Wi-Fi Administration and Operation

Table of Contents

Inti	roduction	2
(Qualified Persons	2
F	Read this Instruction Sheet	2
F	Retain this Instruction Sheet	2
F	Proper Application	2
5	Special Warranty Provisions	2
1	Narranty Qualifications	3
Saf	fety Information	4
ι	Jnderstanding Safety-Alert Messages	4
F	Following Safety Instructions	4
F	Replacement Instructions and Labels	4
Sal	iety Precautions	5
-		Č
Ov	erview	6
Wi-	Fi Authentication Key Generator	9
Dat	tabase Editor Program1	2
Dat	tabase Editor Program 1 Security Key Manager 1	2
Dat S	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1	2 2
Dat S E A	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1	2 2 4
Dat S E A	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 the Database 1	2 2 4
Dat E /	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 the Database 1 Data Entry with Notepad 1	2 2 4 5
Dat E /	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 the Database 1 Data Entry with Notepad 1 Navigation 1	2 4 5 7
Dat E / [N [tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 the Database 1 Data Entry with Notepad 1 Navigation 1 Delete/Undelete 1	2 2 4 5 7 8 9
Dat 8 7 1 1 1 1 1	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 the Database 1 Data Entry with Notepad 1 Navigation 1 Delete/Undelete 1 Jsing a Dongle 2	2 12 14 15 17 18 19 20
Dat E A I I I I I I	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 the Database 1 Data Entry with Notepad 1 Navigation 1 Delete/Undelete 1 Jsing a Dongle 2 Formatting a Dongle 2	2 12 14 15 17 18 19 20 22
Dat E F C C C C C C C C C C C C C C C C C C	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 Add IntelliRupter Fault Interrupters to 1 Data Entry with Notepad 1 Navigation 1 Delete/Undelete 1 Jsing a Dongle 2 Formatting a Dongle 2 Creating Regions and Crews 2	2 12 14 15 17 18 19 20 22 23 24
Dat S E A C I I I V I V I V I V I V I	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 Add IntelliRupter Fault Interrupters to 1 Data Entry with Notepad 1 Navigation 1 Delete/Undelete 1 Jsing a Dongle 2 Formatting a Dongle 2 Creating Regions and Crews 2 Fi Configuration File 2	2 12 14 15 17 18 19 20 22 23 24 26
Dat 5 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 Add IntelliRupter Fault Interrupters to 1 Data Entry with Notepad 1 Data Entry with Notepad 1 Delete/Undelete 1 Jsing a Dongle 2 Formatting a Dongle 2 Creating Regions and Crews 2 Fi Configuration File 2 WAN Radio Configuration and Wi-Fi Access 2	2 12 14 15 17 18 19 20 22 23 24 26
Dat 5 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 Add IntelliRupter Fault Interrupters to 1 Data Entry with Notepad 1 Data Entry with Notepad 1 Delete/Undelete 1 Jsing a Dongle 2 Formatting a Dongle 2 Creating Regions and Crews 2 Fi Configuration File 2 WAN Radio Configuration and Wi-Fi Access 2 Exporting Configuration Files 2	2 12 14 15 17 18 19 22 23 24 26 29
Dat 5 6 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	tabase Editor Program 1 Security Key Manager 1 Enter Master Key Name 1 Add IntelliRupter Fault Interrupters to 1 Add IntelliRupter Fault Interrupters to 1 Data Entry with Notepad 1 Navigation 1 Delete/Undelete 1 Jsing a Dongle 2 Formatting a Dongle 2 Creating Regions and Crews 2 Fi Configuration File 2 WAN Radio Configuration and Wi-Fi Access 2 Exporting Configuration Files 2 Decrypting a Configuration File 3	2 12 14 15 17 18 19 20 22 32 4 26 29 32

Connecting to an IntelliRupter Fault Interrupter	. 33
Loading Wi-Fi Keys With Wi-Fi Admin	. 34
Wi-Fi Admin Functions Uploading Wi-Fi Firmware. Security Event Logs. Wi-Fi Device Status Communication Counters Wi-Fi Module Reboot. WAN Port Settings	. 36 37 39 40 40 41
Wi-Fi Security Key Administration	. 42 42 43 44 47 58 63 66
Loading Wi-Fi Keys With IntelliLink Setup Software	. 69
LinkStart Database Searches	. 71
Removing Wi-Fi Security Keys	74
Excel File Examples Converting MBL_DB.csv to LSDB.txt Entering a New LSDB.txt File Checking File with a Binary Viewer	. 78 . 78 . 82 . 84
Frequently Asked Questions	. 89

NOTICE

This instruction sheet is only applicable to the R0 Communication Module.

Refer to S&C Instruction Sheet 766-524 for an R3 Communication Module using a firmware revision earlier than 3.0 and S&C Instruction Sheet 766-528 for an R3 Communication module using a firmware revision 3.0 or later.



Instruction Sheet 766-522

Introduction

Qualified Develope	
Qualified Persons	
	Only qualified persons knowledgeable in the installation, operation, and maintenance of overhead and underground electric distribution equipment, along with all associated hazards, may install, operate, and maintain the equipment covered by this publication. A qualified person is someone trained and competent in:
	 The skills and techniques necessary to distinguish exposed live parts from nonlive parts of electrical equipment
	 The skills and techniques necessary to determine the proper approach distances corresponding to the voltages to which the qualified person will be exposed
	 The proper use of special precautionary techniques, personal protective equipment, insulated and shielding materials, and insulated tools for working on or near exposed energized parts of electrical equipment
	These instructions are intended only for such qualified persons. They are not intended to be a substitute for adequate training and experience in safety procedures for this type of equipment.
Read this Instruction Sheet	NOTICE
	Thoroughly and carefully read this instruction sheet and all materials included in the product's instruction handbook before installing or operating an IntelliRupter® fault interrupter. Become familiar with the Safety Information and Safety Precautions on pages 4 and 5. The latest version of this publication is available online in PDF format at sandc.com/en/support/product-literature/ .
Retain this Instruction Sheet	This instruction sheet is a permanent part of the IntelliRupter fault interrupter. Designate a location where users can easily retrieve and refer to this publication.
Proper Application	
	The equipment in this publication is only intended for a specific application. The application must be within the ratings furnished for the equipment. Ratings for the equipment can be found on the nameplate affixed to IntelliRupter fault interrupter as and in S&C Specification Bulletin 766-31.
Special Warranty Provisions	The standard warranty contained in the seller's standard conditions of sale, as set forth in Price Sheets 150 and 181, applies to the IntelliRupter fault interrupter and its associated options except for the control group as applicable. For these devices, the first and second paragraphs of said warranty are replaced by the following:
	(1) General: The seller warrants to the immediate purchaser or end user for a period of 10 years from the date of shipment that the equipment delivered, with the exception of a radio, will be of the kind and quality specified in the contract description and will be free of defects of workmanship and material. Should any failure to conform to this warranty appear under proper and normal use within 10 years after the date

of shipment, the seller agrees, upon prompt notification thereof and confirmation the equipment has been stored, installed, operated, and maintained in accordance with recommendations of the seller and standard industry practice, to correct the nonconformity either by repairing any damaged or defective parts of the equipment or (at seller's option) by shipment of necessary replacement parts.

The seller's warranty does not apply to any equipment that has been disassembled, repaired, or altered by anyone other than the seller. This limited warranty is granted only to the immediate purchaser or, if the equipment is purchased by a third party for installation in third-party equipment, the end user of the equipment. The seller's duty to perform under any warranty may be delayed, at the seller's sole option, until the seller has been paid in full for all goods purchased by the immediate purchaser. No such delay shall extend the warranty period.

The seller further warrants to the immediate purchaser or end user that for a period of two years from the date of shipment the software will perform substantially in accordance with the then-current release of specifications if properly used in accordance with the procedures described in seller's instructions. The seller's liability regarding any of the software is expressly limited to exercising its reasonable efforts in supplying or replacing any media found to be physically defective or in correcting defects in the software during the warranty period. The seller does not warrant the use of the software will be uninterrupted or error-free.

For equipment/services packages, the seller warrants, for a period of one year after commissioning, that the IntelliRupter fault interrupters will provide automatic fault isolation and system reconfiguration per agreed-upon service levels. The remedy shall be additional system analysis and reconfiguration of the IntelliTeam® SG Automatic Restoration System until the desired result is achieved.

Warranty Qualifications

The standard warranty contained in the seller's standard conditions of sale, as set forth in Price Sheets 150 and 181, does not apply to major components not of S&C manufacture, such as batteries, customer-specified remote terminal units and communication devices, as well as hardware, software, resolution of protocol-related matters, and notification of upgrades or fixes for those devices. The seller will assign to the immediate purchaser or end user all manufacturers' warranties that apply to such major components.

The seller's standard warranty does not apply to any components not of S&C manufacture that are supplied and installed by the purchaser or to the ability of seller's equipment to work with such components.

Warranty of equipment/services packages is contingent upon receipt of adequate information on the user's distribution system, sufficiently detailed to prepare a technical analysis. The seller is not liable if an act of nature or parties beyond S&C's control negatively impact performance of equipment/services packages; for example, new construction that impedes radio communication, or changes to the distribution system that affect protection systems, available fault currents, or system loading characteristics.

Understanding Safety-Alert Messages

Several types of safety-alert messages may appear throughout this instruction sheet and on labels and tags attached to the product. Become familiar with these types of messages and the importance of these various signal words:

▲ DANGER

"DANGER" identifies the most serious and immediate hazards that will likely result in serious personal injury or death if instructions, including recommended precautions, are not followed.

⚠ WARNING

"WARNING" identifies hazards or unsafe practices that can result in serious personal injury or death if instructions, including recommended precautions, are not followed.

⚠ CAUTION

"CAUTION" identifies hazards or unsafe practices that can result in minor personal injury if instructions, including recommended precautions, are not followed.

NOTICE

"NOTICE" identifies important procedures or requirements that can result in product or property damage if instructions are not followed.

Following Safety Instructions

If any portion of this instruction sheet is unclear and assistance is needed, contact the nearest S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C's website **sandc.com**, or call the S&C Global Support and Monitoring Center at 1-888-762-1100.

NOTICE

Read this instruction sheet thoroughly and carefully before
operating an IntelliRupter fault interrupter.



Replacement Instructions and Labels

If additional copies of this instruction sheet are required, contact the nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

It is important that any missing, damaged, or faded labels on the equipment be replaced immediately. Replacement labels are available by contacting the nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

▲ DANGER



IntelliRupter PulseCloser Fault Interrupters operate at high voltage. Failure to observe the precautions below will result in serious personal injury or death.

Some of these precautions may differ from your company's operating procedures and rules. Where a discrepancy exists, follow your company's operating procedures and rules.

- QUALIFIED PERSONS. Access to an IntelliRupter fault interrupter must be restricted only to qualified persons. See the "Qualified Persons" section on page 2.
- 2. **SAFETY PROCEDURES.** Always follow safe operating procedures and rules.
- PERSONAL PROTECTIVE EQUIPMENT. Always use suitable protective equipment, such as rubber gloves, rubber mats, hard hats, safety glasses, and flash clothing, in accordance with safe operating procedures and rules.
- SAFETY LABELS. Do not remove or obscure any of the "DANGER," "WARNING," "CAUTION," or "NOTICE" labels.
- OPERATING MECHANISM AND BASE. IntelliRupter fault interrupters contain fast-moving parts that can severely injure fingers. Do not remove or disassemble operating mechanisms or remove access panels on the IntelliRupter fault interrupter base unless directed to do so by S&C Electric Company.
- 6. ENERGIZED COMPONENTS. Always consider all parts live until de-energized, tested, and grounded. The integrated power module contains components that can retain a voltage charge for many days after the IntelliRupter fault interrupter has been de-energized and can derive a static charge when in close proximity to a high-voltage source. Voltage levels can be as high as the peak line-to-ground voltage last applied to the unit. Units energized or installed near energized lines should be considered live until tested and grounded.

- GROUNDING. The IntelliRupter fault interrupter base must be connected to a suitable earth ground at the base of the utility pole, or to a suitable building ground for testing, before energizing an IntelliRupter fault interrupter, and at all times when energized.
- The ground wire(s) must be bonded to the system neutral, if present. If the system neutral is not present, proper precautions must be taken to ensure the local earth ground, or building ground, cannot be severed or removed.
- VACUUM INTERRUPTER POSITION. Always confirm the Open/Close position of each interrupter by visually observing its indicator.
- Interrupters, terminal pads, and disconnect blades on disconnect-style models may be energized from either side of the IntelliRupter fault interrupter.
- Interrupters, terminal pads, and disconnect blades on disconnect-style models may be energized with the interrupters in any position.
- MAINTAINING PROPER CLEARANCE. Always maintain proper clearance from energized components.

This document is applicable for IntelliRupter Installer versions 3.5.x or later, which can only operate with WiFiAdminInstaller 2.0.0 and later. For IntelliRupter Installer versions 3.4.9 and earlier, refer to S&C Instruction Sheet 766-521.

Two programs are used to generate security keys. The Security Key Generator creates the key files, and the Security Key Manager database editor assigns keys to specific Intelli-Rupter fault interrupters.

The distribution engineer or a security administrator has responsibility for authentication key security. The most secure procedure is installing the Security Key Generator program on a security PC and installing the Security Key Manager program on a separate database PC. Keys generated on the security PC are then transferred with a secure means, such as a USB thumb drive (dongle), to the database PC.

The Security Key Generator program, by default, saves key files in the LinkStart folder. The default path is found at: C:\ProgramData\S&C Electric\LinkStart.

Note: The Program Data folder is a hidden folder and will require the folder options to be set to "Show hidden files" before it can be viewed. The Security Key Manager and LinkStart programs also store files in a LinkStart folder located at: \Users\Public\Documents\S&C Electric\LinkStart for Windows 10 and Windows 11. This folder requires administrative privilege and uses folder security for access to existing files and for adding new files.

Transferring data is simple. Using administrative and folder privileges on both computers, move the files from the security PC LinkStart folder to the database PC LinkStart folder.

NOTICE

The key files are generated on the security PC. For each named key there will be two files, one with a .pub file name extension and one with a .pri extension. Both files are part of a single key pair used half by the Wi-Fi module and half by the LinkStart program.

It is important to back up and properly manage the key files. When a key is generated it can never be regenerated. This means the Security Key Generator program will not duplicate a key set if the same key name is used. Instead of duplication, two different sets of key files with the same name will be generated.

Take care to avoid this situation, so a user will not be locked out because the wrong key that has the "right" name is used.

For authentication purposes, the LinkStart program encrypts specifically defined data with its private key, so it can be decrypted by the Wi-Fi module using the public key on the mobile computer. The Wi-Fi module, in turn, encrypts different specifically defined data with its private key, so it can be decrypted by LinkStart using the Wi-Fi module public key. This requires the Wi-Fi module to be supplied with a private key and a different pair's public key and for LinkStart to be supplied with the public part of the first key pair and the private part of the second key pair.

The most secure method for deploying security keys is through the use of an external USB device called a dongle. The dongle is a USB thumb drive that uses a proprietary software interface to read and write its contents. It provides a secure storage location for the necessary keys used to connect to an IntelliRupter fault interrupter. The dongle can only be loaded with keys by the Security Key Manager, which also sets up the admin and user password to access the keys stored on the dongle.

The dongle contents are only accessible by the Security Key Manager and the LinkStart program; Windows Explorer and other applications cannot read or write to the dongle or view its contents.

The purpose of the admin password used in the Security Key Manager is to protect the contents of the dongle by making it accessible only to the administrator who initially configured the dongle. Another individual with an installation of the Security Key Manager will not be able to read the contents or write new contents to he dongle without this password. Should the admin password be lost, the only recourse is to reformat the dongle and erase it to the initial factory default state.

There are three options for security key deployment. The simplest is when keys are deployed using the common or master keys throughout the system. The second is to break the system into logical groups of devices called regions. The third is to use regions with crews to further control device access.

The Security Key Manager program expects to find both of the required key files present in the LinkStart folder and will use the private and public keys for the key names specified in the MasterKey.txt file created on the *Master Key Entry* screen. When the configuration file is exported by Security Key Manager, it should be transferred to the portable PC that will be used in the field to transfer the configuration file to specific IntelliRupter fault interrupters.

When the key names for the two master keys are IntelliRupter fault interrupter master key: "MasterIR" and mobile master key: "MasterLT," the Security Key Manager will require both the MasterIR.pri and MasterLT.pub files be present so it can include them in the configuration file. However, it will not expect the other files from these two pairs (MasterIR.pub and MasterLT.pri) to be in the LinkStart folder.

The file needed for configuring IntelliRupter fault interrupters to use security keys will have the extension ".wm" and will include either the individual serial number of the IntelliRupter fault interrupter or the universal serial number: install.00-0000000.wm, depending on the choice used when exporting from Security Key Manager. The files needed for any LinkStart program to connect to an IntelliRupter fault interrupter AFTER it has been loaded with the configuration file install.00-0000000.wm would be the files not included in the configuration files: MasterIR.pub and MasterLT.pri.

