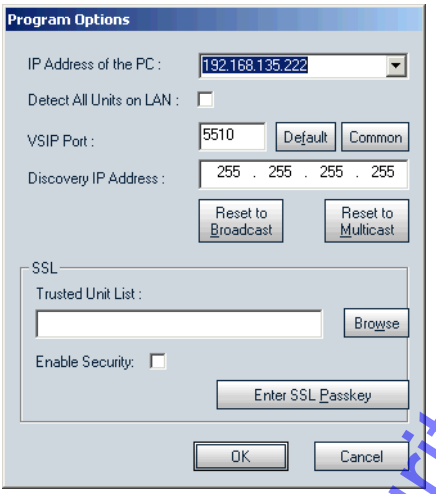
2 Power up the S3100 unit and connect it on the Ethernet network.

3 Start the SConfigurator software included on the *SmartSight Utilities* CD shipped with your unit.

The **SConfigurator** window appears.

4 From the **General** tab, click **Program Options**.

The **Program Options** window appears.



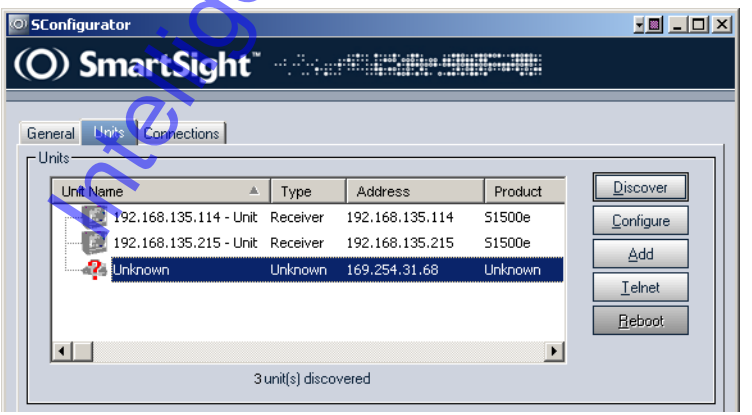
5 Ensure that the **VSIP Port** value is 5510; otherwise, click **Default**.

6 Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.

7 Check **Detect All Units on LAN**, then click **OK**.

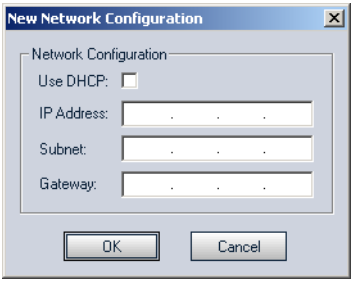
8 Choose the **Units** tab, then click **Discover**.

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



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

The **New Network Configuration** window appears.



10 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.

11 Click **OK**.

The S3100 unit reboots with its new network configuration.

To set the wireless parameters:

1 In SConfigurator, choose the **Units** tab, then click **Discover**.

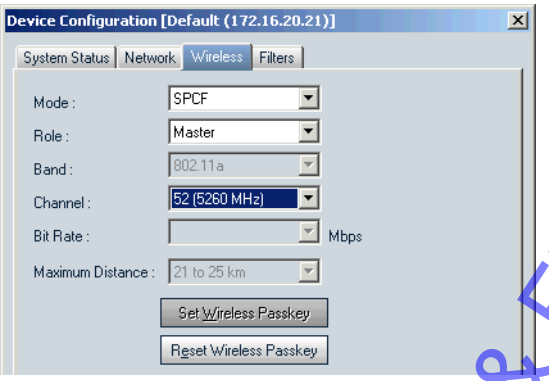
The new outdoor wireless bridge appears in the **Units** list.

2 Select the new S3100, then click **Configure**.

The **Device Configuration** window appears.

3 To change the name of the unit, click the **System Status** tab, then enter a meaningful name in the **Unit Name** field.

4 Click the **Wireless** tab.



5 Ensure that the content of the **Mode** field is **SPCF**.

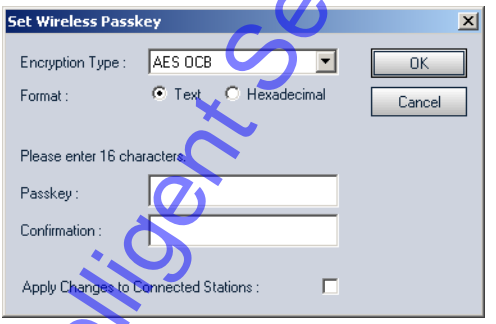
6 Ensure that the content of the **Role** field is **Master**.

