


# Wi-Fi Administration and Operation

## Table of Contents

Section	Page	Section	Page
<b>Introduction</b>		<b>Connecting to an IntelliRupter Fault Interrupter</b>	24
Qualified Persons . . . . .	2	<b>Loading Wi-Fi Keys with Wi-Fi Admin</b>	25
Read this Instruction Sheet . . . . .	2	<b>Wi-Fi Admin Functions</b>	
Retain this Instruction Sheet. . . . .	2	Uploading Wi-Fi Firmware . . . . .	26
Special Warranty Provisions. . . . .	2	Security Event Logs . . . . .	26
Use the Latest LinkStart Software Revision. . . . .	2	Wi-Fi Device Status . . . . .	28
<b>Safety Information</b>		Communication Counters. . . . .	29
Understanding Safety-Alert Messages. . . . .	3	Wi-Fi Module Reboot . . . . .	29
Following Safety Instructions . . . . .	3	WAN Port Settings . . . . .	30
Replacement Instructions and Labels . . . . .	3	<b>Wi-Fi Security Key Administration</b>	
<b>Overview</b> . . . . .	4	Software Installation . . . . .	31
<b>Wi-Fi Authentication Key Generator</b> . . . . .	6	Key Creation . . . . .	32
<b>Database Editor Program</b>		Security Key Manager . . . . .	33
Security Key Manager . . . . .	8	Exporting Configuration Files . . . . .	35
Enter Master Key Name . . . . .	10	USB Dongle . . . . .	43
Add IntelliRupter Fault Interrupters to the		Using LinkStart . . . . .	47
Database . . . . .	11	Installing a Configuration File . . . . .	49
Data Entry with Notepad. . . . .	12	<b>Loading Wi-Fi Keys with IntelliLink® Remote Setup Software</b> . . . . .	51
Navigation. . . . .	13	<b>LinkStart Database Searches</b> . . . . .	53
Delete/Undelete . . . . .	14	<b>Removing Wi-Fi Security Keys</b> . . . . .	56
Using a Dongle . . . . .	15	<b>Excel File Examples</b>	
Formatting a Dongle . . . . .	16	Converting MBL_DB.csv to LSDB.txt. . . . .	58
Keying a Dongle . . . . .	17	Entering a New LSDB.txt File . . . . .	62
Creating Regions and Crews . . . . .	18	Checking File with a Binary Viewer . . . . .	64
<b>Wi-Fi Configuration File</b>		<b>Frequently Asked Questions</b> . . . . .	68
WAN Radio Configuration and Wi-Fi Access . . . . .	19		
Exporting Configuration Files . . . . .	21		
Decrypting a Configuration File . . . . .	23		



Qualified Persons

 **WARNING**

The equipment covered by this publication must be installed, operated, and maintained by qualified persons who are knowledgeable in the installation, operation, and maintenance of overhead electric power distribution equipment along with the associated hazards. A qualified person is one who is 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 the special precautionary techniques, personal protective equipment, insulating 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

Thoroughly and carefully read this instruction sheet before programming, operating, or maintaining your S&C IntelliRupter PulseCloser Fault Interrupter. Familiarize yourself with the Safety Information on page 3. The latest version of this instruction sheet is available online in PDF format at [sandc.com/en/support/product-literatureasp](http://sandc.com/en/support/product-literatureasp).

Retain this Instruction Sheet

This instruction sheet is a permanent part of your S&C IntelliRupter PulseCloser Fault Interrupter. Designate a location where you can easily retrieve and refer to this publication.

Special Warranty Provisions

The standard warranty contained in S&C’s standard conditions of sale, as set forth in Price Sheet 150, applies to the IntelliRupter® fault interrupter and its associated options except for the control group (the protection and control module and communication module) and S&C SpeedNet™ Radio, as applicable. For these devices the first paragraph of said warranty is 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 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 that the equipment has been stored, installed, operated, inspected, 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 the seller’s option) by shipment of necessary replacement parts.

Replacement control groups and S&C SpeedNet Radios provided by the seller or repairs performed by the seller under the warranty for the original equipment will be covered by the above special warranty provision for its duration. Replacement control groups and S&C SpeedNet Radios purchased separately will be covered by the above special warranty provision.

This warranty does not apply to major components not of S&C manufacture, such as batteries and communication devices, as well as hardware, software, resolution of protocol-related matters, and notification of upgrades or fixes for those devices. However, S&C will assign to the immediate purchaser or end user all manufacturers’ warranties that apply to such major components.

Use the Latest LinkStart Software Revision

Install the latest IntelliRupter fault interrupter software on your computer—available at: [sandc.com/en/support/sc-customer-portal/](http://sandc.com/en/support/sc-customer-portal/). The installation will provide the latest version of LinkStart Software. If LinkStart encounters earlier software on a Wi-Fi card, it will require an automatic software update and then proceed with any Wi-Fi tasks.

## Understanding Safety-Alert Messages

Several types of safety-alert messages may appear throughout this instruction sheet and on labels attached to the IntelliRupter fault interrupter. Familiarize yourself 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 you do not understand any portion of this instruction sheet and need assistance, 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 S&C Headquarters at (773) 338-1000; in Canada, call S&C Electric Canada Ltd. at (416) 249-9171.

### **NOTICE**

Read this instruction sheet thoroughly and carefully before installing or operating your S&C IntelliRupter fault interrupter.



## Replacement Instructions and Labels

If in need of additional copies of this instruction sheet, 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 your nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

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 IntelliRupter 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, like 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 that 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: \Documents and Settings\All Users\Application Data\S&C Electric\LinkStart\ for Windows® XP and at \Users\Public\Documents\S&C Electric\LinkStart for Windows 7. 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 backup 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 which 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 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 using 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 the 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 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 by 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.