The portable PC used to upload the .wm Wi-Fi configuration file should have both the .wm file and the two separate key files. Any other portable PC that connects to the IntelliRupter fault interrupters after the configuration file has been uploaded will only need to have the two separate key files: MasterIR.pub and MasterLT.pri, with a master key deployment.

When using regions, or regions with crews, the requirements are similar, but the key pairs will differ depending on the key files assigned when setting up the regions or the regions with crews. The "Wi-Fi Security Key Administration" section on page 40 provides more information about the file relationships for each of the deployment options, and the workflow for deploying and removing keys.

The Security Key Generator provides an option to generate time-controlled and time-limited keys. Time-controlled keys can be created to only become active after a specified date, and they can be active indefinitely or for a limited time period after the activation date. Limited-life keys can be created that will only be valid for a set number of days after activation. They can be activated on the first use or on a predetermined start date.

Time-controlled keys can be used to control contractor access or to create automatic re-keying schemes that limit the number of visits to a device. The default key-length setting of 128 provides the best use of storage capacity, allowing approximately 50 key pairs to be stored in a device. The 256 setting provides a higher encryption level but will result in fewer keys stored—approximately 30 key pairs per device.

When using regions with crews, multiple time-controlled crew keys can be deployed, making it possible to have several years of time-limited keys deployed in a device, so new keys can be issued to the mobile computers on a periodic basis without having to visit each device in the field.

See S&C Instruction Sheet 766-523, "Wi-Fi and Security Administration," for additional information.

Before using the Security Key Manager program to assign keys to various devices, regions, and crews, the keys must be generated using the Security Key Generator. Figure 1 shows the default path to the folder where the keys will be written. The default folder for Windows 10/Windows 11 is \ProgramData\S&C Electric\LinkStart\.

A different folder can be manually selected by clicking on the **Select Save Folder** button. Both the Security Key Manager and the LinkStart program look in the default LinkStart folder for the keys and database files, so use of this folder is recommended.

S&C Electric Excellence Through Inno	Company ration	Security	Key	Generato Version 3.2.
Choose folder for the keys:	Or use this folder:			
Select Save Folder	C:\ProgramData\S&C Electric\LinkStart\			
Enter the Name for the key pair: MasterIR				
128 •				
Enter optional Time To Live in days:				
Enter optional Activation Date mm/dd/yyy	y			
NOW				
	5.0			

Figure 1. The Security Key Generator screen.

The two key-length options are 128 and 256. 128 is the default, which provides the best use of storage, allowing approximately 50 key pairs stored per device. The 256 setting provides a higher encryption level but will result in storing fewer keys—approximately 30 key pairs stored per device. To generate the keys needed as master keys, or region keys, first select the desired key length. Then, select two names—one key for the IntelliRupter fault interrupter and one for the PC computer.

In the Wi-Fi Security Key Administration section on page 40, "MasterIR" will be used as the device master key and "MasterII" will be used as the mobile master key. One of the region-key sets will be named "Region1IR" for the device pair and the other "Region1LT" for the mobile key pair.

Type one name into the Name field for the key pair and click on the **Make Key** button. Two keys will be generated with the same name, but each with a different extension. See Figure 2 on page 10.

S&C Electric Excellence Through Inno	Company	Security Key Generator Version 3.2.1.
hoose folder for the keys:	Or use this folder:	
Select Save Folder	C:\ProgramData\S&C Electric\LinkStart\	
nter the Name for the key pair:	Name' Masteri T	
elect the key length in bytes:	Name, manerer	
128 -	Size: 128 bytes, 1024 bits	
nter optional Time To Live in days:		
inter optional Activation Date mm/dd/yy	w	
	1 1	

Figure 2. Selecting key-length options and the key name.

Repeat this process for the second key name. When done, the four key files have been saved in the LinkStart folder, where the Security Key Manager program will look for them. When using two separate computers, move these files from the security PC to the Link-Start folder on the database PC.

NOTICE
Each generated key is unique. Therefore, a lost key cannot be replaced by re-entering that key name. A unique key will be generated the second time that same name is used, and the new key cannot be used to replace the first key.
When using regions with crews, select one name for each crew in addition to the two

When using regions with crews, select one name for each crew in addition to the two names selected for each region. See Figure 3.

Excellence Through Innov	ation	Security Key Generator Version 3.2.1:
hoose folder for the keys:	Or use this folder:	
Select Save Folder	C:\ProgramData\S&C Electric(LinkStart)	
nter the Name for the key pair:		
Crew1	Name: Crew1	
elect the key length in bytes:		
128 🔹	Size: 128 bytes, 1024 bits	
inter optional Time To Live in days:		
inter optional Activation Date mm/dd/yyyy	,	
Now		
Make Key	Exit	

Figure 3. Selecting a name for each crew.



After the keys are created, they will be stored in the \ProgramData\S&C Electric\Link-Start folder. See Figure 4.

Figure 4. The key files are stored in the LinkStart folder.

The Security Key Manager can create crew keys activated at first use. They will last for a set number of days or be valid only during a specific date range.

If only the **Activation Date** setpoint is entered, the key is valid after that date for an unlimited duration. If only the **Time to Live In Days** setpoint is entered, the key will be valid when the IntelliRupter fault interrupter first uses it for the number days specified. If both the **Activation Date** and the **Time to Live In Days** setpoints are configured, the key is only valid after that date for the number of days specified. If a timed key is not needed, leave these fields blank.

The Security Key Manager does not allow a limited-life key to be installed as a master key. It will allow regions or crews to use a single-time key pair. When a time key is used with a region keyset or a crew keyset that does not include a master keyset, the security keys revert back to the factory default key after the timed key expires.

Security Key Manager

Security Key Manager is a Windows software program intended for use by an IntelliRupter fault interrupter Wi-Fi system administrative user. The program is designed to create configuration files intended for upload to the IntelliRupter fault interrupter Wi-Fi module. It also generates a database file of IntelliRupter fault interrupters, regions, and crews Link-Start can use (LSDB.txt).

Keys can optionally be associated with IntelliRupter fault interrupters, regions, and crews. These keys are also incorporated into the configuration files. The administrative user can then disburse the configuration files, database file, and optional keys to the appropriate LinkStart users.

The Security Key Manager contains **Devices**, **Regions**, **Crews**, and **Wi-Fi Module Access Credentials** tabs. It also provides dongle support and includes many useful user interface features.

Regions provide a way to group IntelliRupter fault interrupters, and crews provide a way to group personnel. Wi-Fi module access credentials are the name and password pairs associated with an access level used when accessing the LinkStart *Wi-Fi Administration* screen. Dongle support allows exporting keys to a secure USB dongle. User-interface enhancements improve the user experience.

The Security Key Generator can create 128-byte or 256-byte keys. The Security Key Manager packages these keys into a configuration file. LinkStart and the Wi-Fi module firmware in the communication module use these keys to negotiate an authenticated session. LinkStart and the Wi-Fi module are able to use either 128-byte or 256-byte keys for authentication.

The screen in Figure 5 appears, overlaying the main *Security Key Manager* screen, and is the first time the Security Key Manager is run after installation. When the Provide for Master Key checkbox is checked and the **OK** button is clicked, the Security Key Manager program is configured to work with a pair of master key names to provide company-specific authentication security during the connection setup between a PC computer and an IntelliRupter fault interrupter. The selected options can be changed at any time by clicking on the **Options** button on the *Main* screen.

Provide for Master Key Provide for Regional Specific Keys Provide for Crew Specific Keys	
Provide for Regional Specific Keys Provide for Crew Specific Keys	
Provide for Crew Specific Keys	
Provide for WiFi Module Access Credentials	
Change Export Directory	
C:\ProgramData\S&C Electric\LinkStart\	

Figure 5. The Device Security Architecture Options screen.

Each checkbox represents its own tab on the *Main* screen of the Security Key Manager. Each of these options is explained later in this document. Figure 6 shows the main *Security Key Manager* screen displayed before the Provide for Master Key checkbox has been selected. Note the addition of the **Master Key** button on the screen in Figure 7, with text to the right of the button. Clicking on the **Options** button reopens the IntelliRupter Security Architecture Options dialog box and allows entering changes.

Security	y Key Manager			×
ile <u>E</u> dit	Iools			
S _s	S&C Electr Excellence Thro	ric Company ugh Innovation	Security Key	Manager Version 3.2.1.
Doubl	e-Click or Press E	inter to Edit		
Devi	Serial Number	Device Name	Device Location	
1 2	00-0000000	Universal	Universal Serial Number	
U		Find Record		
	1.1			
Opt	tions Decrypt	Files Export		
Ins	sert Dele	te Undelete Move	Up Move Down Save	Exit
-				

Figure 6. The Security Key Manager screen.

Devi	ccs Regions Crews	WiFi Module Access	1
1	Serial Number	Device Name	Device Location
2			
		Find Record	

Figure 7. The Security Key Manager screen with the Options button.

Enter Master Key Name

Click on the **Master Key** button on the main *Security Key Manager* screen. The Master Key Set dialog box opens. See Figure 8.

Master	YKey Set	
Device Master Key	Mobile Mast	er Key 📩
		ок



Select the two key names and click on the **OK** button. See Figure 9.

	Master	Key Set	
Device Master I MasterIR	Key T	Mobile Master H	Key •

Figure 9. Both names selected on the Master Key Set dialog box.

The names are now listed on the *Main* screen at the right of the **Master Key** button. See Figure 10.

e <u>E</u> dit	Iools		Contra	
5₅∕ ∕°C	S&C Electric	c Company In Innovation	Security Key Man Versio	age 1 3 2 1
Double	-Click or Press Ent	er to Edit		
Devic	Regions Crews	WiFi Module Access		
12	00-0000000	Universal	Universal Serial Number	
-		Fiel Decent		
Maste	Kau Mastan	Find Record		
maste	Waster	toy ook Masterin Masteri		
	ons Decrypt F	lles Export		
Opti				

Figure 10. The Security Key Manager screen showing the Master Key Set names.

Add IntelliRupter Fault Interrupters to the Database

The IntelliRupter fault interrupters can now be added to the database. If there is an existing database file named **MBL_DB.csv**, Microsoft Excel can be used to convert that database. See the "Excel File Examples" section on page 78 for the conversion procedure. The default file created when the program ran the first time has one record, the universal serial number, which can address any Wi-Fi module not connected to a control in an IntelliRupter fault interrupter.

To enter new information, first click on the **Insert** button to create a line for the new entry. This opens the Device Edit dialog box where the IntelliRupter fault interrupter information can be entered. If multiple entries exist in the database, the new line will be inserted below the line selected in the database list. See Figure 11.

Serial No	Device Name	Device Location
00-0000000	Universal	Universal Serial Number
08-0001234	IR1234	Ware House
	1 1	

Figure 11. The Device Edit dialog box.

As an alternative to the **Insert** button on the *Main* screen, use the <Insert> key on the keyboard or right click on a line and select "Insert Item" on the menu. See Figure 12.

S&C Electric	Company		Security Key	Mana Version
le-Click or Press Ent	er to Edit			
ces Regions Crews	WiFi Module Access			
Serial Number	Device Name	Device Location		
00-000000	Universal	Universal Seri	Edit Item Enter Insert Item Ins	
			Delete Item Del Undelete Backspace	
			Move Up Alt+Up Move Down Alt+Down	

Figure 12. Inserting an item directly on the Security Key Manager screen.

Click in each field to enter the information. When finished making entries, click the **Done** button to transfer the data to the *Main* screen on the next line. See Figure 13.

Secur	ity Key Manager		
le <u>E</u> d	lit <u>T</u> ools		
5 _{*(}	S&C Electric Excellence Throug	c Company	Security Key Manager Version 3.2.1.3
Dout	ble-Click or Press Ent	er to Edit	
	Serial Number	Device Name	Device Location
1	00-0000000	Universal	Universal Serial Number
2	(u) 08-0001234	IR1234	Ware House

Figure 13. A new item entered on the Main screen

Repeat this process to enter information for each IntelliRupter fault interrupter. Click on the **Insert** button and type information in the Device Edit dialog box for each new record added to the database. The Device Name entry must not contain spaces, but spaces are allowed in the **Device Location** field. To edit an existing entry, select it and double click on the entry line. This opens the Device Edit dialog box.

Data Entry with Notepad

The same data file can be created by using Notepad, and the entry will be saved as LSDB. txt in the LinkStart folder. When entering data, be sure to always end each line by clicking on the <Enter> key on the keyboard. It is also important after the last line of text to click on the <Enter> key on the keyboard. Failure to do this prevents recognition of the last line. See Figure 14.

Eile E	dit Format	<u>V</u> iew <u>H</u> elp		
00-00 08-00 08-00 08-00	00000 08734 08736 08737	Universal IRPC1005 IRPC1006 IRPC1007	Universal Serial Number First Cross after Johns Road MP27 Johns Road MP32 Jims Road at rail grade crossing	

Figure 14. Entering data with the Notepad screen.

The Security Key Manager also can load the text file when it is saved in the same folder as the key files in the LinkStart folder.

A file can be created or edited in Excel. Save that file using the tab delimited *.txt extension, and Excel adds tab character field delimiters. See the Excel File Examples in Figure 98 on page 78.

Depending on which options are enabled (i.e.: Regions, Crews, Wi-Fi Module Access credentials), the *Main* screen will have a row of tabs along the top to allow the user to change the view to that feature by clicking on a tab. See Figure 15.

Devi	Ices Regions Crews	WiFi Module Access	
-	Serial Number	Device Name	Device Location
3 4	(u) 08-0008736 (u) 08-0008737	IRPC1006 IRPC1007	Johns Road MP32 Jims Road at rail grade crossing
Mas Op	iter Key Master I ptions Decrypt Fi	Find Record Key Set: MasterIR MasterLT lles Export	

Figure 15. The feature tabs on the Main Security Key Manager screen.

Navigation

Tabbed List-Box Column Sort—The columns will sort when the column header is clicked on in *List View* screen. Clicking once sorts lowest value to highest, and clicking again sorts highest to lowest. The first column with the index numbers will reset the sort to the index order and only sorts from lowest to highest. The IntelliRupter fault interrupter list always anchors the "Universal Record" as the top item, regardless of the sort order.

Unassigned Record Indicator—A record that is unassigned will be preceded by "(u)" in the item's second column field. A record is considered unassigned when the **Regions** option is enabled and the IntelliRupter fault interrupter is not assigned to any region, or when the **Regions** and **Crews** options are enabled and a region is not assigned to any crew. These records can be easily found by typing the text "(u)" into the **Find Record** field. The "Universal Record" is never flagged as unassigned.

Dynamic Button State—Buttons that perform actions on records will display as active or disabled (grayed out and not selectable). The state is dynamically updated when various actions are performed. These dynamically updated buttons include:

Delete—Disabled when the "Universal Record" is selected or there are no items in the List View

Undelete—Disabled if no record has been deleted or a record has been restored

Move Up-Disabled if the topmost item is selected or when the List View is sorted

Move Down—Disabled if the "Universal Record" is selected, the bottommost item is selected, or when List View is sorted

Keyboard Shortcuts—Certain keystrokes perform operations on the Main List View(s). These keys include:

Up Arrow-Selects one record up

Down Arrow-Selects one record down

Right Arrow/Tab—Next List View tab

Left Arrow/SHIFT + Tab—Previous List View tab

ALT + Up Arrow-Moves the selected record up one row, if allowed

ALT + Down Arrow—Moves the selected record down one row, if allowed

Delete or Del—Deletes the selected record, if allowed

Backspace—Undeletes a record if one has been deleted

Space—Brings the selected record into view, if not visible

Enter-Edits the selected record

Tooltip Help—Certain buttons display help text when the mouse hovers over that button. These include:

Master Key	Undelete
Options	Move Up
Decrypt Files	Move Down
Export	Export (on the <i>Export</i> screen)
Insert	Extract (on the <i>Export</i> screen)
Delete	Delete File (on the <i>Decrypt</i> screen)

Context Menu—A context-sensitive popup menu of operations appears when a record is right-clicked. These operations mirror the button functionality found in the same screen. These operations include:

Edit Item	Insert Item
Delete Item	Undelete
Move Up	Move Down

Unsort List (return the view to a record number sorted state)

These popup menu items may be grayed out if the command is not valid for that record (the corresponding button is also grayed out). The popup menu is available for all tab views on the *Main* screen.

Copy/Paste Record (Edit Dialog)—The copy-and-paste buffer for the *Edit* screens only applies to the specific tab selected. For example, if an IntelliRupter fault interrupter record is copied, it cannot be pasted in a *Region Edit* screen. The **Paste Record** button remains grayed out if there is nothing stored in the copy-and-paste buffer.

Delete/Undelete Deleting a record with certain options enabled will cause changes that are not reversible with the **Undelete** command.

If the **Provide for Regional Specific Keys** option is checked and an IntelliRupter fault interrupter record associated with a region is deleted, that association is also removed. The record can be restored, but the association cannot be restored. If the user attempts to delete a record in this situation, the dialog box shown in Figure 16 will appear explaining the consequences.



Figure 16. A dialog box message that appears after a record-deletion attempt.