7 Select the desired frequency channel.

8 Change the wireless passkey:

- Click **Set Wireless Passkey**.

  The **Set Wireless Passkey** window appears.



- Select the format of the passkey.
- In the **Passkey** field, enter the passkey (case-sensitive).

  The passkey must have exactly 16 characters if the format is **Text**, or 32 digits if **Hexadecimal**.

  For the wireless connection to be secure, do no enter a known name (like a street name), but instead use a mix of digits and letters. Furthermore, do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

- In the **Confirmation** field, enter again the passkey.
- Clear **Apply Changes to Connected Stations**.
- Click **OK**.

9 Back in the **Wireless** tab, click **OK**.

The S3100 unit is configured with the new parameters and reboots.

10 Using SConfigurator, ensure that the S3100 and its stations communicate well together:

- In the **Units** tab, the associated S1100w units should be hierarchically positioned under the S3100.
- In the **Wireless** tab of the S3100, the S1100w units should be in the **Stations** list.

Installation of the Equipment

After ensuring that the bridge and its stations are communicating properly in a lab, you can install the unit and its antenna in its final location.

You can install the outdoor wireless bridge either on a wall or on a pole.

Warnings

When installing collocated wireless systems, you have to take into account the distance limitations listed on page 16.

Always mount the unit with the mating connectors pointing downwards. Otherwise moisture may penetrate the unit; the associated repair costs are not covered by the warranty.

To install the S3100:

1 Plug the assembled PoE injector on the unit.

2 Connect your Ethernet cable in the PoE injector.

3 Install the S3100 in its final location:

- On a wall—Put four screws on the two side brackets and fix the unit at the desired location.
- On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the unit; then attach the brackets on the pole with the stainless steel clamps.

4 If you are installing the S3100 equipment in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add additional external surge protection to the PoE injector.

For more information, see page 65.

5 To enable the built-in surge protection, connect the unit to the ground using the grounding lug on its left side.

Use a large diameter wire (minimum AWG 10), and make it as short as possible.

6 If the S3100 unit will be directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield.

7 Connect the loose end of your Ethernet cable into an Ethernet device or your computer.

Warning

To avoid damaging your Ethernet equipment, ensure that the Ethernet cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

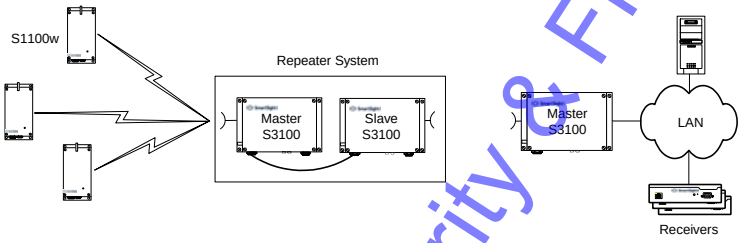
8 Power the unit by connecting the electric plug of the PoE injector into the outlet.

9 Install the antenna.

For the detailed procedure, see page 40.

Repeater Application

A repeater is used as a range extender for wireless links, when you need a device to retransmit the signals coming from S1100w units towards the Ethernet LAN. It is made up of two identical S3100 units, a master and a slave; any of the two can act as the master. You normally link the S1100w units to the master bridge. A repeater requires two wireless cells (for more information, see page 18). Here is a typical repeater application:



All devices in this setup (including the receivers and the S1100w units) must be in the same IP subnet.

To set up the repeater, you have to perform the following tasks:

1. Assembling the power devices
2. Configuring the master S3100 in the repeater
3. Configuring the slave S3100 in the repeater
4. Configuring and installing the master S3100 connected to the LAN
5. Installing the repeater units

Assembly of the Power Devices

Prior to configuring the two S3100 units, you need to assemble their power cord and power supply.

To assemble a power device:

1. Plug the weatherproof connector of the supplied power cord into the auxiliary 24V AC power connector of the unit.
2. Connect the loose end of the power cord into a 24V AC power supply.

Configuration of the Master Unit in the Repeater

Before installing the unit, you need to set its IP and wireless parameters.

To set the parameters of the master:

1. Set the IP parameters of the unit.

   See the complete procedure on page 29.