If the key names for the two master keys are IntelliRupter master key: “MasterIR” and mobile master key: “MasterLT,” the Security Key Manager will require the files **MasterIR.pri** and **MasterLT.pub** both 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 31 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 for Windows 7. The default folder for Windows XP is C:\Documents and Settings\All Users\Application Data\S&C Electric\LinkStart\ and for Windows 7 it 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.

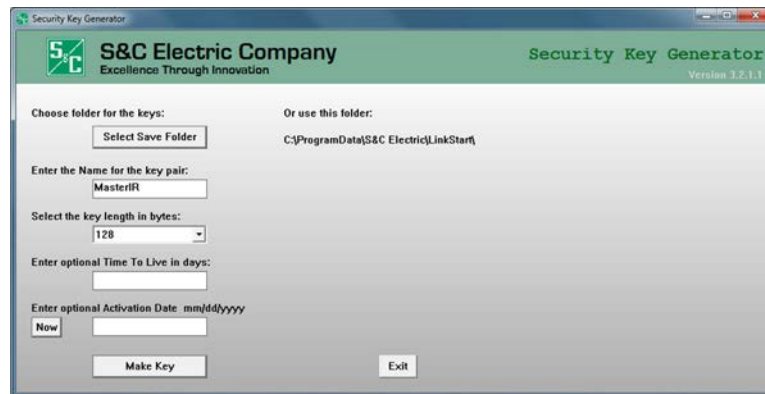


Figure 1. The Security Key Generator screen.

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, second 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 31, “MasterIR” will be used as the device master key and “MasterLT” 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.

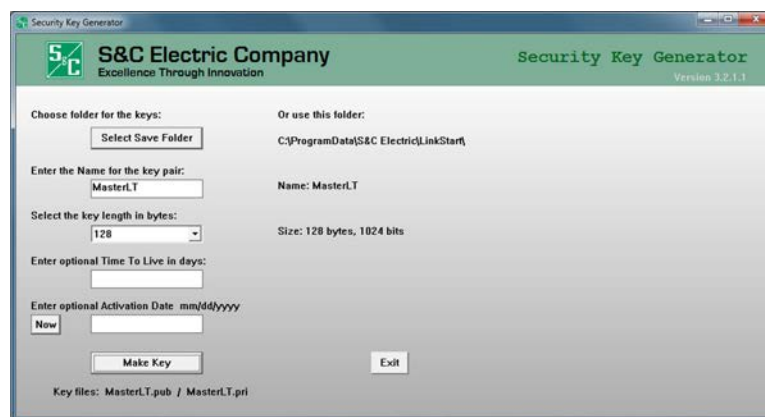


Figure 2. Selecting key-length options and the key name.

Repeat this process for the second key name. Now the key files, four of them, 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 LinkStart folder on the database PC.



## NOTICE

Each time a key is generated it 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 names selected for each region. See Figure 3.

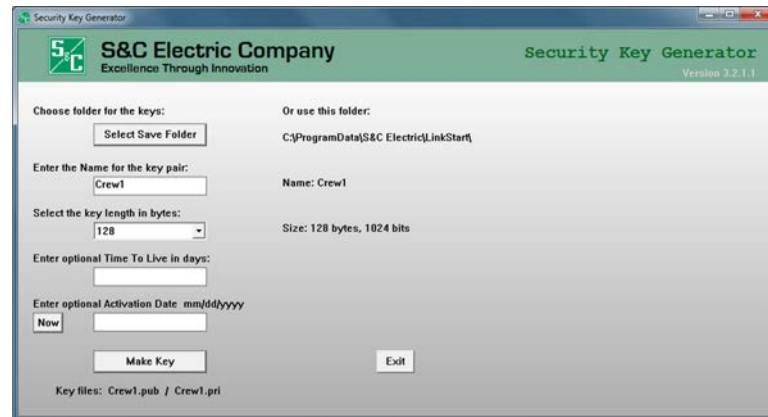


Figure 3. Selecting a name for each crew.

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

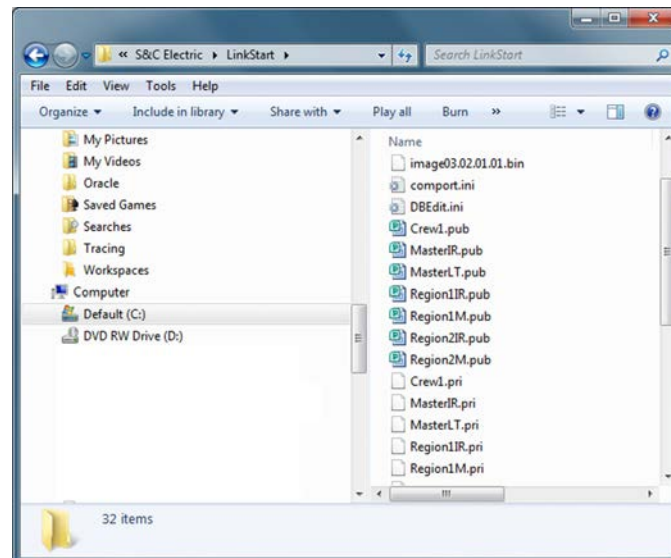


Figure 4. The key files are stored in the LinkStart folder.

The Security Key Manager can create crew keys that will be activated at first use and last for a set number of days or that are 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 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 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 that LinkStart 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 tabs for **Devices**, **Regions**, **Crews**, and **Wi-Fi Module Access Credentials**. 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 *Wi-Fi Administration* screen of LinkStart. 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, the first time the Security Key Manager is run after installation.