Clicking on the **Yes** button causes the record to be deleted and the association removed. If the **Region** and **Crew** options are enabled, then the same situation exists for a region record and the association that exists between it and one or more crews. A similar dialog will appear in this case. See Figure 17.



Figure 17. A dialog box that appears when a Region is in use by a Crew(s).

Using a Dongle

For extra security, a USB thumb drive, referred to as a "dongle," can be purchased to provide a secure container for the keys. This section describes dongle use.

The ability to inspect a dongle and clear its contents is provided on the *View Dongle* screen, which is accessed by the **View Dongle** button on the *Main* screen. This button is only shown if a dongle is installed when the Security Key Manager application is launched. See Figure 18.

ecurity Edit	y Key Manag t <u>I</u> ools	ger										×
5. C	S&C Excelle	Electri	ic Con Igh Innov	npany _{ration}			S	Securi	ity	Key	Manag Version 3.3	jer 2.1.2
Devi	ces Real	r Press En	iter to Ec	lit								
	Serial N	umber	Device	Name		Devic	e Location					
1 2 3 4	(u) 08-0000 (u) 08-00 08-0008 08-0008	000 108734 736 737	Univer IRPC10 IRPC10	sal 105 106 107		Unive First C Johns Jims f	rsal Serial N Cross after Ju Road MP32 Road at rail g	umber ohns Road grade cros	MP27 sing			
Mast Opt	ter Key	Master	Key Set Files	Find Reco : <not assign<br="">Export</not>	ned> <n View I</n 	ot Assign Dongle	ed>					•

Figure 18. Figure 18. The Main Security Key Manager screen.

Clicking on the **View Dongle** button opens the *View Dongle* screen. Clicking on the **Read Dongle** button opens the Enter Admin Password dialog box. Enter the password and click on the **OK** button to view the dongle contents. See Figure 19.

S&C Electric Co	ompany novation	Security	Key Manage
Double-Click or Press Enter to	Edit		-4613400-5.2.1
Devices Regions			
Enter Admin Password (SN:5) Enter Admin Password:	Dongle	1 MP2	7
	OK.		
-			
я.			
Read I	Dongle Format Dongle	Exit	
Read I	Dongle Format Dongle	Exit	
Read I Master Key Master Key S	Dongle Format Dongle Find Record Set: <not assigned=""> <not assigned<="" th=""><th>Exit</th><th></th></not></not>	Exit	
Read I Master Key Master Key S Options Decrypt Files	Dongle Format Dongle Find Record Set: Not Assigned> Not Assigned Export View Dongle	Exit	

Figure 19. The Password dialog box to view dongle contents.

Figure 20 shows an example of the View Dongle dialog box.

	View	v Dongle	
Serial Number: User Password: Private Keys: Public Keys: Number of Keys: Bytes Free:	5 irtUser1! dkCrew1 dkRegion1 2 48851		
۲		_	
ſ	Read Donale	Format Donale	Exit

Figure 20. The View Dongle dialog box.



Figure 21 shows the View Dongle dialog box when the dongle is blank.

Figure 21. The View Dongle dialog box when the dongle is blank.

Formatting a Dongle

Dongles do not have a default password. When a new dongle is first used it must be formatted. To format the dongle, open the View Dongle dialog box and click on the **Format Dongle** button. Click on the **OK** button on the Note dialog box. See Figure 22. When formatting is complete, the message "Dongle Format Success" displays in the View Dongle dialog box. The dongle is now ready to use.

Note	
Are you sure you want to Format this dongle?	[Cancel]
	ОК

Figure 22. The View Dongle Note dialog box.

Keying a Dongle

To place a set of keys in a dongle, select the keys and click on the **Export to Dongle** button. The Setup Password for Dongle dialog box opens if this is a newly formatted dongle. Otherwise, the Enter Admin Password dialog box opens. Enter the appropriate passwords and click on the **OK** button. See Figure 23.

When creating an Admin or User password, it must meet the following requirements:

- Minimum of eight characters in length, maximum of 11 characters
- Contains at least one uppercase letter (A-Z)
- Contains at least one lowercase letter (a-z)
- Contains at least one number (0-9)
- Contains at least one symbol (! @ # \$ % ^ & * () = _ +)
- No spaces between characters

e <u>E</u> dit <u>T</u> ools			_	_	_	_
S&C S&C	CELectric Co lence Through Inc	ompany novation		Se	ecurity Ke	y Manage Version 3.2
etup Passwords f	or Dongle	aine ne d	Detekanje f	iles		
Admin Password User Password			Cancel DK		1 MP27	
				- 1		
L						
Open Expo	rt Dir Export to	Dongle	Export	Exit		_
Open Expo	rt Dir Export to	Dongle	Export	Exit		
Open Expo Options	rt Dir Export to Decrypt Files	Dongle	Export View Dong	Exit		_

Figure 23. The Setup Passwords for Dongle dialog box.



After the dongle has been keyed, the Notice dialog box opens. Click on the **OK** button to proceed. See Figure 24.

Figure 24. The Notice dialog box.

Creating Regions and Crews

When the **Provide for Region Specific Keys** option is selected, the **Regions** tab will be available on the *Main* screen next to the **Device** tab. Click on the **Regions** tab and click on the **Insert** button on the *Security Key Managers Main* screen to open the Region Edit dialog box. See Figure 25.

Region Name	Region Edit	Devices in this Region S/N Eqpt ID	Unassigned Devices
Region1	Region1IR	08-0008736 IRPC1006 08-0008737 IRPC1007	08-0008734 IRPC1005
	Mobile Key		\longleftrightarrow
	Region1M	•	
Copy Record	Paste Record		ОК

Figure 25. The Region Edit dialog box.

Each IntelliRupter fault interrupter can be assigned to only one region, and when assigned it is no longer available for another region. After assigning a unique name to a region (spaces and special characters are not allowed, though the dash "-" and underline "_" characters are acceptable), choose two key pairs to allow connectivity and assign IntelliRupter fault interrupters to the region. The key pairs allow access to all IntelliRupter fault interrupters assigned to that region. An IntelliRupter fault interrupter is added to a region by selecting an item in the Unassigned Devices list and either double-clicking on that item or clicking on the **Double-Arrow** button. After being assigned to a region, it is removed from the Unassigned Devices list.

IntelliRupter fault interrupters can be removed from a region by selecting an item in the Devices in this Region list and either double-clicking on that item or clicking on the **Double-Arrow** button. When removed, it will be returned to the Unassigned Devices list.

If the **Provide for Crew Specific Keys** option is selected the **Crews** tab will be available on the *Main* screen next to the **Regions** tab. Click on the **Crews** tab and click the **Insert** button on the *Security Key Managers>Main* screen to open the Crew Edit dialog box. See Figure 26.

	Cre	w Edit		
Crew Name	Crew Key		Regions	Available Regions
Provid	[01		Regioni	Regionz
Crew/2	Crew?	<u> </u>		
Crew3	Crew3			<>
Course Descent	Paste Record			OK

Figure 26. The Crew Edit dialog box.

WAN Radio Configuration and Wi-Fi Access

A Wi-Fi configuration file generated by the Security Key Manager program contains the Wi-Fi settings and the authentication security key files. This file loads into the Wi-Fi module to configure security. A master key set uses only a single configuration file that is generated and loaded into every IntelliRupter fault interrupter. For a master key set, the configuration file should be generated from the universal serial number, and only the universal serial number settings need to be configuration file, based on that specific IntelliRupter serial number. If this approach is used, each device in the database will have a unique configuration file for each IntelliRupter fault interrupter is required and will automatically be generated through the export process.

The WAN radio serial port is used to connect to the WAN radio configuration port to allow setup and troubleshooting of the WAN radio through the Wi-Fi connection. To configure the WAN radio serial port settings and the Wi-Fi administrative passwords, select the IntelliRupter fault interrupter (or the universal serial number) on the *Security Key Manager Main* screen by double-clicking on it to open the Device Edit dialog box. See Figure 27.

		Device Edit
Serial No	Device Name	Device Location
00-0000000	Universal	Universal Serial Number
08-0008734	IRPC1005 IRPC1006	First Cross after Johns Road MP27 Johns Road MP32

Figure 27. The Device Edit dialog box.

Now, click on the **Settings** button to open the Wi-Fi Module Settings (Universal Record) dialog box. See Figure 28.

WiFi Modu	lle Settings (Univ	ersal Record)
Bits/Sec	Data Bits Parity 8 bit v none v	Stop Bits Flow Control
	WiFi User PV user	Module Passwords V Admin PW admin
		ОК

Figure 28. The Wi-Fi Module Settings (Universal Record) dialog box.

The **Bits/Sec** (baud rate), **Data Bits**, **Parity**, **Stop Bits**, and **Flow Control** settings for the selected device can be configured. Click on the **Down-Arrow** icon to display a list to select the value to change.

The user and admin passwords can also be changed here by clicking in the appropriate field and entering a password.

When finished, click on the **Save** button and on the **Exit** button. The settings are recorded in an .ini file and will now remain associated with this device. The universal serial number will have the .ini file **00-0000000.ini**.

When the **Provide for Wi-Fi Module Access Credentials** option is selected, the Wi-Fi module password settings will not be shown in the Wi-Fi Module Settings dialog box. See Figure 29.



Figure 29. The Wi-Fi Module Settings (Using Universal Record) dialog box.

Those settings will be entered in the Wi-Fi Module Access Credentials Edit dialog box. To open this dialog box, click on the Wi-Fi Module Access tab, and then click on the Insert button. See Figure 30.

Security Key Manager			
File Edit Tools			
5.2 S&C Electric Company	ıy	Security	Key Manager
Excellence Through Innovation			Version 3.2.1.1
Double-Click or Press Enter to Edit			
Devices Regions Crews WiFi Module	Access		
User Name	Password	Ac	cess
1 Admin	UseCapsNumbersS	Symbols!1 Ad	Imin
WiFi Module A	Access Credentials E	Edit	
User Name	Password	Access	
Admin	UseCapsNumbersSymbols!1	Admin	-
		,	
2			
Copy Record Paste Record		OK	
			_
Master Key Master Key Set: Mas	terIR MasterLT		
	()		
Options Decrypt Files Exp	ort		
Insert Delete Unde	elete Move Up Mov	ve Down S	Save Exit

Figure 30. The Wi-Fi Module Access Credentials Edit dialog box.

With this option, multiple passwords with an access level of either admin or user can be configured. Users only have the authority to configure the **WAN Radio Serial Port** setting.

User names can be 1-33 characters long, contain no spaces, and must be unique. When creating an admin or user password, it must meet the following requirements:

- Minimum of eight characters in length, maximum of 24 characters
- Contains at least one uppercase letter (A-Z)
- Contains at least one lowercase letter (a-z)
- Contains at least one number (0-9)
- Contains at least one symbol (! @ # \$ % ^ & * () = _ +)
- No spaces between characters

Exporting Configuration Files

The contents of the Export dialog box and the results of the export process depend on the options enabled. The dialog box shown in Figure 31 opens when only the **Provide for Master Key** option is selected.

To export master keys, click on the **Export** button on the *Security Key Manager Main* screen to open the Export Configuration and Database Files dialog box. To generate a universal configuration file from the universal serial number, select the universal serial number "00-0000000 Universal" and click on the **Export** button. This generates the master key configuration file in the LinkStart folder: install.00-0000000.wm.

	Jonnigu	il ation ai		ernes	
00-0000000	Universal	Universal Seri	al Number	07	
08-0008734	IRPC1005	Indus Road M	er Jonns Road MF 1932	21	
08-0008737	IRPC1007	Jims Road at r	rail grade crossing)	
Export	Confia	uration ar	nd Databas	e Files	
00-0000000	Universal	Universal Seri	ial Number		_
08-0008734	IRPC1005	First Cross aft	ter Johns Road MI	27	
08-0008736	IRPC1006	Johns Road M	IPJZ rail grade crossin		

Figure 31. The Export Configuration and Database Files dialog box.

To generate a unique configuration file for each IntelliRupter fault interrupter, select the serial numbers of the desired devices and click on the **Export** button. The following master key configuration files will be generated and placed in the *LinkStart* folder based on these selections:

install.08-0008734.wn

install.08-0008736.wn

install.08-0008737.wn

If the **Provide for Region Specific Keys** option is selected, the Export Configuration and Database Files dialog box displays the available regions for export. To generate configuration files for each region, select the region or regions to export and click on the **Export** button. If using the control key while selecting, a non-consecutive selection can be made. See Figure 32.

Region 1 Region3 Begion2		

Figure 32. Selecting non-consecutive entries.

If the **Provide for Crew Specific Keys** option is selected, the Export Configuration and Database Files dialog box displays the available crews for export. To generate configuration files for each crew, select the crew or crews to export and click on the **Export** button. Unlike master keys that export directly to the LinkStart folder, region keys and crew keys export to a subfolder under LinkStart that has the region or crew name. See Figure 33.

Organize 🕶 🔭 Open Play Inclu	de in library 🔻		Share with 🔻 😕	• ==	
🚺 My Music	^	Na	ame		Date
My Pictures		1	Crew1		9/4/
📓 My Videos		í.	Region1		9/4/
Joracle		1	Region2		9/4/
Saved Games	_	D	Temp		9/3/
Searches	E	E	image03.02.01.01.bin		7/23
		5] comport.ini		9/4/
Vorkspaces		ä	DBEdit.ini		9/4/
Performeter		P	Crew1.pub		9/3/
		P	MasterIR.pub		9/3/
DVD KW Drive (D:)	-	•	III		,

Figure 33. The LinkStart folder.

Decrypting a Configuration File

To view the contents of a configuration file that has the .wm file extension, click on the **Decrypt Files** button on the *Security Key Manager Main* screen to open the Config File Decryption dialog box. Click to select the name of the file to be viewed, and click on the **Decrypt File** button. See Figure 34.

The **Extract Files** button allows extracting a copy of the key files from the .wm Wi-Fi configuration file.

Select File To Decrypt	Decrypted File Contents	
install.08-0008734.wm	install.08-0008734.wm Size: 1504 Flags 00000001 Timestamp 09/04/2012 18:21:48 CRC calculated 4CF2C268 Match File 08-0008734.ini Size: 31 Ini: <admin 8<br="" 9600="" noradio="" user="">File Region1IR.pri Size: 993 File ShortTime.pub Size: 417</admin>	UTC es N 1 N>

Figure 34. The Config File Decryption dialog box.

Start the LinkStart program and select the IntelliRupter fault interrupter to be connected to. Scroll through the database by clicking on the **Prev** and **Next** buttons, or click on the **Clear** button, and enter text in the **Device Name** field to perform a dynamic search of the database. When the record is available in the drop-down list, click on it to select it.

WiFi Connection Management
File Edit Tools
S&C Electric Company Excellence Through Innovation LinkStart Version 3.2.2.1
Connect to a Device
Device Name: Universal Prev Next
Serial Number: 00-0000000 Clear
Connect Connection Progress
Belkin USB Wireless Adaptor

Then, click the **Connect** button. See Figure 35.

Figure 35. The Wi-Fi Connection Management dialog box.

After the connection is established, select the **Tools** option, click on **Wi-Fi Administration** option, and log in with an administrator password. See Figure 36.

💀 WiFi Connection Management				
File Edit Tools				
S _s C	IntelliLink Download Utility	LinkStart		
Connect to	WiFi Administration Ctrl+A Detailed Logging			
Device Name:				
Device Location:				
Serial Number: 08-9001020				
Disconnect IntelliLink Download Utility Connection Successful				
A18 Active Connection Channel 8		-50 dBm		

Figure 36. The Tools option and the Wi-Fi Administration selection.

	1	
WAN Port Settings		
WiFi Passwords]	
Transfer WiFi Settings	<- Update Available	
Reload WiFi Firmware]	
Transfer Security Logs]	
Device Status]	
Communications Counters	1	

When logged in, click on the **Transfer Wi-Fi Settings** button. See Figures 37 and 38.



WiFi Administration				
WiFi Configuration	n and Setup			
Transfer Encrypted WiFi S	Settings File			
Send File to WiFi Module:	Select and Send			
Get File from WiFi Module:	Get			
Apply 🔽 Ov	erride Base Memory at next power-on			
Settings File in WiFi Module: 0	1/01/1601 00:00 UTC 0×00000002			
Settings File available: install.00-0000000.wm				
ID: 09/09/2012 12:56 U	TC 0x00000001			
Get File from WiFi Module: Apply © Ov Settings File in WiFi Module: 0 Settings File available: install. ID: 09/09/2012 12:56 U	Get erride Base Memory at next power-on 11/01/1601 00:00 UTC 0x00000002 00-0000000.wm TC 0x00000001 Done			

Figure 38. The Wi-Fi Configuration Setup dialog box after clicking on the Transfer Wi-Fi Settings button.

Notice that **install.00-000000.wm** is displayed as the available file in this example. If the file displayed is correct, click on the **Select and Send** button to transfer the new configuration.