2. Set the wireless parameters of the unit:

   - Its mode must be **SPCF**.
   - Its role must be **Master**.

   See the complete procedure on page 31.

Configuration of the Slave Unit in the Repeater

Before installing the unit, you need to set its IP and wireless parameters.

To set the parameters of the slave:

1. Set the IP parameters of the unit.

   See the complete procedure on page 29.

2. In SConfigurator, choose the **Units** tab, then click **Discover**.

   The new bridge appears in the **Units** box.

3. Select the new S3100, then click **Configure**.

   The **Device Configuration** window appears.

4. To change the name of the unit, click the **System Status** tab, then enter a meaningful name in the **Unit Name** field.

5. Click the **Wireless** tab.

6. In the **Mode** field, select **SDCF**.

7. In the **Role** field, select **Slave**.

8. Click **OK** to save the settings.

   The unit reboots.

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

10 Select the slave unit, then click **Configure**.

The **Device Configuration** window appears.

11 Click the **Wireless** tab.

12 Select the desired bit rate.

13 Set the wireless passkey to a value different from that of the master in the repeater system (since the two S3100 units belong to two different wireless cells).

14 Back in the **Wireless** tab, click **OK**.

The slave unit reboots.

15 Using SConfigurator, ensure that the master and slave units communicate well together:

- In the **Units** tab, the slave unit should be hierarchically positioned under the master.
- In the **Wireless** tab of the master, the slave unit should be in the **Stations** list.

Configuration and Installation of the Master Unit Connected to the LAN

You configure and install the master S3100 unit connected to the Ethernet LAN for a point-to-multipoint application, with the following exceptions:

- Its wireless mode must be **SDCF**.
- Its wireless passkey must be the same as the slave's in the repeater system.

For the complete procedure, see page 26.

Installation of the Repeater Units

After ensuring that the master and slave S3100 units are communicating properly in a lab, you can install them in their final location.

You can install the S3100 units either on a wall or on a pole.

Warnings

When installing collocated wireless systems, you have to take into account the distance limitations listed on page 16.

Always mount the unit with the mating connectors pointing downwards. Otherwise moisture may penetrate the unit; the associated repair costs are not covered by the warranty.

To install the repeater units:

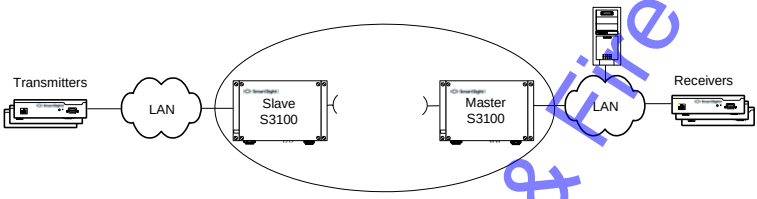
1. Install the master and slave units back to back in their final location:
   - ❖ On a wall—Put four screws on the two side brackets and fix the unit at the desired location.
   - ❖ On a pole—Screw the pole mount brackets (supplied with your shipment) in the back of the unit; then attach the brackets on the pole with the stainless steel clamps.
2. To enable the built-in surge protection, connect each unit to the ground using the grounding lug on its left side.

   Use a large diameter wire (minimum AWG 10), and make it as short as possible.
3. If the S3100 units will be directly exposed to the sun in an environment likely to reach 122°F (50°C), install sun shields.
4. Connect the supplied crossover Ethernet cable between the two units.
5. Power the units using the assembled power devices.
6. Install the antennas.

   For the detailed procedure, see page 40.

Wireless Bridge Application

You can use S3100 units to access remote or hard to reach video servers, or to send video through a long distance link. To build such an application, you need two bridge units (*S3100* product code); any of the two can act as the master. For example:



For the general configuration and installation procedures, see “Point-to-Multipoint Application,” page 26. You need to apply the following wireless configuration values:

1. For the slave unit:
   - Its mode is **SDCF**.
   - Its role is **Slave** (for more information, see “Configuration of the Slave Unit in the Repeater,” page 36).
2. For the master unit:
   - Its mode is **SDCF**.
   - Its role is **Master**.
   - Its wireless passkey must be the same as the slave’s.

Installation of the Antenna

You install the antenna after the S3100 unit is in place. The antennas provided by SmartSight are designed to be mounted on a mast or pole of 2–3 inch (5–7.5 centimeter) diameter.