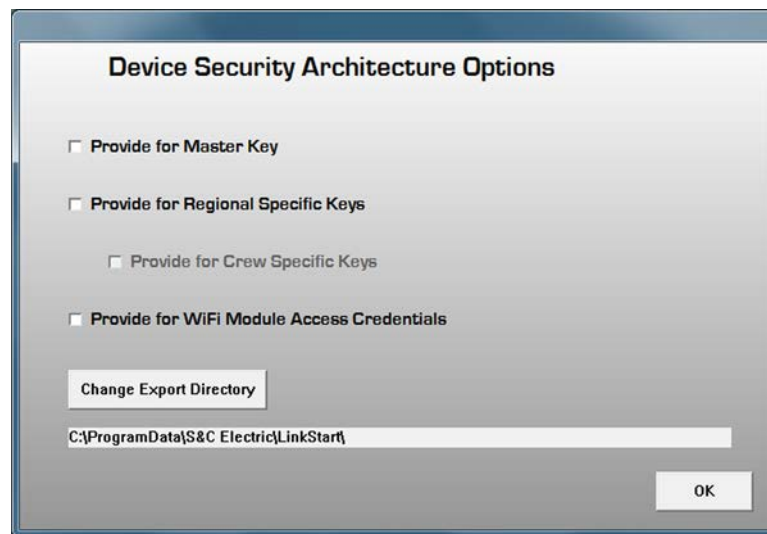


Figure 5. The *Device Security Architecture Options* screen.

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.

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.

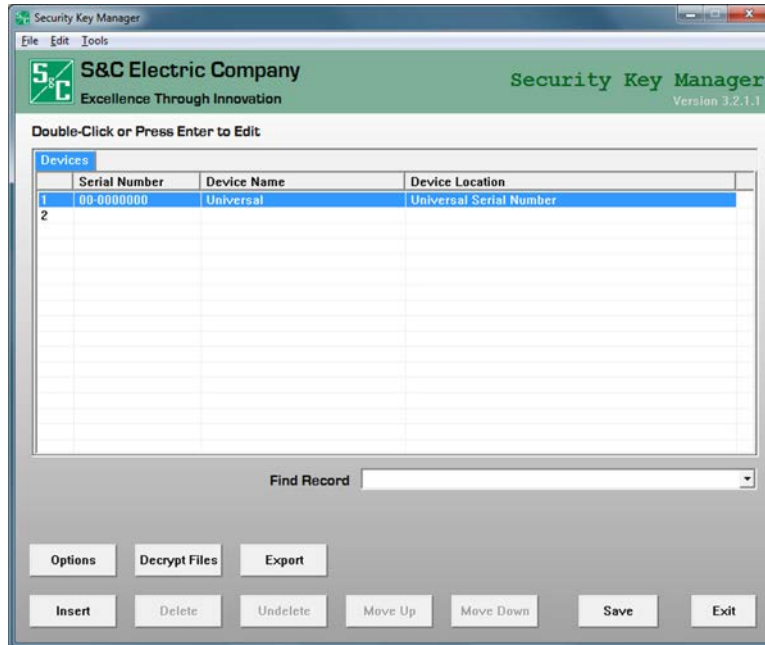


Figure 6. The *Security Key Manager* screen.

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.

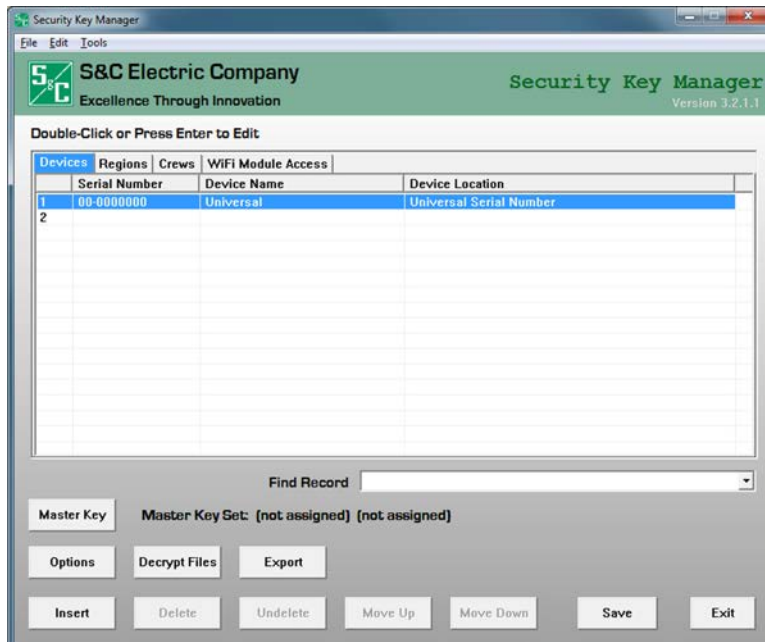


Figure 7. The *Security Key Manager* screen with the Options button.

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.



Figure 8. The Master Key Set dialog box.

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



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.

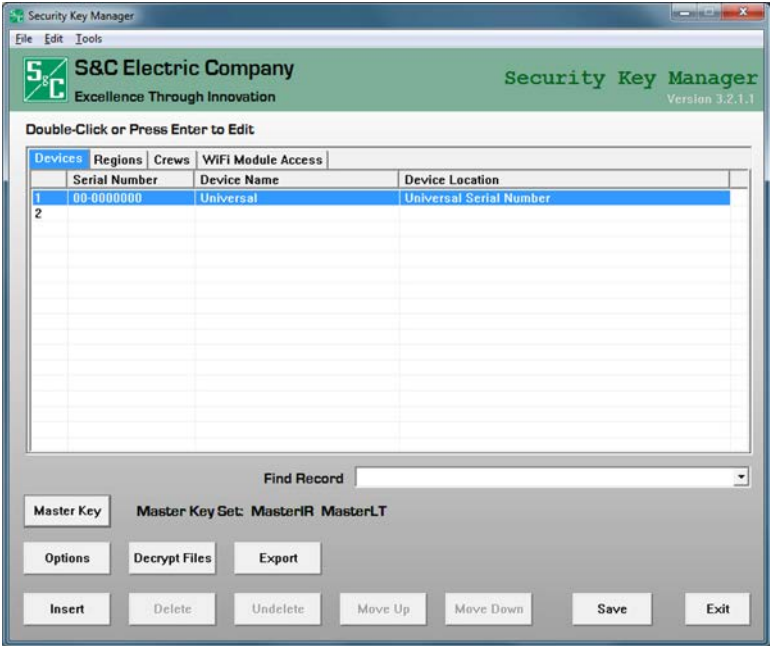


Figure 10. The *Security Key Manager* screen showing the Master Key Set names.