If the desired file is not displayed in the bottom left corner of this dialog box, and more than one file is available, hold-down the <Ctrl> key on the keyboard and click on the **Select and Send** button to open a file dialog box. Select the desired file and click on the **Open** button. The selected file will be sent to the Wi-Fi module.

The **Get** button is used to pull a copy of the existing settings file prior to uploading the new settings file. If selected, a file with the name install.XX-XXXXX.wd, where XX-XXXXXX = the serial number of the connected device, will be created in the directory containing the new settings file.

When working with a docking station, check the Override Base Memory at next power-on check box and click on the **Apply** button. This causes the security information to be written to the base memory module (BMM). If this box is not checked, the data in the BMM will overwrite the new configuration in the Wi-Fi module. The same is also true when transferring a communication module from an IntelliRupter fault interrupter with an updated BMM to one that does not have an updated BMM.

Click on the **Select and Send** button to upload this file to the IntelliRupter Wi-Fi module and base memory module.

Click on the **Done** button, and click on the **Log Out** button.

Uploading Wi-Fi Firmware

To upgrade the Wi-Fi module firmware, select the **Reload Wi-Fi Firmware** button on the *Wi-Fi Admin* screen. Then, click on the **Upload Wi-Fi Firmware** button to complete the process. See Figure 39.

WIFI Configuration and Setup	
Reload WiFi Firmware to WiFi Module	
Upload WiFi Firmware	
Existing Version 03.02.01.01	
Module Serial Number 00:40:9D:37:0B:38	
	Done

Figure 39. The Upload Wi-Fi Firmware button on the Wi-Fi Administration dialog box.

To download the Wi-Fi security log, select **Wi-Fi Security Log** on the *Wi-Fi Admin* screen. Then, click on the **Download Security Log** button to complete the process. See Figure 40.

WiFi Administration				
WiFi Configuration and Setup				
Transfer Security Log				
Get File from WiFi Module:	Download Security Log			
	Done			

Figure 40. The Download Security Log button on the Wi-Fi Administration dialog box.
Security Event Logs

The Wi-Fi module will post events to the security event log. The file resides on the Wi-Fi module. The LinkStart software will download these logs to a file named **Security-Log.<Serial Number>.<Date Time Stamp>.txt** for a user logged in with administrative access. The log maintains the last 400 security events, purging the oldest entry to make space for a new entry.

Commands will be added to the Wi-Fi module and Wi-Fi subsystem (WFM) to allow the MCU to request these logs. The Wi-Fi module automatically sends the security log to the MCU after a completed connection attempt, and the log will be sent 15 minutes after the connection was disconnected. This mechanism keeps the MCU copy of the security log up to date. The file on the MCU is stored in the CompactFlash file system (the file is: HISTLOG/SECURITY.LOG).

The security event descriptions are listed in Table 1 on page 38.

Security Event	Additional Data	Description
Init Security Log		No security log was present. A new log was started.
WM App Start Up	Firmware version	WM is starting up from a reboot or power cycle.
MCU Time Sync		WM has gotten the current time from the MCU for the first time since startup.
MCU WLAN Command	Wi-Fi Enabled/ Wi-Fi Disabled	MCU has sent a command to enable or disable Wi-Fi connectivity.
Connection Wake Up		WM has received a wake up SSID.
Connection Start		WM has established a physical Wi-Fi connection.
Connection End	Local/Remote	Connection has been terminated either remotely (by LinkStart) or locally (by WM).
Authenticate Start		Begin authenticating client (RSA packet received).
Authenticate Success	Hardware Keys/ Selected Keys	Client authentication successful.
Selected Key 1/2	Key Name	Name of selected keys used for connection estab- lishment.
Key Check	No valid keys found	During connection establishment the keys were found to be unusable (expired). The WM will switch to hardware keys.
Authenticate Fail	Reason	Client not able to authenticate (e.g. wrong key, wrong version, etc.).
User Mac Address	Mac Address	Mac address of client.
User Computer Name	Name	Computer name of client.
User Dongle SN	Serial Number	Serial number of dongle attached to client computer (optional).
User Name	Name	Windows login name of client.
User Hard Drive	Single Character	Hard drive the client is running LinkStart on.
User Hard Drive SN	Serial Number	Serial number of the drive client is running LinkStart on.
Alarm	Alarm Type	An alarm was generated (e.g. Replay Attack, Login Failed, Rescue Mode, Diagnostic Mode, Cleared).
Login Success	Name	Client logged in successfully.
Login Fail	Name	Client failed login attempt.
Configuration File Upload	Success/Fail	Configuration file was uploaded.
Configuration File Download		Configuration file was downloaded.
Firmware File Upload	Success/Fail	Firmware file was uploaded.
File Upload Failed	Sock Error	Firmware or configuration upload attempt timed out.
Reboot Requested		LinkStart has request the WM to reboot.
Rebooting		WFM is performing a soft reset.

Table 1. Security Event Log Entries

Wi-Fi Device Status

To see device status, click on **Wi-Fi Status** button on the *Wi-Fi Admin* screen. Then, click on the **Done** button to close the Device Status dialog box. See Figure 41.

WiFi Configuration	and Setup	
Device Status		
Derice blaids		
Date and Time:	9/10/2012 15:48:26 UTC	
Keep Alive Packets Sent:	749	
Keep Alive Packets Received:	3,629	
Module Session Retry Events:	0	
LinkStart Session Retry Events:	0	
Alarm State		
Replay Attack:	Inactive	
Login Failure:	Inactive	
		Done

Figure 41. The Device Status dialog box.

The Device Status dialog box automatically refreshes every 10 seconds and displays:

- MCU date and time
- Count of the transmitted and sent keep-alive packets
- Module session retry events
- LinkStart session retry events

Note: A retry event occurs when a DNP packet needs to be resent. It is incremented once for each packet that needs resending, not for each retransmitted packet. For example, packet 2 needs to be resent and took 5 retransmits to send it successfully, but the retry event is incremented only once for this packet. The module session represents Wi-Fi module retry events (WM sends to LinkStart), and the LinkStart session represents Link-Start retry events (LinkStart sends to WM). The retry event values are cleared at the start of each LinkStart connection attempt.

• Alarm state for a replay attack and a login failure (listing all alarms that are active or inactive)

Note: Replay attack prevention information is preserved on the IntelliRupter fault interrupter. The MCU stores and retrieves this information. This allows a Wi-Fi module to be changed, and the state of replay attacks will still be reserved. These data are requested by the Wi-Fi module from the MCU on startup and used to monitor for a replay attack. Each time a wakeup of the Wi-Fi module occurs, the replay attack file is sent to the MCU. The MCU stores this file on the compact flash file system as file: SETTINGS/REPLAY.DAT.

Communication Counters

To review Wi-Fi communication statistics, click on the **Communication Counters** button on the *Wi-Fi Admin* screen. Then, click the **Done** button to close the Communications Counters dialog box. See Figure 42.

WiFi Configuratio	n and Setup	
Communications Counter	s	
Configuration Changes:	1	
Module Up Time:	0 days 01:04:24	
WLAN Packets Sent:	3,858	
WLAN Packets Received:	12,730	
WAN Packets Sent:	0	
WAN Packets Received:	0	
Device Packets Sent:	1,338	
Device Packets Received:	1,331	

Figure 42. The Communications Counters dialog box.

The Communications Counters dialog box automatically refreshes every 10 seconds and displays:

- Count of configuration changes made directly through LinkStart software
- Count of the received and transmitted packets between LinkStart software and the Wi-Fi module (WLAN)
- Count of the received and transmitted packets between the Wi-Fi module and the device
- Count of the received and transmitted packets between the Wi-Fi module and the external radio (WAN)

Wi-Fi Module Reboot To reboot the Wi-Fi module, select the **Reboot Wi-Fi Module** option on the *Wi-Fi Admin* screen. Click on the **Yes** button to reboot or the **No** button to abort. See Figure 43.



Figure 43. The Reboot Wi-Fi Module dialog box.

WAN Port Settings

To change the WAN port settings, select the **WAN Port Settings** option on the *Wi-Fi Admin* screen. Use the list boxes to enter the desired changes and click the **Done** button to return to the previous screen.

The WAN port is a serial port that connects to the WAN radio configuration port in the IntelliRupter communication module to allow a serial connection from a configuration application on the PC to the WAN radio. See Figure 44.

	Config	urati	on a	nd Set	up	
WAN	Radio Se	rial Port	Setting	S		
	Bits per	Second	Data I	Bits	Parity	
	9600	-	8	*	none	-
	s	top Bits		Flow Co	ntrol	
	F	1	-	none	-	
						Apply
					_	
						Done
						Done

Figure 44. The WAN Radio Serial Port Settings dialog box.

Software Installation

This section describes the steps to create and deploy Wi-Fi security keys. Before starting, obtain two IntelliRupter fault interrupters or two IntelliRupter control modules with docking stations and communication modules. This also requires a USB flash drive and two computers, one for the security PC and one for the user PC.

Administrative permissions are required for both computers. A single computer with multiple profiles can also be used. The user PC needs a Wi-Fi adapter to communicate with the IntelliRupter fault interrupter control modules. Optionally, a security dongle is required to deploy the security keys on the user PC.

Install the Security Key Generator and the Security Key Manager software on the security PC. These programs can also be installed on separate PCs, which provides the most secure key management.

The Wi-Fi security programs are available in the S&C Automation Customer Support Portal. However, the security programs are only available to users registered as a security administrator. To register as a security administrator, contact your local S&C representative.

Next, install LinkStart software on the user PC. LinkStart software is included in the IntelliRupter software installer stored in the IntelliRupter Software workspace located on the S&C Automation Customer Support Portal. Installer version 3.5.0 or later is required. The **IntelliRupter Screensets**, **LinkStart**, and **Wi-Fi Module Firmware** options must be checked. See Figure 45.

S&C Electric IntelliRupter Installer 3.5.7		
IntelliRupter® Software	Installer	
Choose the items to install. Each item has its own installer.		
	Version(s) to be Installed	Version(s) Currently Installed
IntelliRupter Screenset and Applications	3.5.1	3.4.7, 2.3.3, 3.2.9, 1.3.18, 3.1.17, 1.7.6,
IntelliLINK and Update Utility	504.51	504.51
SpeedNet Radio Configuration Program	1.1.2.5	1.1.2.5
Curve Library	2.2	2.2
LinkStart (WiFi Connectivity)	3.2.1.1	3.1.6.1
ViFi Module Firmware	3.2.1.1	3.1.6.1
🔄 WaveWin	F.B.0.0	F.B.0.0
If any of the above items is already installed, then check and clicking Install will allow you to reinstall or uninstall th	ting its box he item.	
Select IntelliLINK for Other Products for S&C Automa Products other than IntelliRupter	ation	
IntelliLINK for Other Products	429	429
Some of the above installers install sample files to folders under t the user has only read access to files in those folders and needs below.	the Shared Documer write access, check	nts folder. If k the box
Copy Sample Files to Selected Folder (after	Install)	
Install Done		

Figure 45. The IntelliRupter Software Installer dialog box.

If necessary, upgrade the Wi-Fi module firmware to version 3.2.0.0 or later before proceeding.

On the USB flash drive, create four new folders named: stageone, stagetwo, stagethree, and stagefour.

Key Creation Use the Security Key Generator program to create the following keys:

MasterIR	[to be used as the device master key]
MasterLT	[to be used as the mobile master key]
Region1	[to be used as the device key for region1]
Region1M	[to be used as the mobile key for region1]
Crew1	[to be used as the crew key for the crew1]

Create each key by entering the names into the **Enter the Name for key pair**: field. The key length can be either 128 or 256. Do not configure any of the other options for these keys. See Figure 46.

Security Key G	enerator			
5 <u>-</u> C	S&C Electric Con Excellence Through Innovation	npany	Security Key	Generator Venim 32.1.1
Choose fold	er for the keys:	Or use this folder:		
	Select Save Folder	C:\ProgramData\S&C Electric\LinkStart\		
Enter the Na	me for the key pair:			
	ShortTime	Name: ShortTime		
Select the lo	ry length in bytes:			
	128 •	Size: 128 bytes, 1024 bits		
Enter option	al Time To Live in days:			
	3	Days active: 3		
Enter option	al Activation Date mm/dd/yyyy			
Now	9/3/2012	Works from 3 September 2012 through 5 S	eptember 2012	
		-		
	Make Key	Exit		
Key file	s: ShortTime.pub / ShortTime.pri			

Figure 46. The Security Key Generator dialog box.

Create a key with the name Crew2. Enter "1" in the **Enter optional Time To Live in days:** field before clicking on the **Make Key** button. Then, make a key with the name Crew3. Enter "1" in the **Enter optional Time To Live in days:** field and tomorrow's date in the **Enter optional Activation Date mm/dd/yyyy** field before clicking on the **Make Key** button.

When only the **Activation Date** field is entered, the key will be valid for an unlimited amount of time after the activation date. If only the **Time to Live in days:** field is filled in, the key is valid when it is first used by the IntelliRupter fault interrupter for the number days specified. If both the Activation Date and the **Time to Live in days:** setpoints are configured, the key will only be valid after that date for the number of days specified. The keys are saved in the LinkStart folder. For Windows 10/Windows 11 they are saved in the folder: \ProgramData\S&C Electric\LinkStart\. See Figure 47.



Figure 47. The LinkStart folder.

Security Key Manager

The first time the Security Key Manager is run after installation, the Device Security Architecture Options dialog opens. For this exercise, do not check any of the options, just click on the **OK** button to open the *Main* screen. See Figure 48.

Device Security Architectur	e Options
F Provide for Master Key	
Provide for Regional Specific Keys	
Provide for Crew Specific Keys	
Provide for WiFi Module Access Credential	5
Change Export Directory	
C:\ProgramData\S&C Electric\LinkStart\	
	OK

Figure 48. The Device Security Architecture Options dialog box.

If the program has already been run and options were selected, click on the **Options** button on the *Main* screen, uncheck all the checked options, and click on the **OK** button. See Figure 49. When the Security Key Manager is installed, the default record universal serial number is automatically created.

The universal serial number can be used to connect to a Wi-Fi module that is not connected to an IntelliRupter fault interrupter or a docking station, or to an IntelliRupter fault interrupter, or docking station that has the base memory module (BMM) removed. See Figure 49.

Eile	Security Edit	Key Manager								×
	5. °C	S&C Elec Excellence T	ctric hrough	Company Innovation			Secur	ity	Key	Manager Version 3.2.1.1
	Double	e-Click or Pres	ss Ente	r to Edit						
	Devid	es Regions (Crews	WiFi Module Acces	6					
		Serial Number		Device Name		Device Locati	on			
		00-0000000		Universar		oniversal set	nar number			
				Find Red	broc					•
				1.	1					
-	Opt	ions Dec	rypt Fil	Export						
	Ins	sert	Delete	Undelete	Move	Jp Move	e Down	Sav	/e	Exit

Figure 49. The Security Key Manager dialog box.

Right click on the universal serial number record. This opens a drop-down menu. The black items can be selected and the grey items are not available. See Figure 50.

uble	Click or Press Ent Regions Crews	er to Edit WiFi Module Access Device Name	Device Location	
	00-0000000	Universal	Universal Seri	Edit Item Enter Insert Item Ins
			_	Delete Item Del Undelete Backspace
				Move Up Alt+ Up Move Down Alt+Down
lacte	r Key Master I	Find Record	т	

Figure 50. This menu opens when the universal serial number line is selected.

Click on the **Insert Item** option, enter the serial number for the first device, and enter the device name (spaces are not allowed in the name) and the device location (spaces are allowed). Click on the **OK** button to complete the entry. See Figure 51.

Serial No	Device Name	Device Edit Device Location
00-0000000	Universal IDS1	Universal Serial Number Test Center Unit 1
07-1234006	IDS2	Test Center Unit 2
Copy Record	Paste Record	Settings

Figure 51. The Device Edit dialog box.

Repeat the process for the second device. This time, click on the **Settings** button and change the **Bits/Sec** setpoint to 115200 before clicking on the **OK** button. See Figure 52 on page 47.

Bits/Sec	Data Bits	Parity Stop	Bits Flow C	ontrol
9600	• 8 bit • n	one - 1 b	it - none	•
9600 14400 19200 38400 57600		WiFi Modu	ile Passwords	-
115200	-	User PW	Admin	PW

Figure 52. The WAN Radio Port Settings dialog box.

Exporting Configuration Files

Click on the **Export** button on the *Main* screen to open the Export Configuration and Database Files dialog box. Select all entries and click on the **Export** button.

Exporting without any options selected creates empty configuration files. Loading an empty configuration file into a Wi-Fi module removes any preexisting keys and causes the module to revert back to factory default keys. See Figure 53.

00-0000000 Universal Univers	sal Serial Number Unit 1	
07-1234006 IDS2 Test Center	Unit 2	_
		- 1
		-

Figure 53. The Export Configuration and Database Files dialog box.

The keys are automatically stored in the Export directory. Save these files in the stageone folder on the USB thumb drive for later use. The **Export** function automatically overwrites pre-existing files that have the same serial number or name. See Figure 54.



Figure 54. The LinkStart folder.