To install the antenna:

1. Install the antenna above the S3100 unit. If you bought your antenna from SmartSight, use the supplied pole mount bracket.

   For illustrations of pole mount installations, see page 61.

2. Screw the SMA connector of the antenna cable to the S3100 main antenna port and tighten it with a 0.25-inch (0.6 centimeter) wrench.

   Warnings

   Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lb-in (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at www.pasternack.com).

   Do not use the auxiliary antenna connector and do not remove its termination cap.

3. Apply two or three layers of electrical tape around all RF connections.

   The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.

4. Carefully align the antenna with those of the other units (S1100w stations or master/slave S3100) so that they have RF line of sight.

5. To improve the signal level between two units, use the antenna alignment utility from SConfigurator.

LEDs

The S3100 unit comes with three bicolor (green-red) LEDs that provide detailed information on the unit activity.

- LAN—For the Ethernet network (802.3) status:

Condition	Indication
Steady green	The unit is connected to the Ethernet network.
Flashing green (1-sec. flash every 3 sec.)	The unit is in normal operation but is not connected to the network.
Flashing green (0.1 sec. off for each packet)	A packet is received or transmitted.
Red blink (0.1 sec.)	There is a communication error.
Flashing red (0.1 sec. intervals)	The unit is being identified.
Flashing red (1 sec. intervals)	On a master unit: There is another master currently running with the same frequency channel. (For more information, see page 43.)

- RF—For the wireless LAN (802.11) status:

Condition	Indication
Flashing green (1-sec. flash every 3 sec.)	The unit is in normal operation without any connected station.
Steady green	The unit is in normal operation with at least one connected station.
Flashing green (0.1 sec. off for each packet)	A packet is received or transmitted.
Red blink (0.1 sec.)	There is a communication error.
Flashing red (0.1 sec. intervals)	The unit is being identified.
Flashing red (1 sec. intervals)	On a master unit: There is another master currently running with the same frequency channel. (For more information, see page 43.)

- System status—For the general unit status, similar to the single status LED on the other SmartSight units:

Condition	Indication
Steady red (1 sec.)	The unit is powering up.
Steady green (3 to 5 sec.)	The unit is loading its firmware.
Flashing green (1 sec. intervals)	The unit is in normal operation.
Flashing red (1 sec. intervals)	The IP address of the unit is already assigned to another unit in the network. or On a master unit: There is another master currently running with the same frequency channel. (For more information, see page 43.)
Flashing green-red (1 sec. intervals)	The unit is undergoing a firmware update.
Flashing red (0.1 sec. intervals)	The unit is being identified.

Warning

The following power-up conditions on the system status LED 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, then 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 restart the firmware update procedure.

Duplicate Master Detection

The duplicate master detection problem occurs when two master S3100 units—with at least one using the SPCF mode—are using the same frequency channel and are “seeing” each other.

More specifically, the problem is detected when the second S3100 is booting up. This bridge refuses to start its wireless operations (to prevent any interference with the working setup) and makes its three LEDs flash red (1-second intervals). In the CLI of the unit, the **Current SPCF Connection Status** parameter turns to **Duplicate master detected**. This parameter is accessed by going through the following path: **Advanced > Communication Status and Statistics > Wireless Status**.

The already running master will not change its behavior.

Finding a “Lost” S3100

Since the S3100 does not have a serial port, you may have difficulty accessing it if you do not remember its IP address or VSIP port. For instance, if you enabled security on the unit, you cannot access it with Telnet; if you lost its VSIP port, you cannot locate it with SConfigurator.

To find a “lost” S3100 unit, you need to use SConfigurator and the common VSIP port.

To find a lost S3100:

1. Open SConfigurator.
2. From the **General** tab, click **Program Options**.
3. Click **Common** to set the common VSIP port, then **OK**.
4. Click the **Units** tab.
5. Click **Discover**.

   All units on the network, regardless of their configurable VSIP ports, appear in the **Units** list. Locate the lost S3100 and write down its VSIP port and IP address in the form located at the end of the *S3100 Quick Installation Guide*.

4

Setting Parameters with the CLI

The S3100 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.

Getting Started

You access the CLI through a network connection.

Starting the CLI

You can use the Telnet command to open the command line interface of the S3100.