## 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 58 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.

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.

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.

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.

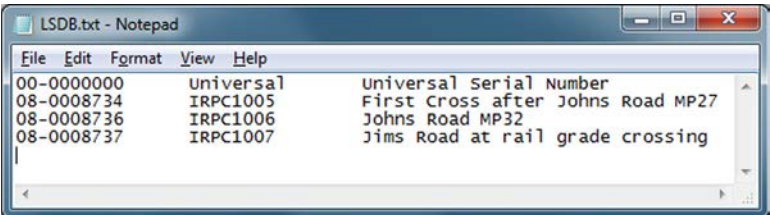


Figure 14. Entering data with the *Notepad* screen.

The text file can also be loaded by the Security Key Manager 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 instructions on page 58.

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.

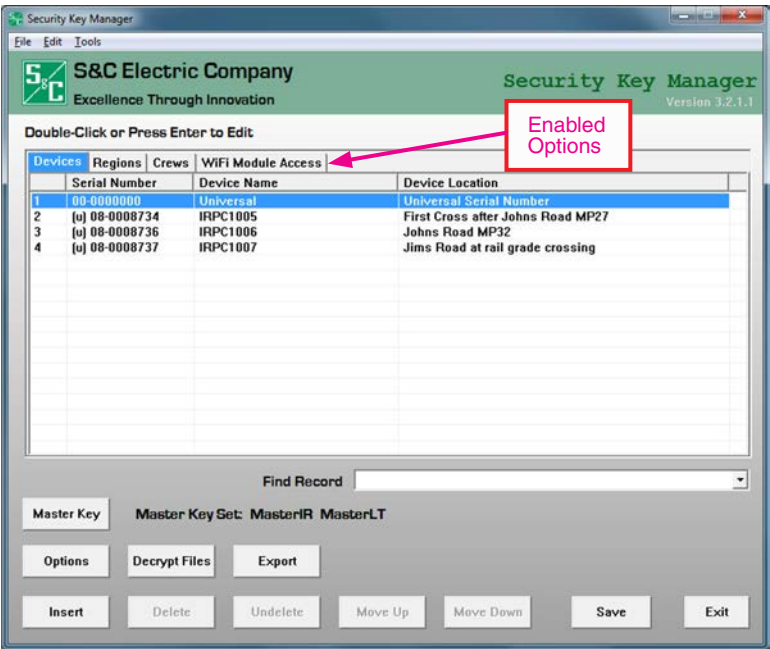


Figure 15. The feature tabs on the *Main Security Key Manager* screen.

## Navigation

**Tabbed List-Box Column Sort**—The columns will sort when the column header is clicked 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 clickable). 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 List View is sorted

**Move Down**—Disabled if the “Universal Record” is selected, the bottom-most 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:

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

<b>Edit Item</b>	<b>Insert Item</b>
<b>Delete Item</b>	<b>Undelete</b>
<b>Move Up</b>	<b>Move Down</b>

**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 shown in Figure 16 will appear explaining the consequences.

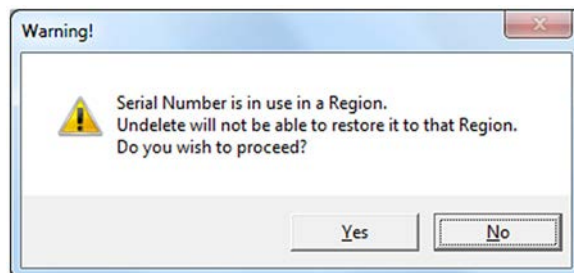


Figure 16. The Serial Number Used In A Region warning dialog box.

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.

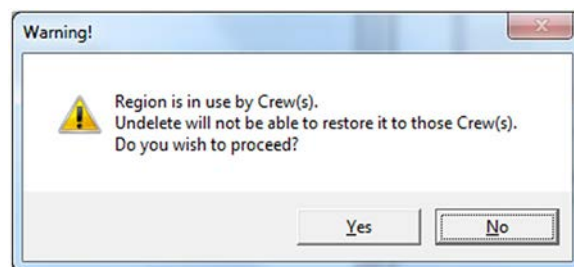


Figure 17. The Region Is Used By Crews warning dialog box.



## 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.

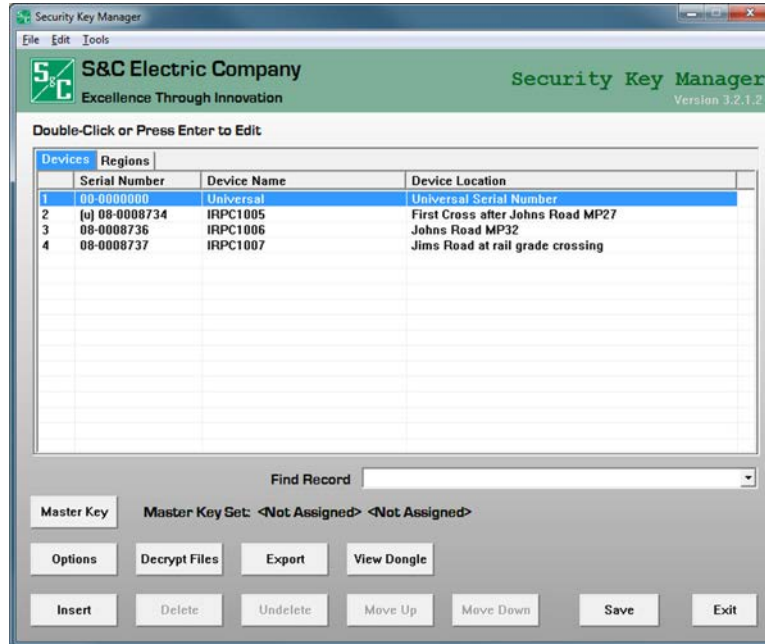


Figure 18. The Main Security Key Manager screen.