Click on the **Options** button on the *Main* screen, check the **Provide for Master Keys** option, and click on the **OK** button. The **Master Key** button is now shown in the bottom section of the *Main* screen with text at right. See Figure 55.

Securi	ity Key Manager			
e <u>E</u> di	it <u>T</u> ools			
5, ⁄°[S&C Electr	ric Company ugh Innovation	Security Key	Manage: Version 3.2.1.
Doub	ole-Click or Press E	nter to Edit		
Dev	Serial Number	Device Name	Device Location	
1 2	00-0000000 08-9001038	Universal IDS1	Universal Serial Number Test Center Unit 1	
3	07-1234006	IDS2	Test Center Unit 2	
-				
		Find Pacand		
Mas	ster Key Maste	r Key Set: <not assigned=""> <no< td=""><td>ot Assigned></td><td></td></no<></not>	ot Assigned>	
Op	ptions Decrypt	Files Export		
				-
1.1		11 11 11 11 11 11 11 11 11 11 11 11 11		

Figure 55. The Security Key Manager Main screen.

Click on the **Master Key** button, select the **MasterIR** option as the **Device Master Key** setting and the **MasterLT** option as the **Mobile Master Key** setting. Click on the **OK** button. See Figure 56.

IVIGSUE	
Device Master Key MasterIR 💽	Mobile Master Key MasterLT

Figure 56. The Master Key Set dialog box.

The key names now appear on the *Main* screen next to the **Master Key** button. See Figure 57.

Devi	le-Click or Press Er	nter to Edit		
	Serial Number	Device Name	Device Location	
1	00-0000000	Universal	Universal Serial Number	
2	08-9001038	IDS1	Test Center Unit 1	
		Find Record		
Mast	ter Key Master	Key Set: MasteriR MasterL	r	

Figure 57. Key names shown displayed next to the Master Key button.

Click on the ${\bf Options}$ button, check the Provide for Regional Specific Keys check box, and click on the ${\bf OK}$ button.

	Then, click or	n the Regions tal	o followed by the	Insert button	on the Main	screen. S	see
Figu	re 58.						

Edit Iools	yu.		_				
C S&C	Electric Co	ompany iovation			Security	7 Key	Manage Version 3.2.1
ouble-Click o	r Press Enter to	Edit					
Devices Reg Region	ions Name	Devie	e Key	,	dobile Key		
		Find Re	cord				
Master Key	Master Key S	et: MasteriR	MasterLT				
Options	Decrypt Files	Export	1				
1	Delate	11-1-1-1-				0	5.4
Insert	Delete	Undelete	Move Up	Movel	Jown	Save	Exit

Figure 58. The Security Key Manager Main screen.

IntelliRupter fault interrupters can be added to a region by selecting a device in the Unassigned Devices list and by clicking on the **Double-Arrow** button. Select one IntelliRupter fault interrupter for Region 1. Then, enter "Region1" in the **Region Name** field, select the **Region1IR** option for the **Device Key** field, select the **Region1M** option for the **Mobile Key** field, and click on the **OK** button. This completes the creation of Region1. Repeat the process to create Region2. See Figure 59.

D	Region Ed	it	Devices in this Region		Unarrighted Devices
Region Name	Device Key	0	18-9001038 IDS1		07-1234006 IDS2
Region1	Region1IR	•			
	Mobile Key			$\langle - \rangle$	
	Region1M	•			
Conv Record	Paste Recard				OK

Figure 59. The Region Edit dialog box.

After entering the regions, click on the **Export** button on the *Main* screen, select both regions, and click on the **Export** button on the Export Configuration and Database Files dialog box. A folder is created in the ProgramData>S&C Electric>LinkStart folder for each selected region.

Each folder contains the key pairs needed for a mobile device to connect to that region's IntelliRupter fault interrupters, a new **LSDB.txt** database file, and a Wi-Fi configuration file for each IntelliRupter fault interrupter in the region. The configuration files each contain an IntelliRupter fault interrupter serial number in the file name. See Figure 60.

Export Configuration a	and Database Files		
Region1 Region2			
🚱 🔵 🚽 « Default (C:) 🕨 ProgramDa	sta 🔸 S&C Electric 🔸 LinkStart 🔸 📼 🍫 Search LinkSta	nt.	
Organize 🕶 🎇 Open Play Ind	clude in library ▼ Share with ▼ Burn New folder	III • 🚺	
3 DRAWINGS-Visio	^ Name	Date modified	
	🔒 Region1	9/11/2012 9:55 AM	ľ
Deckton			
Desktop	💷 🎍 Region2	9/11/2012 9:55 AM	
C C C C C C C C C C C C C C C C C C C	tric + LinkStart + Region1 + 47 Search Region.	9/11/2012 9:55 AM	
Corganize ▼ Include in library ▼ Sh	tric → LinkStart → Region1	9/11/2012 9:55 AM	
Crganize Include in library Sh Crganize Sh	tric > LinkStart > Region1 - + +> Search Region. hare with - Play all Burn New folder Name install.08-9001038.wm	9/11/2012 9:55 AM	
Crganize Include in library SkiC Elect Organize Corganize SkiC Elect Organize SkiC Elect SkiC Elect Organize SkiC Elect SkiC Ele	tric → LinkStart → Region1	9/11/2012 9:55 AM	
Crganize ▼ Include in library ▼ Sh Crganize ▼ Include in library ▼ Sh Cracle Saved Games Searches Tracing	tric → LinkStart → Region1	9/11/2012 9:55 AM	
Corganize	tric > LinkStart > Region1 - 47 Search Region hare with - Play all Burn New folder Name install.08-9001038.wm LSDB.txt Region1IR.pub Region1M.pri	9/11/2012 9:55 AM Date modified 9/11/2012 9:55 AM 9/10/2012 6:12 PM 9/3/2012 11:11 AM 9/3/2012 11:11 AM	
Corganize	tric → LinkStart → Region1	9/11/2012 9:55 AM Date modified 9/11/2012 9:55 AM 9/10/2012 6:12 PM 9/3/2012 11:11 AM 9/3/2012 11:11 AM	

Figure 60. The LinkStart>Region1 folder contents.

Save each of the region folders to the stagetwo folder on the USB thumb drive.

When the Region1 configuration file: install.08-9001038.wm is decrypted, notice the Region1 folder only contains the Region1 key files **Region1IR.pub** and **Region1M.pri**, and the configuration file also contains the master key pair. To create an administrative PC, copy the MasterIR.pub and **MasterIT.pri** key files and the LSDB.txt database file to the LinkStart folder of the target PC. See Figure 61.

Select File To Decrypt	Decrypted File Contents	
install.08-9001038.wm	install.08:9001038.wm Size: 3808 Flags 00000001 Timestamp 09/11/2012 16:41:03 UTC CRC calculated 13E34A73 Matches File 08:9001038.ini Size: 31 Ini: <admin 1="" 8="" 9600="" n="" noradio="" user=""> File MasterIR.pri Size: 992 File MasterL.T.pub Size: 416 File RegionIIR.pri Size: 993 File Crew1.pub Size: 413 File Crew2.pub Size: 413</admin>	

Figure 61. The Config File Decryption dialog box.

Click on the **Options** button on the *Main* screen and check the **Provide for Crew Specific Keys** check box. Leave the Provide for Master Key and Provide for Regional Specific Keys check boxes checked as well, and click on the **OK** button. Click the **Crews** tab on the *Security Key Manager Main* screen, and click on the **Insert** button on the *Main* screen to open the Crew Edit dialog box. See Figure 62.

Create four crews, and name them Crew1, Crew2, Crew3, and AdminCrew. Match them with their identically named keys that were created earlier.

For the AdminCrew, select "<MasterKey>" for the **Crew Key** field. Assign Region1 to Crew1, Region2 to Crew2, and Region1 and Region2 to Crew3.

Remember, Crew2 will only work for one day after it is first activated, and Crew3 will only work tomorrow. The MasterCrew does not get regions assigned to it because it automatically gains access to all IntelliRupter fault interrupters through the master keys. See Figure 62 on page 53.

Crew Name	Crew Key		
1 Crew1	Crew1		
2 Crew2	Crew2		
4 MasterCrew	<masterkey< td=""><td>></td><td></td></masterkey<>	>	
			the second s
	Crew E	dit	
rew Name	Crew Key	Regions	Available Regions
		Region1	Region2
real	Crew1	-	
You/	Crow?		
rew3	Crew3		
			<->
			a de la companya de la
	Crew E	dit	
rew Name	Crew Key	Regions	Available Regions
rew2	Crew2		Region1 Region2
(asterCrew)	(MasterKey)		regione
	(musiciney)		
			$\langle \rightarrow \rangle$

Figure 62. The Crew Edit dialog box.

When crew assignment is completed, click on the **Export** button on the *Main* screen, select all crews, and click on the **Export** button on the Export Configuration and Database Files dialog box to create the crew files.

Configuration files incorporating the master keys, the regions, the crews, and the corresponding crew keys will be saved in the LinkStart folder. These files will be saved with the corresponding keys for each crew in a folder with the same name as the crew. Save these folders in the stagethree folder in the thumb drive. See Figure 63.

	and the second se	
Export Configuration and	Database Files	
Crew1		
Crew2		
Crew3 MasterCrew		
🌀 🔵 😼 « ProgramData 🕨 S&C Electric 🕨 Links	itart 🕨 🗸 🎸	• Search LinkStart
Organize 🔻 😰 Open 🔻 Burn New folder		8≣ ▼ 🛄 🔞
闥 My Videos	 Name 	Date modified
🔊 NetHood	Crew1	9/11/2012 11:41 AM
🎉 Oracle	L Crew2	9/11/2012 11:41 AM
PrintHood	Crew3	9/11/2012 11:41 AM
Recent	MasterCrew	9/11/2012 11:41 AM
🔊 SendTo	 Name 	^ Date modified
A C		·
Start Menu		out mountain
Templates	Crew1.pri	9/3/2012 12:31 PM
3 Tracing	Install.08-9001038.	.wm 9/11/2012 11:41 Al
📙 Workspaces	LSUB.btt	9/10/2012 0:12 PM
Computer	regionatic.pub	3/3/2012 11:11 AIV
🕽 🔵 🗢 🕌 « S&C Electric 🕨 LinkStart 🕨 MasterCro	w • 4	Search MasterCrew
Organize ▼ Include in library ▼ Share with ▼	w	> Search MasterCrew
Organize ▼ Include in library ▼ Share with ▼ isonation	w v folder	Search MasterCrew Search MasterCrew
Organize ▼ Include in library ▼ Share with ▼ SendTo Start Menu	w - 43 Burn New folder Name R install.07-1234006.	Search MasterCrew
Organize ▼ Include in library ▼ Share with ▼ SendTo Start Menu Templates	w	Search MasterCrew SEarch MasterCrew Date modified wm 9/11/2012 11:41 Al wm 9/11/2012 11:41 Al
Organize ▼ Include in library ▼ Share with ▼ SendTo Start Menu Templates Tracing	w v v v 43 Burn New folder Name Binstall.07-1234006. Binstall.08-9001038. LSDB.bt	Search MasterCrew SEarch MasterCrew Date modified wm 9/11/2012 11:41 Al wm 9/11/2012 11:41 Al 9/10/2012 6:12 PM
Organize ▼ Include in library ▼ Share with ▼ SendTo Start Menu Templates Tracing Workspaces	w v v v solution Burn New folder Name Binstall.07-1234006. Binstall.08-9001038. LSDB.btt Binstall.08-9001038. LSDB.btt	Search MasterCrew
	w v v v solution Burn New folder Name Binstall.07-1234006. Binstall.08-9001038. LSDB.btt BiMaster/R.pub Master/L.pri	Search MasterCrew Search MasterCrew Date modified wm 9/11/2012 11:41 AF 9/10/2012 16:12 PM 9/3/2012 10:48 AM 9/3/2012 10:48 AM 9/3/2012 12:50 PM
Image: Start of the start	w v v v solder Burn New folder Name Pinstall.07-1234006. Pinstall.08-9001038. LSDB.btt Pinstall.08-9001038. LSDB.btt Pinstall.08-9001038. MasterIR.pub	Search MasterCrew

Figure 63. The expanded LinkStart folder.

The Master Crew folder contains all of the configuration files, while the crew folders only contain the IntelliRupter fault interrupters from the region the crew is assigned to. Also notice the difference in keys contained in the Crew1 folder compared to the Master-Crew folder.

Click on the **Options** button on the *Main* screen and check the Wi-Fi Module Access Credentials check box. Leave the Provide for Master Key, Provide for Regional Specific Keys, and Provide for Crew Specific Keys check boxes checked.

When a Wi-Fi module access credential is created, the credential password requires a minimum strength. An acceptable password meets the following requirements:

- Minimum of eight characters in length, maximum of 24 characters
- Contains at least one uppercase letter (A-Z)
- Contains at least one lowercase letter (a-z)
- Contains at least one number (0-9)
- Contains at least one symbol (! @ # \$ % ^ & * () = _ +)
- No spaces between characters

User and admin names can be 1-33 characters long, containing no spaces, and must be unique.

The access level for an entry has two options: Admin or User.

A Wi-Fi module access credential is a name and password pair used for logging in to the *Wi-Fi Administrative* screen of the LinkStart software. Create the user name, password, and access combinations shown below.

With the **Wi-Fi Module Access** tab selected in the *Main* screen, click on the **Insert** button to open the Wi-Fi Module Access Credentials Edit dialog box and create three users. Name the first "Admin," and give it the password "irtAdmin1" and the access level "Admin." Name the second and third "User1" and "User2." Set the passwords as "irtUser1" and "irtUser2." Set the access level "User" for each. See Figure 64 on page 56.

Dev	vices Regions Crews WiFi Moo	lule Access		1	-
	User Name	Password		Access	_
2	User1	intAdmin !!		User	
3	User2	irtUser2!		User	
Adr	min	irtAdmin1!	Admin	•	
Use	er1	irtUser1I	User		
Coj	py Record Paste Record			ок	

Figure 64. The Wi-Fi Module Access Credentials Edit dialog box.

Click on the **Devices** tab and select a device. This opens the Device Edit dialog box. Click on the **Settings** button to open the Wi-Fi Module Settings (Custom Settings) dialog box. Note the **Wi-Fi Module Passwords** option is no longer available on the Wi-Fi Module Settings (Custom Settings) dialog box. See Figure 65.

S&C Excelle	Electric	h Innovation	Security Key Manag Version 3.2
Double-Click o	r Press Ent	er to Edit WiFi Module Access	
Serial N	lumber	Device Name	Device Location
2 08-9001	038	IDS1	Test Center Unit 1
3 07-1234	006	IDS2	Test Center Unit 2
08-9001038	IDS1	Bits/Sec	Data Bits Parity Stop Bits Flow Control v 8 bit v none 1 bit v none v
07-1234006			
Copy Record	Paste R	con	
Copy Record	Paste Re	corr	
Copy Record Master Key Options	Paste R Master r Decrypt Fi	corr cey 1	

Figure 65. The Wi-Fi Module Settings (Custom Settings) dialog box.

Decrypt the Crew1 configuration file named install.08-9001038.wm. It should be in the stagethree folder. If it isn't there, make sure to save a copy there before proceeding. Look at the line beginning with "Ini:" and note the first line below it contains file "MasterIR.pri Size:992." See Figure 66.

elect File To Decrypt	Decrypted File Contents	
nstall.08-9001038.wm	install.08-9001038.wm Size: 2880 Flags 00000001 Timestamp 08/11/2012 18:38:14 UTC CRC calculated 66F9DA23 Matches File 08-9001038.ini Size: 33 Ini: <admin 1="" 115200="" 8="" n="" noradio="" user=""> File password.pw Size: 58 File MasterLT.pub Size: 416 File Region1IR.pri Size: 933 File Crew1.pub Size: 413 File Crew2.pub Size: 413</admin>	E

Figure 66. The Config File Decryption dialog box.

Click on the **Export** button on the *Main* screen, select all the available crews, and click on the **Export** button on the Export Configuration and Database Files dialog box. The configuration file install.08-9001038.wm in the Crew1 folder has now been overwritten.

Decrypt the configuration file again and notice the first file below the line beginning with "Ini:" now contains "File password.pw Size 58." The password.pw file contains credentials created in the **Wi-Fi Module Access** tab. Folders Crew1, Crew2, Crew3, and MasterCrew have been overwritten or recreated with the new password.pw file added to each. Save these folders to the stagefour folder on the USB dongle. See Figure 67.

elect File To Decrypt	Decrypted File Contents	
install.08-9001038.wm	install.08-9001038.wm Size: 2880 Flags 00000001 Timestamp 09/11/2012 18:38:14 UTC CRC calculated 66F9DA23 Matches File 08-9001038.ini Size: 33 Ini: <admin 1="" 115200="" 8="" n="" noradio="" user=""> File password.pw Size: 58 File MasterLT.pub Size: 416 File Region1IR.pri Size: 993 File Crew1.pub Size: 413 File Crew2.pub Size: 413</admin>	* ×

Figure 67. The Config File Decryption dialog box.