Note

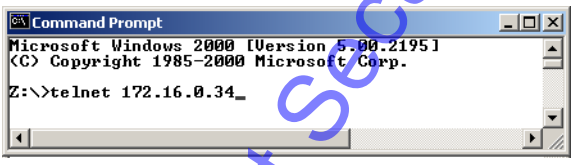
Ensure that your PC and the S3100 unit are in the same IP subnet.

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**.



The CLI main menu appears.

```
*********************************
Main Menu
---------------------------------
Menus:
1) Access Management
2) System Status
3) Network
4) Ethernet Communication
5) Bridge Communication
6) Wireless Communication
7) 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.

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 Telnet session.

```
*********************************************
Main Menu \ Access Management \ User Accounts
---------------------------------------------
Parameters:
1) User Accounts          : Disabled
2) Administrator User Name: USERNAME
3) Administrator Password : PASSWORD

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
- SSL

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

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

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. Be aware that it is the only available update method for the S3100, since it does not have a serial port.

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, you will not have access to the unit CLI anymore.

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. It also means that you cannot access the unit anymore with Telnet and you cannot perform firmware updates through the IP network on it.

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) or nDVR (in the Resource Administration Tool).

System Status

The system status information indicates the current values of internal S3100 parameters, including the firmware version.

```
************************************************
Main Menu \ System Status
------------------------------------------------
Parameters:
   Firmware Version    : 2.60-  build 112
   Build Date          : Nov 19 2003 at 12:22:57
   CPU Info            : Rev. 1.0
   CPU Frequency       : 165000000
   Uptime              : 00:17:38
   Serial Number       : 00079a-10000f
   CPLD Version        : 0
   Flash Size          : 4
   Internal Value 1    : 3452804 / 8
   Audio Hardware      : Absent
   Production Date     :
   Unit Firmware Size  : 2495 KB
   Backup Firmware Size: 749 KB

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

Network

The Network menu allows you to configure several parameters to ensure the compatibility between the S3100 and its IP network.

```
*********************************************
Main Menu \ Network
---------------------------------------------
Parameters:
1) DHCP Configuration        : Disabled
2) Local IP Address          : 192.168.135.81
3) Subnet Mask               : 255.255.255.0
4) Gateway                   : 192.168.135.2
5) Primary DNS Server Address: 192.168.135.2
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 D, page 63.

You can set this option only if the S3100 is connected to a network that uses a DHCP server.

Local IP Address

The IP address is the identifier of the S3100 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.

Write down the final IP address in the form located at the end of the *S3100 Quick Installation Guide*.

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.

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.