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.

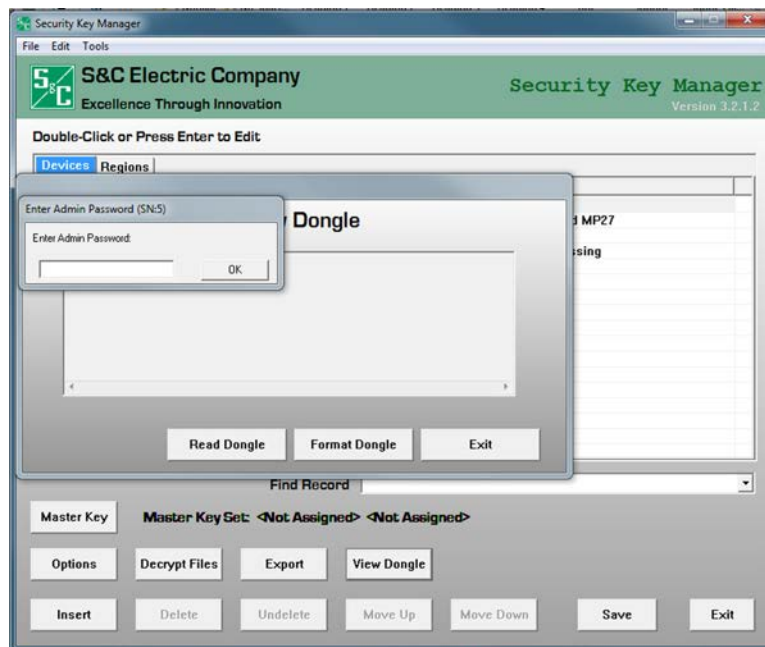


Figure 19. The Password dialog box to view dongle contents.

### Formatting a Dongle

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

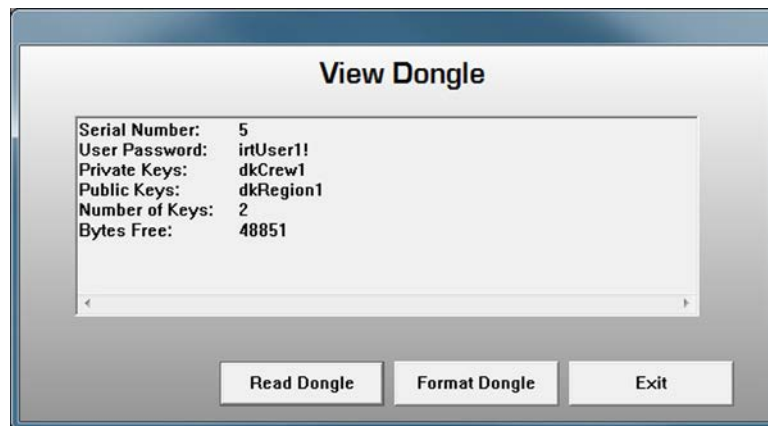


Figure 20. The View Dongle dialog box.

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

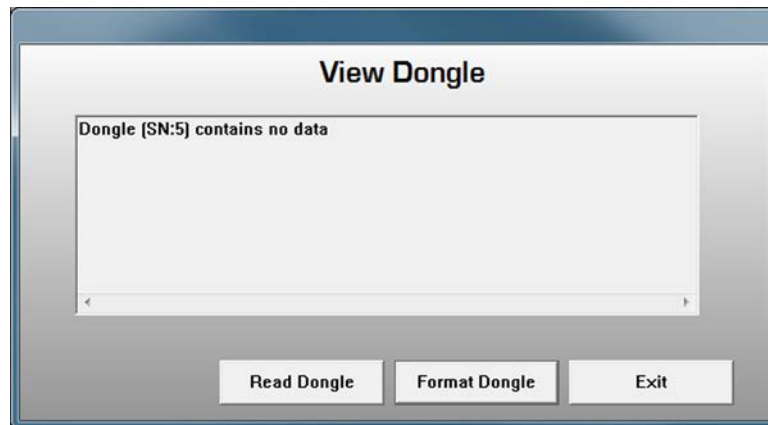


Figure 21. The View Dongle dialog box when the dongle is blank.

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.



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

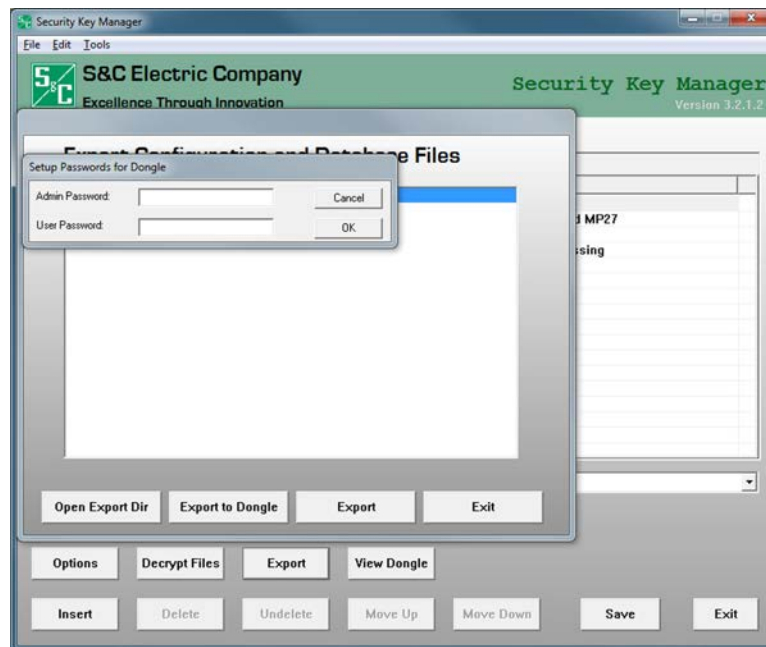


Figure 23. The Setup Passwords for Dongle dialog box.