USB Dongle

When using a USB dongle, close the Security Key Manager program and plug the dongle into a USB port. Restart the Security Key Manager program and notice the *Main* screen now has a **View Dongle** button.

Click on the **View Dongle** button to open the dialog box. Click on the **Read Dongle** button. If the dongle is empty and ready for use, the message shown in Figure 68 opens. If prompted for a password instead, the dongle already contains data. Reformatting the dongle erases its contents and passwords, making it available for new data. See Figure 68 on page 59.

Security	Key Mana	ger					×
e <u>E</u> dit	Tools						
5, ⁄°C	S&C Excelle	Electric Con ance Through Inno	mpany _{vation}		Security	Key	Manager Version 3.2.1.2
Doubl	e-Click c	or Press Enter to E	dit				
Devie	ces Reg	ions Crews WiFi	Module Access				
	Serial						
1	00-00						
2	08-90		Viev	v Dongle			
3	07-12			Ū			
		Dongle (SN:5) contains no data				
-							
		4			,		
				100	-	-	
			Read Dongle	Format Dongle	Exit		
				J			
	C		Fille Hocore				× -
Mast	er Key	Master Key Se	t: MasterIR Master	LT			
8							
Opt	ions	Decrypt Files	Export	v Dongle			

Figure 68. The View Dongle dialog box.

Close any open dialog boxes and click on the **Export** button on the *Main* screen. The Export Configuration and Database Files dialog box now has an **Export to Dongle** button. Click on the **Export to Dongle** button and a prompt opens to create an admin password and user password. The dongle has the same password requirements as the Wi-Fi Module Access credentials. For this example, use "irtAdmin1!" for the admin password and "irtUser1!" for the user password. Enter the passwords and click on the **OK** button to complete the export. See Figure 69.

un Passwords fr	or Donale		
dmin Password:	ittAdmin1!	Cancel	
ser Password:	irtUser1!	ок	

Figure 69. The Setup Passwords for Dongle dialog box.

Exit the Export Configuration and Database Files dialog box, and click on the **View Dongle** button on the *Main* screen. Enter the admin password "irtAdmin1!," when prompted, and the contents of the dongle will be displayed. See Figure 70.

	View Dongle	
Serial Number: User Password: Private Keys: Public Keys: Number of Keys: Bytes Free:	5 irtUser1! Crew1 Region1IR 2 48853	
*		F.

Figure 70. The View Dongle dialog box.

When a dongle is connected to the user PC and LinkStart software is first started, the Enter Password to Access Dongle dialog box opens. See Figure 71. Without the correct user password, LinkStart software cannot connect to an IntelliRupter fault interrupter that has been encrypted with the keys in the dongle.

WiFi Connection Management	
Enter Password to Access Dongle	
Enter User Password:	LinkStart Version 3.2.2.1
Connect to a Device	= = =
Device Name: Device Location: Serial Number: 08-9001020	
Cancel Connection Progree	55
Making WiFi Connection	

Figure 71. The Enter Password to Access Dongle dialog box.

Now that the configuration files, corresponding keys, and the dongle are set up, Intelli-Rupter fault interrupters can be connected through the LinkStart program. To use the keys, Wi-Fi firmware version 03.02.01.01 or later must be installed in the Wi-Fi module. If this hasn't been done, connect to the IntelliRupter fault interrupter and update the Wi-Fi module firmware. Review the "Uploading Wi-Fi Firmware" section on page 36 before proceeding.

An administrative login is required to transfer keys from the USB thumb drive to the user PC. After transferring the files, log in as a user before connecting to the IntelliRupter fault interrupter. Be sure when sending a configuration file to the IntelliRupter fault interrupter it has a matching serial number. For example, when connecting to ISD1 with serial number 08-9001038, the configuration file should be install.08-9001038.wm.

Re-keying an IntelliRupter fault interrupter implies the keys are already installed and a new WM configuration will be uploaded that contains different keys. The present keys, the new keys, and the new configuration file all need to be in the default LinkStart folder before connecting to the LinkStart program.

First, connect to the LinkStart program with the present keys. Then, select "Tools," click on the **Wi-Fi Administration** option, and log in with an admin access-level username and password. Then, click on the **Transfer Wi-Fi Settings** button and send the new configuration file. Subsequently delete the old keys from the LinkStart folder, disconnect from the IntelliRupter fault interrupter, and reconnect using the new keys. This verifies the configuration file was successfully installed and the new keys work.

NOTICE

Be careful when deleting keys. Always make sure they are backed up somewhere before proceeding. If the keys in a module are lost, the Wi-Fi module cannot be accessed, and it must be returned it to the factory to be reset to the factory default settings.

Paste the files in the Region1 folder in the stagetwo folder on the USB thumb drive into the LinkStart folder on the user PC. The default directory for LinkStart files is \Program-Data\S&C Electric\LinkStart. This directory is a hidden directory. It is necessary to use the **Folder Options>View>Show hidden files and folders** command to see the content. Press the <Alt> key to expose the tool bar and select the **Tools>Folder options...** option. See Figure 72 on page 62.



Figure 72. The Folder Options dialog box.

There are two key files named Region1. The file Region1.pub represents half of the device key pair, and the file Region1M.pri represents the other half of the mobile key pair. See Figure 73.

		0++ * LB
Recent Saved Games Saved Games Searches SendTo Sant Menu Tracing Workspaces	Name Region1.pub Region1M.pri RistalL08-9001038.wm LSD8.txt	Date modified 8/21/2012 4:58 F 8/21/2012 4:53 F 8/21/2012 5:31 F 8/21/2012 4:36 F
Tracing Vorkspaces	- 12 -	

Figure 73. The Wi-Fi Key Generator screen.

When the files have been transferred, log in as a user and launch the LinkStart program. If the first IntelliRupter fault interrupter has no keys installed in it, click on the **Connect** button on the *LinkStart* screen. If it does have associated keys, make sure those keys are in the LinkStart folder before starting the LinkStart program.

Using LinkStart Follow these steps to connect to the first IntelliRupter fault interrupter by launching the LinkStart program:

STEP 1. Sselect the **Tools** tab, and click on the **Wi-Fi Administration** option on the *LinkStart Main* screen. See Figure 74.

🔀 WiFi Conned	ction Management	
File Edit To	ols	
S _s C	IntelliLink Download Utility	LinkStart
	WiFi Administration Ctrl+A	Version 3.2.2.1
Connect to	Detailed Logging	
Device Nan	ne:	
Device Locatio	on:	
Serial Numb	er: 08-9001020	
Disc	connect IntelliLink Do	wnload Utility
-	Connection out	
A18 Active Co	nnection Channel 8	-50 dBm

Figure 74. The LinkStart Main screen.

STEP 2. If the LinkStart program was started by clicking on the IntelliLink button, cancel the IntelliLink login request and select the File>Exit option. Then, click on the Leave Connected button to access the LinkStart Main screen. See Figure 75.

	S&C IntelliLINK®. WiFi Connection
S&C IntelliLINK® Remote Setup Software - Setup, Operating, and Troubles	IntelliLINK will now close.
File Connection Tools Help	What would you like to do about the WiFi connection?
Exit Alt+F4	Disable WiFi Access Disconnect Leave Connected Cancel

Figure 75. The IntelliLink will now close dialog box.

STEP 3. Select the **Tools** tab and click on the **Wi-Fi Administration** entry to open the *Wi-Fi Administration* screen. If the device has not been keyed, use the factory default password. Then, click on the **Transfer Wi-Fi Settings** button. See Figure 76.

WiFi Administration	WiFi Administration
WiFi Configuration and Setup	WiFi Configuration and Setup
WAN Port Settings WiFi Passwords Transfer WiFi Settings Reload WiFi Firmware Transfer Security Logs Device Status Communications Counters Log Out	Transfer Encrypted WiFi Settings File Send File to WiFi Module: Send Get File from WiFi Module: Get Apply Override Base Memory at next power-on Settings File in WiFi Module: 09/09/2012 No Settings File available. Done

Figure 76. The Transfer Encrypted Wi-Fi Settings File dialog box.

- **STEP 4.** In the bottom left corner of the screen it should display "Settings File available." Click on the **Send** button. If it does not say "Settings File available," holding down the <Ctrl> key on the keyboard and the **Send** button simultaneously will change to "Select and Send."
- **STEP 5.** Click on the **Select and Send** button and browse to the required configuration file. For the example shown in Figure 77, the file is install.08-901038.wm. Select the file and click the **Open** button to begin the transfer. The control key only changes the **Send** button to "Select and Send" if there are multiple firmware files in the active LinkStart directory. See Figure 77.

WiFi Administration				
WiFi Configuration and Setup				
Transfer Encrypted WiFi Settings File Send File to WiFi Module: Select and Send Get File from WiFi Module: Get Apply Choose a Configuration File	1			X
Settings File in WiFi Modul 🚱 🔵 🕨 « USB (E:	:) ▶ WiFi-Keys ▶ stagetwo ▶	Region1	 Search Region1 	٦
No Settings File available. Organize - New fo	lder)ii • 🗍	0
Start Menu S	k)	Name	Date modified 8/21/2012 5:31 PM	Ty W
⊊ drawingfiles (\\c File	hicago.sandc.ws) (H:) 🚽	« [Config files Qpen Cancel	•

Figure 77. The Transfer Encrypted Wi-Fi Settings File dialog box.

- **STEP 6.** Now, exit the LinkStart program and delete any other files except the ones copied from the Region1 folder. Reconnect to the first IntelliRupter fault interrupter. Click on the **IntelliLink** button and log in to verify proper operation.
- **STEP 7.** Save a snapshot by clicking on the **File** menu and then on the **Save Snapshot** entry. Then, click on the **Tools>Compact Flash Access...** entry and download an event log. These helpful files are for diagnostic purposes or for restoring the settings in a control.
- **STEP 8.** Disconnect and exit the LinkStart program.
- **STEP 9.** Use a second PC and try to connect to the first IntelliRupter fault interrupter with Region2 keys from the stagetwo folder. The LinkStart program should not connect. If a second PC is not available, hide the Region 1 keys in a temp folder and install the Region 2 keys.
- STEP 10. Go to \Users\Public\Documents\S&C Electric\LinkStart for Windows 10/ Windows 11 and open the Wi-Fi log file with the most recent date. Note the statement "Authentication Failed: No Matching Keys," followed by "Sending DISCONNECT Message." See Figure 78.

Eile Edit	Format View Help				
20120810 20120810 20120810 20120810	0 11:50:02.719 A07 0 11:50:02.730 A08 0 11:50:02.730 A08 0 11:50:02.730 A08 0 11:50:02.730 A08	WM Hardware: WIEM Read WM Key File Names Key Count: 3; Length: 43 Received Key File Name Buffer Length: 43	^	CACENERICE Enrough Innovation	Version 3.2.2.1
20120810 20120810 20120810 20120810	0 11:50:02.741 A09 0 11:50:02.741 A09 0 11:50:02.741 A09 0 11:50:02.741 A09 0 11:50:02.741 A09	Find Matching RSA Keyset WM Key File: MasterKeyIR.pri WM Key File: MasterKeyLT.pub WM Key File: CrewL.pub		Connect to a Device Device Name Liniversal Prev	Next
20120810 20120810 20120810 20120810 20120810 20120810	0 11:50:02.743 A09 0 11:50:02.743 A19 0 11:50:02.844 A20 0 11:50:02.845 A20 0 11:50:03.146 A21	Authentication Failed: No Matching Keys Sending DISCONNECT Message Closing KeepAlive Thread Closing RSSIThread Thread Stopping UDP AESCOM Bridge No. 1 Thread		Device Location: Universal Serial Number Serial Number: 00-0000000	Clear
20120810 20120810 20120810 20120810 20120810 20120810 20120810	0 11:50:03.246 A22 0 11:50:03.346 A23 0 11:50:04.347 A23 0 11:50:04.448 A24 0 11:50:04.480 A27 0 11:50:04.483 A28	Stopping VCom Router Thréad Deinitializing Version 3 messaging Unable to stop Inbound Monitor Thread Closing KeepAlive Socket Removing Connection Profile		Connect Connection Progress	

Figure 78. The Wi-Fi Connection Manager dialog box.

Installing a Configuration File

Use a PC with the correct "keys," and re-connect to the first IntelliRupter fault interrupter.

Install the configuration file for Crew1 in the stagethree folder into the first IntelliRupter fault interrupter. Then, install the configuration file for Crew2 into the second IntelliRupter fault interrupter using the same method described above. Notice the difference in the key pairs. Compare these to the key pair in the AdminCrew folder. See Figure 79.



Figure 79. The Crew2 and MasterCrew folders.

After sending the configuration file to the second IntelliRupter fault interrupter, exit the LinkStart program, and try to reconnect with the Crew1, Crew2, Crew3, and Admin-Crew keys from the stagethree folder. The second IntelliRupter fault interrupter should only connect with the Crew2 and AdminCrew keys.

The default directory for LinkStart files is C:\ProgramData\S&C Electric\LinkStart. This directory is a hidden directory. It will be necessary to use the **Folder Options>View>-Show hidden files and folders** option to see the content. See the example above.

To simulate a time change, advance the time in the IntelliRupter control to tomorrow's date. This is done by selecting the **Tools>Set Control Clock...** option when connected with IntelliLink software. See Figure 80.

S&C IntelliUNK® Remote Setur	p Software- IntelliRupter - [Operation- ools] Window Help	Main]
	Compact Flash Access	
S ₈ Intelli	Options	
L Pulse	Set Control Clock	
11 Sep 2012	Restart Device	

Figure 80. The IntelliLink Main screen.

Try connecting with each crew key again. For the first IntelliRupter fault interrupter, only Crew1, Crew3 and AdminCrew should connect. Remember the time controlled key for Crew3 was set to activate 24 hours after its creation. For the second IntelliRupter fault interrupter, only Crew3 and AdminCrew should connect. Crew2 will not be able to connect any longer because its **Time to Live in Days** setpoint has expired.

Remove the Crew1, Crew3, and AdminCrew keys and verify the first IntelliRupter fault interrupter cannot be connected.

If there is a USB dongle, close the LinkStart program, insert the dongle, and restart the LinkStart program. When prompted, enter the user password, "irtUser1!," in the example being used. Now, verify that IntelliRupter 1 can be connected.

Remove the USB dongle and install the Crew1, Crew3, and AdminCrew keys.

The only difference between the stagethree and stagefour configuration files is the stagefour file has Wi-Fi Module Access Settings. Rekey the first IntelliRupter fault interrupter with the stagefour configuration file that matches its serial number. Connect with the LinkStart program and click on the **Wi-Fi Admin** button. Now, check whether the credentials created above can be accessed. See Figure 81.

Oser Name Password Access 1 Admin irtAdmin1! Admin 2 User1 irtUser1! User 3 User2 irtUser2! User	
2 User1 intUser1! User 3 User2 intUser2! User	
3 User2 intUser2! User	
WiEi Module Access Cradentials Edit	
Admin irtAdmin1! Admin 💌	
User1 intUser11 User	
Conv Record Paste Record OK	

Figure 81. The Wi-Fi Module Access Credentials Edit dialog box.

To conclude the exercise, remove the security keys with the empty configuration file stored in the stageone folder.

Use the same re-keying approach and transfer the empty configuration files in the stageone folder of the USB thumb drive to the IntelliRupter fault interrupters. This will remove the security keys. Delete all the files and folders from the LinkStart folder on the user PC to return it to its original state. Then, connect to each IntelliRupter fault interrupter to verify the keys have been removed.

When there is a USB dongle, install the dongle and restart the Security Key Manager program. Click on the **View Dongle** button on the *Main* screen, click on the **Format Dongle** button on the View Dongle dialog box, and click on the **OK** button to reset the dongle to the default state.

The Wi-Fi configuration file can be sent to an IntelliRupter fault interrupter by using Intelli-Link® Setup Software. The latest IntelliRupter fault interrupter software must be installed on both the IntelliRupter fault interrupter and the portable computer. The configuration file is saved in the IntelliRupter compact flash memory, and the file is installed from the compact flash memory.

Follow these steps to send a Wi-Fi configuration file:

- **STEP 1.** Copy and rename the Master Key Configuration file from install.XX-XXXXXX. wm to WIFICTRL.WFM.
- STEP 2. Log in to the IntelliRupter fault interrupter with IntelliLink Setup Software.
- STEP 3. In the IntelliLink software menu bar select, "Tools>Compact Flash Access...."
- STEP 4. Navigate to the compact flash settings folder.
- STEP 5. Navigate the PC file system to the location of the renamed WIFICTRL.WFM configuration file. Users may need to allow "view system files" in the Tools>Options menu. See Figure 82.