Wireless Communication

The Wireless Communication menu contains a set of parameters relative to radio frequency (RF).

```
**********************************************************
Main Menu \ Wireless Communication
----------------------------------------------------------

Parameters:
 1) MAC Mode                                  : SDCF
 2) Key Entry Format                          : String
 3) Wireless Passkey                          : ********
 4) Wireless Role                             : Master
 5) Wireless-to-Wireless IP Multicast         : Denied
 6) 802.11a Tx Bit Rate                       : Auto rate control
 7) 802.11a Channel                           : 149 (5745 MHz)
 8) Tx Power Scale                            : 100%
 9) Maximum Link Distance                     : 4-6 mi. (6-10 km)
10) IP Multicast Forward from this Interface: Allowed

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

MAC Mode

The two available MAC (media access control) modes are **SDCF** and **SPCF**. For more information, see page 12.

Key Entry Format

The wireless passkey can have two formats: string (default) or hexadecimal.

Wireless Passkey

The wireless passkey is a unique case-sensitive identifier enabling secure and encrypted RF communication in a wireless cell (that is, with the other slave bridges and S1100w units). The passkey length varies depending on the key entry format:

- 32 digits if hexadecimal
- 16 characters if string

For the wireless connection to be secure, do no enter a known name (like a street name), but instead use a mix of digits and letters. Furthermore, do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

Wireless Role

The wireless role represents the function of the unit in the wireless system. Possible values are: **Master** (default) and **Slave**. For more information, see “System Planning,” page 10.

802.11a Tx Bit Rate

The transmission bit rate is the data rate at which the unit operates. A high bit rate reduces the effective distance between two functional units.

You can set the bit rate in slave S3100 units only.

When a slave unit connects to its master, it automatically receives the best possible value (the **Auto rate control** value), with an RF margin of 15 dB. In the SDCF MAC mode, the bit rate can vary according to the quality of the RF link; in SPCF, it will remain to the set value, to the detriment of the quality.

If you manually change the bit rate, you have to take into account the RF margin. Therefore, a connection between the slave and its master can be possible with a margin lower than 15 dB. If the connection cannot be made at the requested bit rate, it will be performed at a lower rate. Therefore, the forced bit rate can be considered the maximum rate that will be used.

The available bit rates for the slave S3100 unit are: 6, 9, 12, 18, 24, and 36 Mbps.

Note

The 48 and 54 Mbps bit rates will be supported in a future firmware release.

802.11a Channel

On a master bridge, you can choose the RF channel that will be used by the wireless system. The channels available in North America are:

- 52, 56, 60, and 64 in the 5.3 GHz band
- 149, 153, 157, and 161 in the 5.8 GHz band

To know which channels are available elsewhere, refer to the specific country’s legislation.

On a slave bridge, you can specify an initial value for the *roaming* process by which the unit will find its master; however, this initial channel may not be the one used by the master bridge.

Tx Power Scale

The transmission power scale indicates the emitting power of the unit radio. The available values are:

- 100%—The maximum allowed.
- 50%—The power is reduced by 3 dB.
- 25%—The power is reduced by 6 dB.
- 12.5%—The power is reduced by 9 dB.
- Minimum—The power is set at 3 dBm.

You have to lower the transmission power of the unit if the combined power of the radio and the antenna exceeds the maximum value established by your country's regulations (for the list of the maximum values, see page 22).

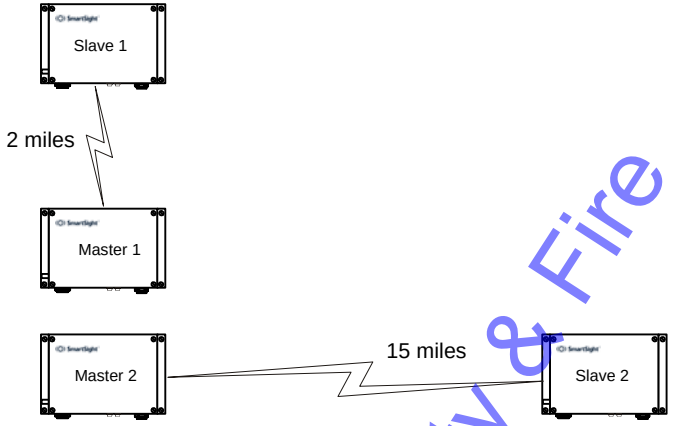
Maximum Link Distance

The maximum link distance parameter appears when the MAC mode is SDCF. It specifies the maximum transmission distance, between any two units, in all wireless cells present in the same geographical region and sharing the same frequency channel.

The two S3100 units making up an SDCF wireless cell must have the same value for this parameter. Possible values are:

- 0-3 miles (0-5 km)
- 4-6 miles (6-10 km)—default
- 7-9 miles (11-15 km)
- 10-12 miles (16-20 km)
- 13-15 miles (21-25 km)

For instance, consider the following setup, where the two wireless cells use the same frequency channel:



Since the two masters are in RF line of sight, all units must set their maximum link distance values to 15 miles. Otherwise packet collisions may occur, resulting in lost data.

Advanced

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

```
************************************************************
*        Smartsight Networks S3100 - 172.16.20.21          *
************************************************************
Main Menu \ Advanced
------------------------------------------------------------
Menus:
1) System Time
2) Power Management
3) VSIP
4) VSIP Statistics
5) Communication Status and Statistics
6) Test and Debug

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

To recognize an S3100 among a large set of units, you can make its three LEDs flash red rapidly.

To identify an S3100 unit:

1. From the main menu, choose **Advanced**, then press **Enter**.
2. Enter **i** to make the LEDs flash red. Re-enter **i** to set the LEDs to their previous 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 user parameters to their factory settings (described in Appendix A, page 57). All user-defined values will be lost.

Following a reset, you will need to reprogram the S3100 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 S3100. A system reboot clears all unsaved changes in the CLI and returns to your preset configuration.

A

Factory Default Configuration

This appendix lists the factory default configuration of the S3100 units.