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

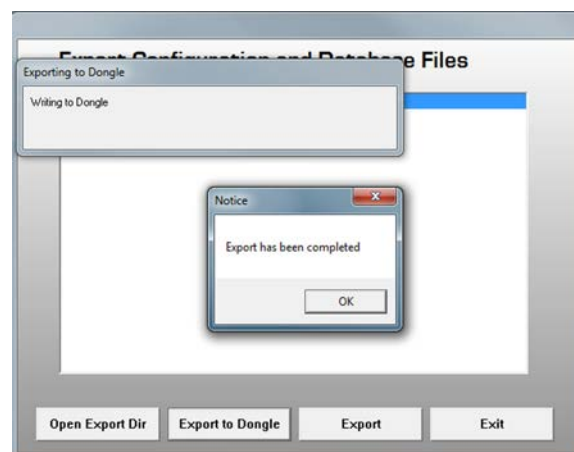


Figure 24. The Notice dialog box.

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.

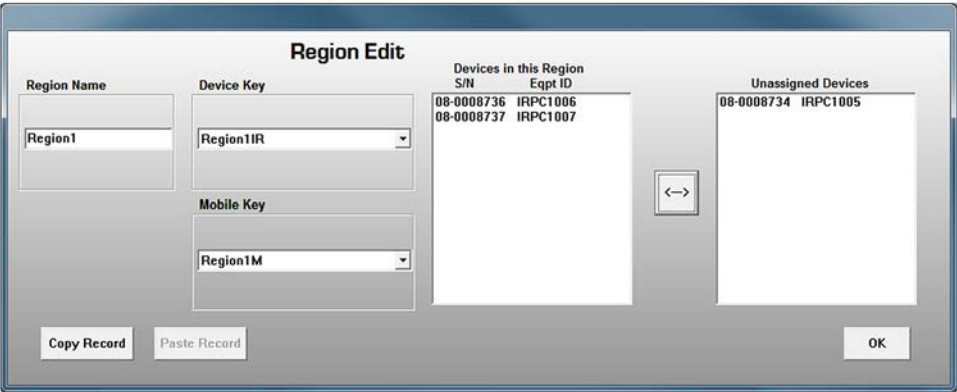


Figure 25. The Region Edit dialog box.

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 ↔ button. After assignment 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 ↔ 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.

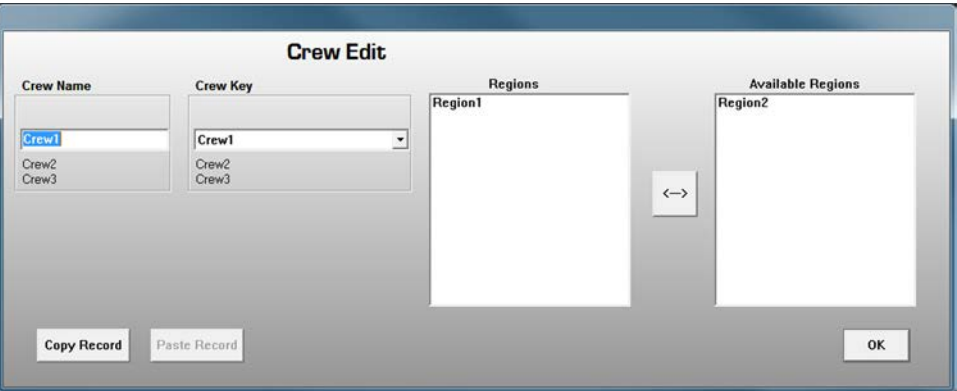


Figure 26. The Crew Edit dialog box.

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 configured. Alternatively, each IntelliRupter Wi-Fi module can be loaded with a unique configuration file, based on that specific IntelliRupter serial number. If this approach is used, each device in the database will have a unique configuration setting file. When using regions, or regions with crews, 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.



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.

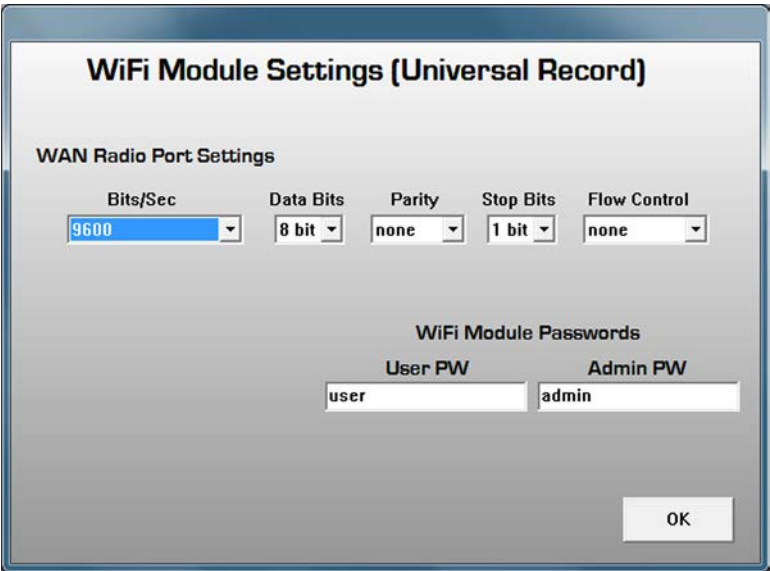


Figure 28. The Wi-Fi Module Settings (Universal Record) dialog box.