Compact Flash Explorer				_IOX
Ne Edit View Tools Help				
Q 0 0				
U. Compact Flash Card				
Pure SETTINGS				0.0.0 B
Part 1	P			
3.41	Name	Size Tj	154	Date Modfied Permissions
D ANICOS	UTIONET.WAN	21,535 F4e		12/31/1999 6:11:36 PM A
A WAVEFORM	SPEEDRET.WAN	21,536 146		12/31/1999 6:11:36 PR -A
3 CO NEON	WHUTS WH	64,035 FM2		1237/1339811:36FR - A
SETTINGS	Samens win	65 FFE		17672010 24126FR - 4
BASEMEM	*1			
	,			
3 PC File System:				
Patr 0:00cuments and Sellings All Uters Application Data	SUC Electric VLinkStart			
🛪 🖸 Trauvait 🗳 🕄	Name	Size	· 1/00	Date Modified
🛞 🎱 Kicssoft Help	HastelR Cortig		File Folder	1/6/2010 12 59 54 PM
🖲 🚞 NSScanAppDataDir	😂 Mastel Rn Confg		File Folder	1/6/2010 1:00.12 PM
- Controller	No Key Config		FleFolder	1/6/2010 1:03:27 PM
3) 💭 Office Gerruine Advantage	Citizen p		FloFelder	1/6/2010 12 09:58 PM
S SUCERONC	🖸 00-000000 ivi	36	iri	1/6/2010 1.02.45 PM
	C8-9001037 ivi	35	iri -	1/5/2010 2 56:33 PM
W S Maded B Confin	DEEckini	45	ini	1/6/2010 1.02:37 PM
3 S Hazel Ro Corto	anoge.03.01.04.04bn	810,942	tin	9/4/2009 9.54:56 AM
🕤 🗁 No Key Carlo	n:tat.00.000000.wm	88	WE	1/6/2010 1:02:51 PM
🕀 😂 temp	1 KeyListbe	42	54	1/6/2010 11:48:32 AM
🛞 🏠 Scelable Software	LISOB M	127	bd	125/2010 12 10 10 PM
🖲 ڬ Sonic	HadoKey bi	58	03	1/5/2010 12 10 40 PM
Synantee	III noticino	168	mb .	1/6/2010 1:02:51 PM
	C WHOTBAWAS	88	WHM	176720101107:02194
Data/StC Electic/LinkStat/WFICTRL/WFIN - stated	· File · Stat		PathFrom	· Path To
O-Documents and Sations Will Ison Marshaving	WIRCIRLW uskosóng	100% D.\D	Documents and Settings VAL.	_ SETTINGS
D#a\StCElectic/LinkStat\WFICTRLW7M - fridhed				
- teolog				
ر ت ا	-			

Figure 82. The Compact Flash Explorer screen.

- **STEP 6.** Upload the WIFICTRL.WFM file from the PC File System to the compact flash. Users may need to select the **YES** button to overwrite the existing file.
- **STEP 7.** Close the Compact Flash Explorer program. In the **IntelliLink** software menu, select "Setup>Communications>WiFi."

STEP 8. On the *Wi-Fi screen*, click on the **Install** button. Then, select the **Transfer Configuration** option and click on the **OK** button to load the new Wi-Fi settings file from the Compact Flash memory.

			The American A White the Veser
IntelliRupter®	Connected to: C9616 Loca	tion: HWY 43 JUST NORTH OF CELESTE RD	Settings Res
PulseCloser		Setup>Communications>V	MiFi
Operation	DNP Senal Ports Routing E	themet west	
Intelli leam SG Setup	Firmuna Varian	2161	
General A Protection General Profile 1 Canceral Profile 2	NAC Address	004000-2244-55	
	Social Number	09.0602170	
General Profile 3	MEEL Status	00-0002110	
General Profile 4 Hot Line Tag	Startun Exchange Seguence	08 - Link to WiEi Activo	
Closing Profile 1	Koonaliyo Statue	Koonslive Active	
Cold Load Pickup	Base Memory Access Status	WiEi Signature Record obtained	
Advanced Setup A Restoration	Transfer WiEi Configuration	Wirt signature Record obtained	
Loop Communications Point Mapping Security Validate/Apply Metering Diagnostics Logs	Note: The following command WiFi Settings File to Compact Bytes Transferred Transfer Status	s will take place immediately. There is no need to Vali Flash Save 0 Ready	idate or Apply settings.
	New WiFi Settings File From Bytes Transferred Transfer Status	Compact Flash Install 0 Ready	

STEP 9. Verify the transfer status has completed. See Figure 83.

Figure 83. The Setup>Communications>Wi-Fi screen.

STEP 10. To check whether this procedure completed correctly, take the portable PC to the IntelliRupter fault interrupter in the field and log in via the Wi-Fi connection with the proper keyset.

The first record of the database is displayed the first time the LinkStart program is run. See Figure 84.

🔀 WiFi Connection Management
File Edit Tools
S&C Electric Company Excellence Through Innovation LinkStart Version 3.2.2.1
Connect to a Device
Device Name: Universal Prev Next
Device Location: Universal Serial Number
Serial Number: 00-0000000 Clear
Connect Connection Progress
Belkin USB Wireless Adaptor

Figure 84. The Wi-Fi Connection Management dialog box.

Click on the **Clear** button to prepare the LinkStart program to search for a character or string of characters that appear anywhere in the main database file. See Figure 85.

WiFi Connection Management	
File Edit Tools	
S&C Electric Company Excellence Through Innovation	LinkStart Version 3.2.2.1
Connect to a Device	• = •
Device Name: Prev Device Location:	Next
Serial Number:	Clear
Connect Connection Progree	SS
Belkin USB Wireless Adaptor	

Figure 85. The Connect to a Device dialog box.

Typing even a single character in the **Device Name** field opens a drop-down list of matches. See Figure 86.

MiFi Connection Mana	agement	
File Edit Tools		
S&C Elec Excellence Th	tric Company rough Innovation	LinkStart Version 3.2.2.1
Connect to a Device		
Device Name: F	F	Prev Next
Device Location: Serial Number:	07-0009014 GP00001 W 07-0009033 GP33582 Je 07-0009050 GP11331 Fr	est end of first river road fferson road amingham A West
Connect	07-0009052 PC78961 Fo 08-0004159 GP12678 Cc 07-0009063 PC54321 Fo 07-0009064 GP65434 Te 07-0009070 GP23451 Fo	rtunata Ln orner of main and cherry in Duvall Iderol Rd onth and Forrest ortySeventh
Belkin USB Wireless Ada	07-1204576 RC66767 Cr 07-0009083 GP56776 Fr	eekside Cafe on tenth ontal Lobe Road

Figure 86. The drop-down list of matches.

Typing another character narrows the search results. See Figure 87.

WiFi Connection Management
File Edit Tools
S&C Electric Company Excellence Through Innovation LinkStart Version 3.2.2.1
Connect to a Device
Device Name: Fr Prev Next Device Location: Serial Number:
Clear 07-0009050 GP11331 Framingham A West Conne 07-0009083 GP56776 Frontal Lobe Road
Connection Progress

Figure 87. More typed characters narrow the search result.
Clicking on an IntelliRupter fault interrupter entry in the match list causes that device to be selected. Then, click on the **Connect** button. See Figure 88.

MiFi Connection Management								
<u>Eile Edit I</u> ools								
S&C Electric Company Excellence Through Innovation	LinkStart Version 3.2.2.1							
Connect to a Device								
Device Name: Universal Prev	Next							
Device Location: Universal Serial Number]							
Serial Number: 00-0000000	Clear							
Connect								
Connection Progres	5							
Intel(R) WiFi Link 5100 AGN								

Figure 88. The Connect to a Device dialog box.

When the IntelliRupter Installer has been loaded on the portable PC, follow the procedures outlined in the "Connecting to an IntelliRupter Fault Interrupter" section on page 30 for each IntelliRupter fault interrupter to be configured.

For the most secure key management, copy only those files needed to a specific portable PC. After the IntelliRupter fault interrupters have been configured with master keys, remove the .WM file from the PC that uploaded the master keys.

Copies of the original key files should be saved in a secure place. If all copies of a key are lost, there is no backdoor to re-create the key.

NOTICE

When the Wi-Fi module security keys have been configured, there is no way to gain access to an IntelliRupter Wi-Fi module without using the correct security keys. If the keys are lost, the communication module must be returned to S&C to have the factory default restored. When the configured security keys are available, the factory default keys can be restored at any time with the following procedure.

To remove configured keys and restore the factory default security keys, run the Security Key Manager program. From the *Main* screen, click the **Options** button and uncheck all items shown in Figure 89. Click the **OK** button. Click the **Yes** button on the confirmation dialog box.

	Station of the local division of the local d
Device Security Architecture Options	
F Provide for Master Key	
Provide for Regional Specific Keys	
Provide for Crew Specific Keys	
Provide for WiFi Module Access Credentials	
Change Export Directory	
C:\ProgramData\S&C Electric\LinkStart\	
	ОК

Figure 89. The Device Security Architecture Options dialog box.

The **Master Key** button has now been removed from the *Main* screen. See Figure 90.

Securi Edi	ty Key Manager it <u>I</u> ools S&C Electr Excellence Thro	vic Company ugh Innovation	Security Key Manage Version 3.2.1
Doub	ole-Click or Press E	nter to Edit	
	Serial Number	Device Name	Device Location
1 2 3 4	00-000000 08-0008734 08-0008736 08-0008737	Universal IRPC1005 IRPC1006 IRPC1007	Universal Serial Number First Cross after Johns Road MP27 Johns Road MP32 Jims Road at rail grade crossing
Op	ntions Decrypt	Files Export	ove Up Move Down Save Exit

Figure 90. The Security Key Manager screen.

Click on the **Export** button on the *Main* screen, select the Universal Serial Number, 00-0000000, and click on the **Export** button on the Export Configuration and Database Files dialog box to generate an empty key file. See Figure 91. Loading the empty key file overwrites the existing key file, removes the security keys, and re-enables factory default.

08-0008734 08-0008736 08-0008737	IRPC1005 F IRPC1006 J IRPC1007 J	Iniversal Seri First Cross aft Johns Road M Jims Road at	al Number er Johns Road IP32 rail grade cross	MP27 ing	

Figure 91. The Export Configuration and Database Files dialog box.

Examine the Universal Configuration file generated after all the security key options were unchecked. Notice there are no key files listed at the bottom of the list on the left. Compare the Figures 92 and Figure 93 on page 77.

Config File Decryption								
Select File To Decrypt install.00-0000000.wm	Decrypted File Contents install.00-0000000.wm Size: 64 Flags 00000001 Timestamp 09/09/2012 12:56:56 UTC CRC calculated 016C1FC2 Matches File 00-0000000.ini Size: 31 Ini: <admin 1="" 8="" 9600="" n="" noradio="" user=""></admin>							
Delete File	Extract Files Exit							

Figure 92. The Universal Configuration file generated.

Select File To Decrypt	Decrypted File Contents	
install.08-0008734.wm	install.08-0008734.wm Size: 1504 Flags 00000001 Timestamp 09/04/2012 18:21:48 UTC CRC calculated 4CF2C268 Matches File 08-0008734.ini Size: 31 Ini: <admin 1="" 8="" 9600="" n="" noradio="" user=""> File Region1IR.pri Size: 993 File ShortTime.pub Size: 417</admin>	
	e	
Delete File	Extract Files	Evit

Figure 93. A serial number-specific configuration file.

Converting MBL_ DB.csv to LSDB.txt

Enter information directly into an LSDB.txt file or convert the file type, as described in the next steps.

Locate the MBL_DB.csv file in the folder: \Documents and Settings\All Users\ Application Data\S&C Electric\LinkStart\Keyfiles, and make a backup of the file. Open this file with Microsoft Excel. The order and quantity of columns may vary depending on the version of the LinkStart software used to create this file. See Figure 94.

	licrosoft Ex	cet - MBL_DB.C	SV												
圈	Ele Edt	Yew Insert I	Format Icols D	jata <u>Window</u> Help									Type a ques	ition for help	0 ×
10	883	alaar	7 M X D	3-310-0	· 9. 2	- 21 71 13	43000	100% -	0						
] Te	ies New Roman	• 12 •	BIUI	著港团 S %		(课课)	H . C	Δ							
	A1	*	& Mode												
	A	В	C	D	E	F	G	H	I	1	K	L	M	N	07
1	Mode	Serial	DeviceName	DeviceLocation	Configured	KeyFile1	KeyFile2	KeyFile3	KeyFile4	KeyFile5	ConfigFile	WANRad	WANRadi	Editor	EditorT
2	TRUE	00-0000000	Universal	Universal access	TRUE						comporting				
3	TRUE	08-9000001	PulseCloser 1	North Side	TRUE										
4	TRUE	08-9000002	PulseCloser 2	South Side	TRUE										
5	FALSE	08-9000003	PulseCloser 3	East Side	FALSE										
6	FALSE	08-9000004	PulseCloser 4	West Side	FALSE										
7	FALSE				FALSE										
8	FALSE				FALSE					1					
9	FALSE				FALSE										
10	FALSE				FALSE				1	-	-				
	N N MB	_D8/							K			M	1		2
Rea	\$1													NUM	

Figure 94. The Microsoft Excel data.

Delete all of the columns except the column containing serial numbers typically labeled "Serial," the column containing device names typically labeled "DeviceName," and the column containing device locations typically labeled "DeviceLocation." See Figure 94 on page 75.

To delete a column, move the mouse cursor over the letter of the column to be deleted and click to select the column. "Column A" in Figure 96 on page 76 shows what a selected column looks like. Then, right-click on the column letter to open the **Options** menu and click on the **Delete** option. Repeat this process until only the Serial, Device-Name, and DeviceLocation columns remain. See Figure 95 on page 79.

	Microsoft Excel - MBL_DB.CSV											
3	Eile Edit View Insert Format Tools Data Window Help											
	E 🗅 🧀 🕞 🖂 🕰 🖏 🖏 🐇 🖻 🛍 • 🕩 🕫 • 🕞 - 😒 Σ • ≙↓ Χ↓ 🛍											
1	Times New Roman • 12 • B I U 医喜喜菌 \$ % , 5% 5% 律律											
	Al 👻 🎓 Mode											
		A		B	С	D	E	F				
	1	Mode	x	Cut	viceName	DeviceLocation	Configured	KeyFile1				
	2	TRUI	6	⊆ору	versal	Universal access	TRUE					
	3	TRUI	12	Paste	seCloser 1	North Side	TRUE					
	4	TRUI	~	Paste Special	seCloser 2	South Side	TRUE					
	5	FALS		To see	seCloser 3	East Side	FALSE					
	6	FALS		Insert	seCloser 4	West Side	FALSE					
	7	FALS		Delete			FALSE					
	8	FALS		Clear Contents			FALSE					
	9	FALS	1	Eormat Cells			FALSE					
	10	FALS		<u>C</u> olumn Width			FALSE					
K	•	F H I		Hide								
R	ead	/		<u>U</u> nhide								

Figure 95. Deleting columns n the Excel program.

Next, select Row 1, the title row, by moving the cursor over the number in the far-left column of the row and clicking on it. Figure 96 shows a selected row. Right click on that number to open the **Options** menu and select the **Delete** option. See Figure 96.

X		¥) • (• -		N	BL_DB.c	sv - Microsoft Ex	cel				x
	File	Home Insert	Page Layo Fo	rmulas Data	Review	v View Develo	per Ad	d-Ins Planning	ξ Acrobat	۵ 🕜 🗆	di X
Pa	aste	K Calibri Image: Triangle in the strength of the strenge strengt	$ \begin{array}{c c} \bullet & 11 & \bullet \\ \hline J \bullet & A^* & A^* \\ \hline \bullet \bullet & \underline{A} \bullet \\ \hline \bullet & \bullet & \underline{A} \bullet \\ \hline \bullet & \bullet & \\ \hline \bullet & & \bullet & \\ \hline \bullet & \bullet & \\ \bullet & \bullet & \\ \hline \bullet & \bullet & \bullet & \\ \hline \bullet & \bullet & \\ \bullet & \bullet &$			General ▼ \$ ▼ % • .00 .00 Number 5	A Styles	Gelete ▼ Format ▼ Cells	Σ · A Z · Z · Sort Filter Edit	Find & Select +	
	Calib	ori • 11 • A*	A \$ + %	, 🔤 rial I	Number	r					~
	в	I 🗏 🏷 - 🛕	* *	8 🕩 📃		С		D	E	F	-
1	Ser	rial Numbe Deice	Name	Device	Locatio	on					<u> </u>
2	\$	Cut	sal	Unive	rsal						=
3		Copy	loser_l	North	Side						
4	2	Paste Options:	loser_2	South	Side						
5		Δ	loser 3	East S	de						
6		Paste Special	loser_4	West	Side						
7		Turce 2pectanii									
8		Insert	-								-
14		Delete						1111			1
Re		Clear Contents				C	ount: 3		00% 🗩	0	+
	8	<u>F</u> ormat Cells <u>R</u> ow Height <u>H</u> ide		-					_		

Figure 96. Deleting rows in the Excel program.

On the Excel menu bar, select the **File>Save As...** option to open the Save As dialog box. Browse to the location to save the new database file. The default location is D:\ Documents and Settings\All Users\Application Data\S&C Electric\LinkStart. Enter LSDB. txt as the file name. Use the **Save As** pull-down menu to select the **Text (Tab delimited)** (*.txt) option and click on the **Save** button. See Figure 97.