The S3100 is programmed at the factory with the following configuration:

Type	Configuration
Access management	◆ User name: USERNAME ◆ 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)
Wireless Communication	◆ Key entry format: String ◆ Wireless passkey: ABCDEFGHIJKLMNOP ◆ 802.11a Tx bit rate: Auto rate control ◆ 802.11a channel: 52 (5260 MHz) ◆ Maximum link distance: 4–6 miles (6–10 km)
VSIP	◆ VSIP Port: 5510 ◆ VSIP multicast IP address: 224.16.32.1 ◆ VSIP discovery IP address: 255.255.255.255

B

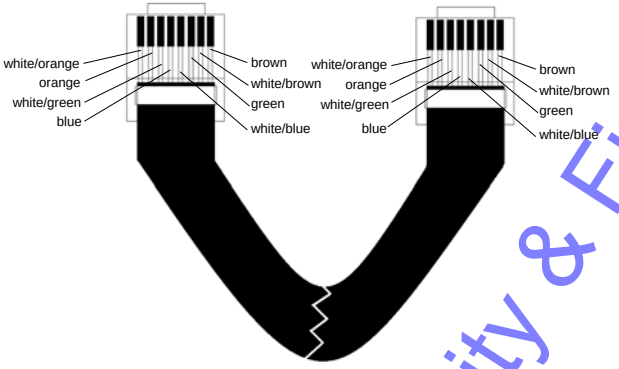
RJ-45 Ethernet Cables

Depending on whether the S3100 unit is integrated on a LAN or not, the Ethernet cable varies:

- If on a LAN, use a straight-through cable.
- If connected directly to a computer, use a crossover cable.

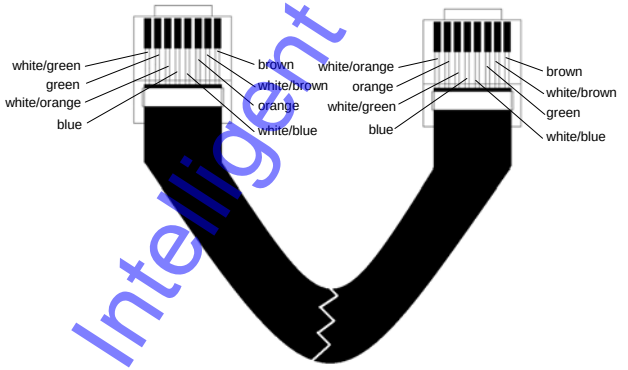
Straight-Through Cable

Here is the bottom view of the RJ-45 connectors on a straight-through Ethernet cable:



Crossover Cable

Here is the bottom view of the RJ-45 connectors on a crossover Ethernet cable:



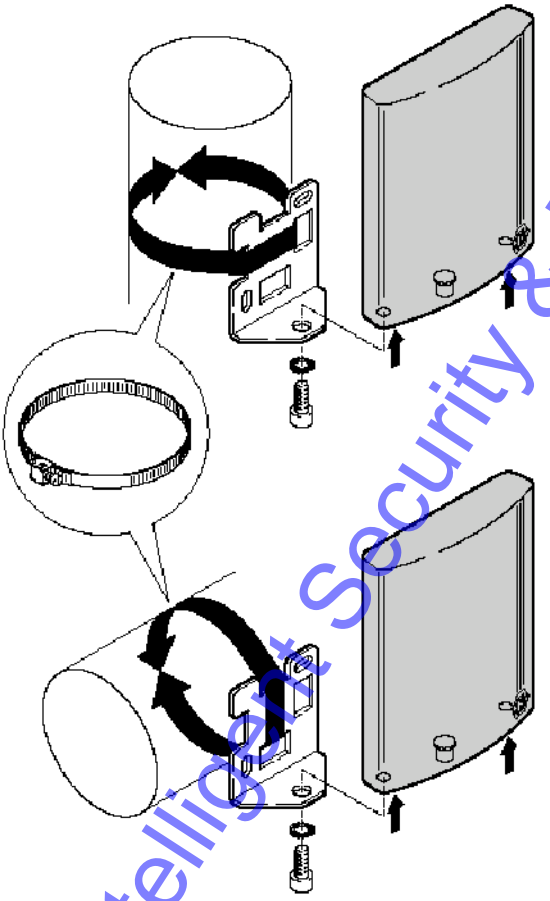
C

Pole Mounting of the Antennas

The installation procedure for the external antenna varies depending on the model.

ANT-WP13-5x/S Antenna

Here is the way to install the 13-dBi antenna to be used in the 5 GHz band:



D

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.