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.

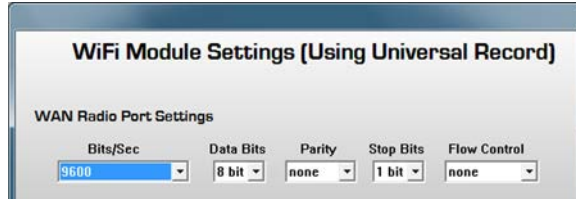


Figure 29. The Wi-Fi Module Settings (Using Universal Record) dialog box.

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.

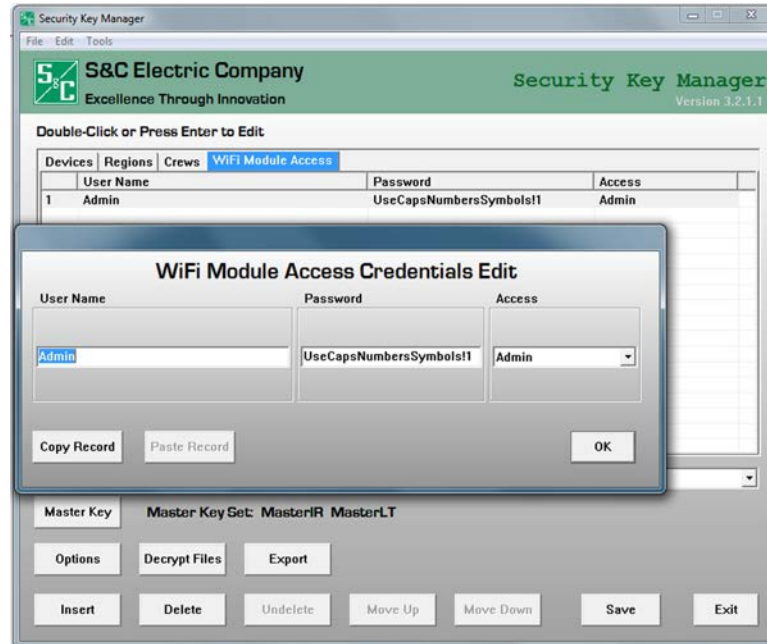


Figure 30. The Wi-Fi Module Access Credentials Edit dialog box.

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 what options are 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**.

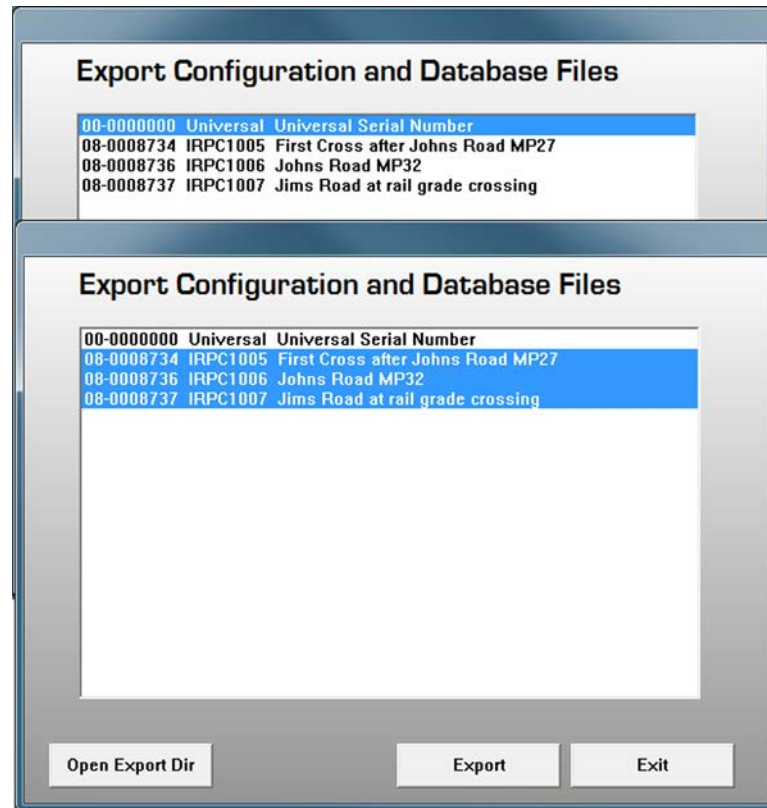


Figure 31. The Export Configuration and Database Files dialog box.

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.

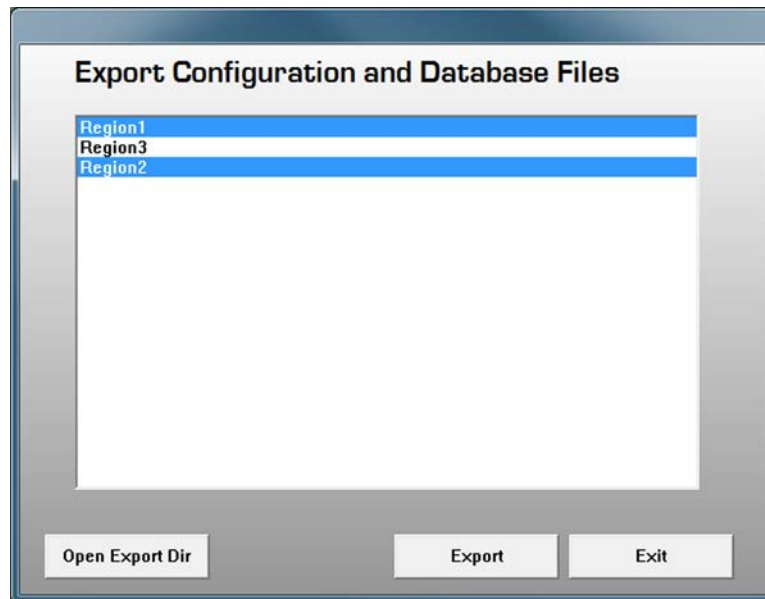


Figure 32. Selecting non-consecutive entries.