W Missonaft Event	IPL DR COV						() (s	
R Line Edt View	Incert Format Tools Da	an us	odow Helo		Type	a question for 1	nelo 📮	
D CR DD OL	23 DA 149 AN IV DA P			10 5 -	A Z 4/h	A A A	100%	
			He w	*.0 .00		-0 00 00		
A 1			3 70	· .00 →.0	· 패는 패는 / [11	• • • •		
AI	× ,x 00-00	100000	0	D	E	F	C	T=
1 00.000000	D	TToirre	real access	D	£	r	9	
2 08 9000001	DulceClocer 1	Morth	Side					
3 08-9000001	PulseCloser 2	South	Side					
4 08-9000003	PulseCloser 3	East S	Side					
5 08-9000004	PulseCloser 4	West	Side					
6	Come to		1	-				
7	Save As						_	كك
H + H MBL DB	Save in: 🛅 l	.inkStart		~	© - 🖸 (Q X 🖬 🗉	• Tools •	
Ready								
	My Recent							
	Documents							
	12							
	Desktop							
	my Documents							
	<u> </u>							
	my Computer							
	My Network	ane:	LSDB.M					Save
	Places Save a	as type:	Text (Tab delim	ited) (*.txt)		2		Cancel
			Text (Tab delim	ited) (*.txt)		-		
			Unicode Text (* Microsoft Excel	.bxt) 5.0/95 Workh	ook (* vis)			
			Microsoft Excel	97- Excel 200	3 & 5.0/95 Wor	kbook (*.xls)	2	
			ICSV (Comma de	simited) (*.cs)	()		2	

Figure 97. The Save As dialog box.

Click on the Yes button to close Excel. See Figure 98.

Microsof	it Excel
i	LSDB.txt may contain features that are not compatible with Text (Tab delimited). Do you want to keep the workbook in this format? • To keep this format, which leaves out any incompatible features, click Yes. • To preserve the features, click No. Then save a copy in the latest Excel format. • To see what might be lost, click Help. Yes No Help

Figure 98. The Microsoft Excel Save As dialog box.

Figure 99 is an example of a converted database.

LSDB.txt - Notepa	d	The Address	- • ×
<u>File Edit Format</u>	View Help	universal access	
08-9000001 08-9000002 08-9000003 08-9000004	Pulsecloser_1 Pulsecloser_2 Pulsecloser_3 Pulsecloser_4	North side south side East side West side	
4			► at

Figure 99. The converted database list.

Entering a New LSDB.txt File

A new LSDB.TXT file can easily be created in Excel.

Starting from a new Excel Workbook, enter the fields by hand, save it as the file LSDBe.xls (different name, in this example, to prevent overwriting the "real" LSDB.TXT file). See Figure 100.

Microsoft Excel -	LSDBe.xls							-02
🚳 Ele Edit View	Insert Format]	[ools Ωata Window Help ≧a 💁 • 🖋 ↔ - ♡ - 🧕 Σ • ½↓ ⅔↓	<u>10</u> 43 10	0% 2.0	Type a	question fo	ir help	8 ×
1 2 2 2 2 3 2 3 2 3 2 3 2 3 2 3 2 3	alie și 🗟 🖗 🖲	A Reply with Changes End Review						
D4 👻	f.							
A	B	C	0	E	F	G	н	17
1 08-0001023	GFPC5492A	Langdon Farm Road South						
2 08-0001025	GFPC5497C	Duck Creek Road West at Hunter Rd						
3 08-0001478	GFPC5502A	West End Railway Ave						
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								L
18								
19								-
20 H 4 > H Sheet1 /	Sheet2 / Sheet3 /	1	1				1	
Ready			1				NUM	(estu

Figure 100. The new Excel file.

Then, click on the **Save As** button using the same file name, but chose the "Save as" type to be a Text Tab Delimited (*.txt) file. See Figure 101.

Save As						2 🛚
Save in:	C UnkStart	· · · · · · · · · · · · · · · · · · ·	v 📀 -	10,>	< 🔟 🖬 • 🛛	Tools -
My Recent Documents Desktop My Documents My Computer	KeyList.b LSDB200 LSDB200 LSDB.bxt LSDB.bxt MasterKe wLSDB.b	kt 90818095630.txt 90818154304.txt t y.txt kt				
No. Mathuart	File game:	LSDBe.bxt			~	Save
Places	Save as type:	Text (Tab delmited) (*	.txt)		~	Cancel

Figure 101. The new file name.

Excel then warns it will only save one sheet—the active sheet. Click on the \mathbf{OK} button. See Figure 102.

Microso	ft Excel
1	The selected file type does not support workbooks that contain multiple sheets. • To save only the active sheet, click OK. • To save all sheets, save them individually using a different file name for each, or choose a file type that supports multiple sheets. OK Cancel

Figure 102. The Excel warning dialog box.

Excel then warns of possible loss of features. Click on the Yes button. See Figure 103.

Microsof	ft Excel
()	LSDBe.txt may contain features that are not compatible with Text (Tab delimited). Do you want to keep the workbook in this format? • To keep this format, which leaves out any incompatible features, dick Yes. • To preserve the features, dick No. Then save a copy in the latest Excel format. • To see what might be lost, dick Help.
	Ites No Heb

Figure 103. The Excel file save warning dialog box.

Excel then changes the file name of the Workbook to LSDBe.txt. See Figure 104.

100	Microsoft Excel	- LSDBe.txt	Tools Data Window Help		_	Type a	cuestion fo	r helo	-00
	🐸 🖬 🖪 🕘	A DIS MIX	20 2 · 3 - · · · 8 Σ · 2 2	<u>100 45</u> 2	00% 🛃	B	34 -	a naip	
	19900	<u>제(5 %)</u> 중 문(A Ve Reply with Changes End Review						
	D4 👻	f.							
	A	B	C	0	E	F	G	н	1.17
1 2	08-0001023 08-0001025	GFPC5492A GFPC5497C	Langdon Farm Road South Duck Creek Road West at Hunter Rd						
4	08-0001478	GFPC5502A	West End Kalway Ave		1				-
5									-
7 8									
9 10									-
11 12									-
13 14				-	-				-
15 16									
17									
19 20								3	
Rea	ty H\LSDBe/	Sheet2 / Sheet3 /		<		4		NUM	>

Figure 104. The new Excel file.

Excel then asks about saving changes. Click on the No button. See Figure 105.



Figure 105. The Excel save changes dialog box.

Checking File with a Binary Viewer

To demonstrate what has been created, open the file with a binary viewer. See Figures 106 and 107.

Open File					2		
Look in:	😂 LinkStart		× ③ •	🖄 🔕 🗙 🔂 🖬 • 1	rools -		
-	Name 🔺	1	Size	Туре	Date Modifie		
	0000000	00.ini	1 KB	Configuration Settings	8/18/2009 3		
Desktop	DBEdit.ini		1 KB	Configuration Settings	8/18/2009 2		
	install.00-	0000000.wm	2 KB	Windows Media Audi	8/18/2009 3		
0	KeyList.tx	t	1 KB	Text Document	8/18/2009 2		
	LSDB200	90818095630.txt	5 KB	Text Document	8/17/2009 1		
My Projects	D LSD82009	90818154304.txt	1 KB	Text Document	8/18/2009 3		
	LSD8.txt		1 KB	Text Document	8/18/2009 3		
	LSDBe.txt		1 KB	Text Document	8/19/2009 6		
	S LSDBe.xk		14 KB	Microsoft Excel Wor	8/19/2009 6		
My Computer	MasterIR.	pri	1 KB	PRI File	8/18/2009 2 8/18/2009 2		
	MasterIR.	pub	1 KB	Microsoft Office Publ			
	B NasterKe	y.txt	1 KB	Text Document	8/18/2009 2		
	🔄 NasterLT.	pri	1 KB	PRI file	8/18/2009 2		
	MasterLT.	pub	1 KB	Microsoft Office Publ	8/18/2009 2		
	<		11				
	File name:			×	Open		
	Files of type:	All files (*.*)		~	Cancel		

Figure 106. The Open File dialog box.

Source Code (Text) Editor (Default)	<u>A</u> dd
XML Editor	Remove
XML Editor with Encoding	Temete
HTML Editor with Encoding	Set as <u>D</u> efault
Notepad (Microsoft® Windows® Operating System)	
Binary Editor	
Resource Editor	

Figure 107. The Open With dialog box.

Figure 108 is the hexadecimal display of the file contents, which include the corresponding character glyphs on the right.

Solution1	- Mi	cros	soft	Vis	ual	Stu	dio												16
<u>File E</u> dit	View	D	ebug	. 1	Cools	: <u>v</u>	Vinde	w		mur	nity	He	lp						
🛐 • 💷 • 🚺	26	1 6		5 B		31	n .	(51	• 5	- [31	2						¥ : (*	5
i ⊳ u ⊂a	a	\$	題(3	. E	3	Hex	1		10	1.2	2	9	Q	-	1	オモノフ	A 🗆 🗖	
. LSDBe.t	xt																	-08	
00000000	30	38	2D	30	30	30	31	30	32	33	09	47	46	50	43	35	08-000102	3.GFPC5	٦
00000020	6D	20	52	6F	61	64	20	53	6F	75	74	68	OD	0A	30	38	n Road So	uth08	
00000030	2D	30	30	30	31	30	32	35	09	47	46	50	43	35	34	39	-0001025.	GFPC549	
00000050	61	64	20	57	65	73	74	20	61	74	20	48	75	6E	74	65	ad Vest a	t Hunte	
00000060	72	20	52	64	OD	OA	30	38	2D	30	30	30	31	34	37	38	r Rd08-	0001478	
000000080	45	47 6E	64	20	43	61	35 69	30 6C	22	61	79	20	41	76	65	20 0D	End Raily	a.west av Ave.	
00000090	ÓÀ																	-,	
																		and the second	
Ready								Of	f 0x0	0000	0000	Ş		Len	0x0	0000	0000	INS	

Figure 108. The hexadecimal display of file contents.

Here are the invisible (non-printing ASCII) characters in the file: the 09 in the 11th character position of the first row; the 09 in the fifth character position of the second row; the 0D and 0A in the 13th and 14th character positions of the third row. ASCII 09 is the "tab" character. ASCII 0D and 0A are the "carriage return" and the "line feed" characters. These carryovers from the old Teletype electromechanical printers are used as delimiters between fields (tabs) and end-of-line or record separators (carriage return and line feed, often referred to as a "new line" pair.

This format, achieved either through using Excel as described above or through using the Security Key Manager program, is compatible with the LinkStart program and the Security Key Manager program.

The same format with a space character instead of the tab character is also compatible with the LinkStart program. The Security Key Manager program can read such a file, but when saving it would write it with the tab characters.

There is no particular limitation to the number of records that LinkStart can work with.

Opening an existing text file is also simple. Figure 109 shows a file with spaces used instead of tab characters.

Text Import Wizard - Step 1 of 3	2 💟
The Text Wizard has determined that your data is Fixed Width. If this is correct, choose Next, or choose the data type that best describes your data. Original data type Choose the file type that best describes your data:	
Qelmited - Characters such as commas or tabs separate each field. - Fields are aligned in columns with spaces between each field.	
Start import at gow: 1 🗇 File grigin: 437 : OEM United States	~
Preview of file C:\Documents and Settings\All Users\Applcation Data\S&C \LSDBb.txt. 1 08-0001023 GFPC5492A Langdon Farm Road South 2 08-0001025 GFPC5497C Duck Creek Road West at Hunter Rd 3 08-0001478 GFPC5502A West End Railway Ave	-
হ হ	_

Figure 109. The Text Import Wizard dialog box.

Excel places rather arbitrary dividers, but these are easily changed. See Figure 110.

ext Import	Wizard - S	step 2 of 3			2
This screen lets	you set field v	vidths (column breaks).			
Lines with arr	ows signify a co	olumn break.			
To CREATE To DELETE	a break line, d a break line, do break line, did	lick at the desired position ouble click on the line.	on.		
Data greview -					
1	10 2	0 30	40	50	60
08-0001023	0 2 GFPC54923	0 30	40 d South		<u>60</u>
08-0001023 08-0001025	0 2 GFPC5492A GFPC5497C	0 30 Langdon Farm Ros Duck Creek Road	40 d South West at F	ş0 Iunter Rd	<u>60</u>
08-0001023 08-0001025 08-0001478	0 GFPC5492A GFPC5497C GFPC5502A	0 30 Langdon Farm Ros Duck Creek Road West End Railway	40 d South West at F Ave	ş0 iunter Rd	<u></u>

Figure 110. The Text Import Wizard dialog box.

In Figure 111, the extra dividers have been removed by double-clicking on them.

ext Import	Wizard - S	tep 2 of 3	26
This screen lets	you set field v	idths (column breaks).	
Lines with arro	ows signify a co	olumn break.	
To CREATE To DELETE To MOVE a	a break line, c a break line, de break line, click	lick at the desired position. buble click on the line. k and drag it.	
Data preview		F (
	0.3	0 30 40 50 60	
08-0001023 08-0001025 08-0001478	GFPC5492A GFPC5497C GFPC5502A	Langdon Farm Road South Duck Creek Road West at Hunter Rd West End Railway Ave	
			~
			Σ
<u><</u>			

Figure 111. Double-clicking on the extra dividers to remove them.

When the final screen appears, click on the **Finish** button. See Figure 112.

ext Import	Wizard - Step 3 of 3		2
This screen let the Data Form 'General' con values to da Data greview	s you select each column and se at. verts numeric values to number tes, and all remaining values to <u>A</u> dvanced	et Column data format ③ General ○ Iext ○ Date: MDY ○ Do not import column (skip)	
2000731 08-000102 08-000102 08-000147	General General GFPC5492A Langdon Fa GFPC5497C Duck Creek GFPC5502A West End R	erm Road South : Road West at Hunter Rd Mailway Ave	

Figure 112. The last step in the Text Import Wizard dialog box.

Microsoft Excel - LSDBb.txt				908
:2	<u>Eile E</u> dit ⊻	iew <u>I</u> nsert F <u>o</u> rma	at <u>T</u> ools <u>D</u> ata <u>W</u> indow <u>H</u> elp	- 8 ×
:[) 💕 🖌 🔓 🙆) 3 3 3	🏅 🖻 🔁 • 🟈 🤊 • 🍮 Σ • 💱 🛄	Ø "; B ;
🔁 🖄 🖓 🗔 🧐 🏹 🗇 🏷 🐉 🖓 🖓 🖓 Keply with Changes End Review 🖕				
_	D4 👻	fx.		
	A	В	C	DEA
1	08-0001023	GFPC5492A	Langdon Farm Road South	
2	08-0001025	GFPC5497C	Duck Creek Road West at Hunter Rd	H
3	08-0001478	GFPC5502A	West End Railway Ave	
4				
5	2			
6				
7				
8				×
H	ISDBb]<]	>
Re	ady		NUR	4

And the text will be properly imported. See Figure 113.

Figure 113. The new import in the Excel program.

This could alternatively have been done by interpreting the input as being space delimited to separate fields one and two and two and three, and removing all the other dividers.

What are the system requirements?

- A portable personal computer with Windows 10, an Intel® Core[™] i7 Processor with 8 GB of RAM (recommended) or a dual-core processor with 4 GB RAM (minimum), a wireless card (onboard or USB), an Internet browser, and access to **sandc.com**
- Administrative privileges
- Microsoft.Net Framework Version 4.8 (To verify whether it has been installed on a computer, open C:\Windows\Microsoft.Net\Framework with Windows Explorer. If v4.8 has not been installed, download it from this link: microsoft.com/net. If the installer does not detect the correct version of .Net, it will not install IntelliLink6 software.)
- Windows PowerShell 5.0 is set for an execution policy of AllSigned (Execution policies of RemoteSigned and Unrestricted will also work. Policy selection should be based on IT department security policy. The AllSigned execution policy will result in the appearance of a dialog after a firmware upgrade has begun. To perform the firmware upgrade, the **Run once** or **Always run** button must be selected. Selection should be based on the IT department security policy. Windows PowerShell comes installed by default in every Windows operating system.)

Can I install more than one key in an IntelliRupter fault interrupter?

No. This implementation is for the master encryption key only and allows only one key in each IntelliRupter fault interrupter.

Can I replace a communication module that has master security keys installed in its Wi-Fi module with a new communication module?

Yes. The security configuration is also stored in the base memory module. When a new communication module is plugged in to an IntelliRupter fault interrupter, the Wi-Fi module reads the security information in the base memory module and resets itself to match the local security configuration. For the laptop to connect, it must have the correct keys that match the IntelliRupter fault interrupter security configuration.

Can I configure Wi-Fi security with a docking station?

Yes. There is a check box in the Wi-Fi Configuration and Setup dialog box for the Wi-Fi module to overwrite the base memory module configuration on next power-up. Select that check box, and click on the **Apply** button.

Can I re-create my key files if I lose them?

No. Even if using the same name each time the key files are generated, the Wi-Fi key program generates a new encryption.

If I lose my key files, is there a back door to unlock the Wi-Fi connection?

No. If the keys have been lost, return the communication module to S&C to have factory default restored.