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

E

Surge Protection

Voltage and current surges can be induced by lightning strikes or power line transients. In the real world, under the right circumstances, these surges can reach sufficiently high levels to damage almost any electronic equipment. Therefore you need to add protection to your units.

The S3100 provides built-in surge protection on the Ethernet/PoE and 24V AC power connectors. The antenna connectors do not have surge protection; this situation should not cause problems as long as you keep the antenna cable short—that is, below 6.6 feet (2 meters).

If you are installing an S3100 unit (*S3100* model) in a heavy lightning environment, or in a site where large AC mains power fluctuations are a common occurrence, SmartSight recommends that you add surge protection on the DATA & PWR port of the PoE injector. It will protect your equipment and the power inserter from surges coming down from the Ethernet cable.

Using a surge protector is strongly recommended if the Ethernet cable runs outside the building for more than 82 feet (25 meters). This device should be installed at the entry point of the cable inside the building. To be effective, this protection equipment must be properly grounded.

PoE protectors recommended by SmartSight include:

Company	Part number	Web site
Citel	MJ8-505-24D3A60	www.citelprotection.com
Transtector Systems	1101-693 TSJ POE-48	www.transtector.com

For the curious mind, a surge protector helps to clamp the surge to safe levels and divert its energy to the earthing point, preventing the surge from damaging your device. Experienced installers know that an effective surge protection must be installed with proper earthing and grounding.

F

Technical Specifications

Here are the S3100 technical specifications:

Network	RF interface	SmartSight SPCF and SDCF
	Frequency	5.250–5.350 GHz (U-NII-2) 5.725–5.825 GHz (U-NII-3/ISM)
	Modulation	OFDM
	Channels	8 non-interfering
	RF Encryption	128-bit AES
	Data rate (max. burst rate)	6, 9, 12, 18, 24, and 36 Mbps
	Ethernet connector	Weatherproof 10/100Base-T (RJ-45)
	Security	SSL-based authentication
	Range (RF line of sight)	5.250-5.350 GHz: up to 2.5 miles (4.0 km) with integrated 13 dBi antenna 5.725-5.825 GHz: up to 2.0 miles (3.3 km) with integrated 13 dBi antenna 5.725-5.825 GHz: up to 5.1 miles (8.2 km) with optional 18 dBi antenna 5.725-5.825 GHz: up to 10.2 miles (16.4 km) with optional 24 dBi antenna
	System gain	5.250-5.350 GHz: 128 dB with integrated 13 dBi antenna 5.725-5.825 GHz: 126 dB with integrated 13 dBi antenna 5.725-5.825 GHz: 135 dB with optional 18 dBi antenna 5.725-5.825 GHz: 147 dB with optional 24 dBi antenna
	Protocols	Transport: RTP/IP, UDP/IP, TCP/IP, or multicast IP Others: DNS and DHCP client
Power	Input voltage	S3100: 48V DC PoE S3100-RP: 24V AC
	Consumption	12W (250 mA at 48V DC) 25 VA at 24V AC
	Connector	Weatherproof circular
Physical	Size	8.1L x 5.5W x 4.1H in. (205L x 140W x 105H mm)
	Weight	2.0 lbs (0.90 kg)
	Environment	-22ºF to 122ºF (-30ºC to 50ºC)
	Humidity	95% non condensing at 122°F (50°C)

	LED indicators	Status, wireless activity, LAN activity
	Antenna connectors	SMA female
Certification and Regulation	USA	FCC part 15 (subparts B, C, and E)
	Canada	RSS-210 and ICES-003

Glossary

This glossary is common to all SmartSight products.

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.

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.

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.

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.

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.

Index

Compliance

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the effective isotropic radiated power (EIRP) is not more than that required for successful communication.

Note

The S3100 units require professional installation. They should be installed in a location that would prevent the general population from approaching from 1 meter of the radiating element.

USA

This device complies with part 15 of the FCC (Federal Communications Commission) rules (see http://www.fcc.gov/).

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the S3100 unit
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Any changes or modifications not expressly approved by SmartSight could void the user's authority to operate the equipment.

Canada

This device has been designed to operate with an antenna having a maximum gain of 16 dBi on the 2.4 GHz frequency band and of 24 dBi on the 5.3 and 5.8 GHz bands. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

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

Intelligent Security & Fire

www.smartsightnetworks.com