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.

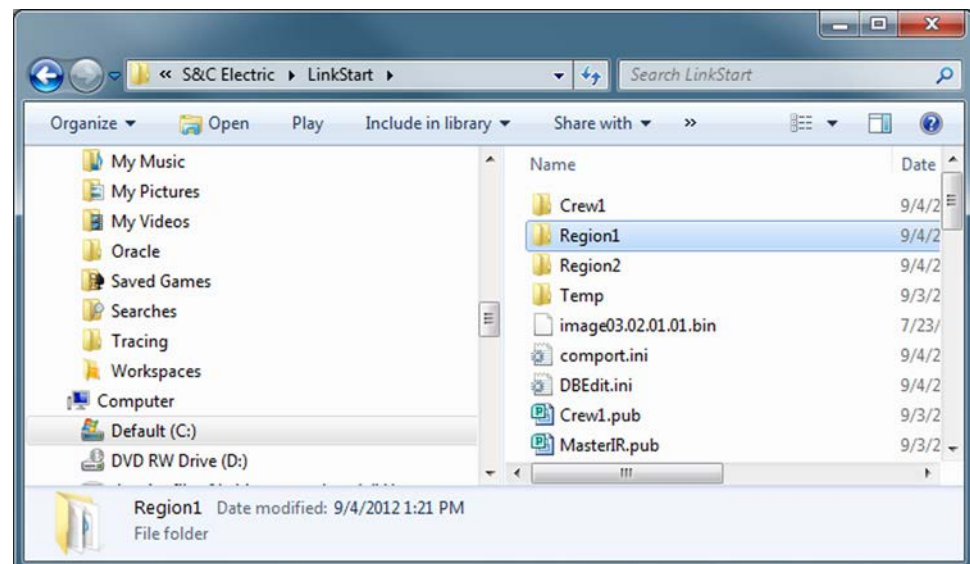


Figure 33. The *LinkStart* folder.

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.

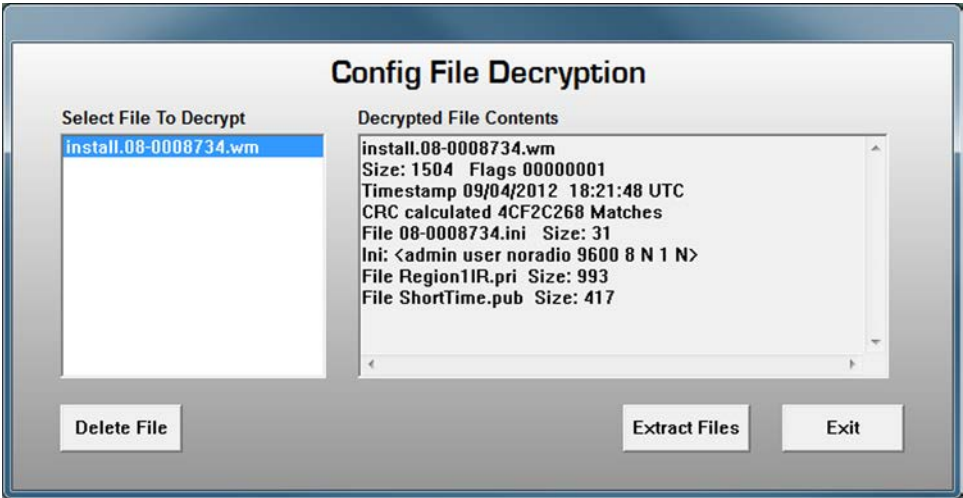


Figure 34. The Config File Decryption dialog box.

## Connecting to an IntelliRupter Fault Interrupter

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.

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

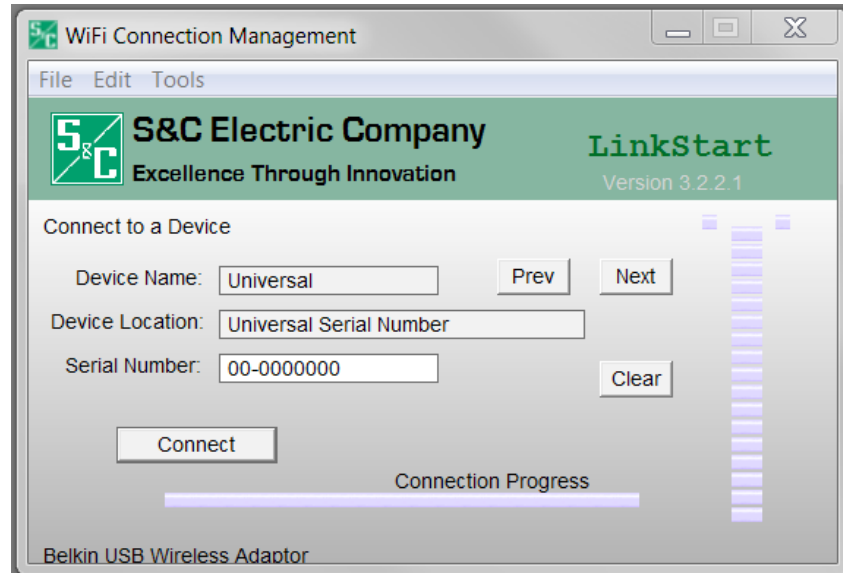


Figure 35. The Wi-Fi Connection Management dialog box.

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

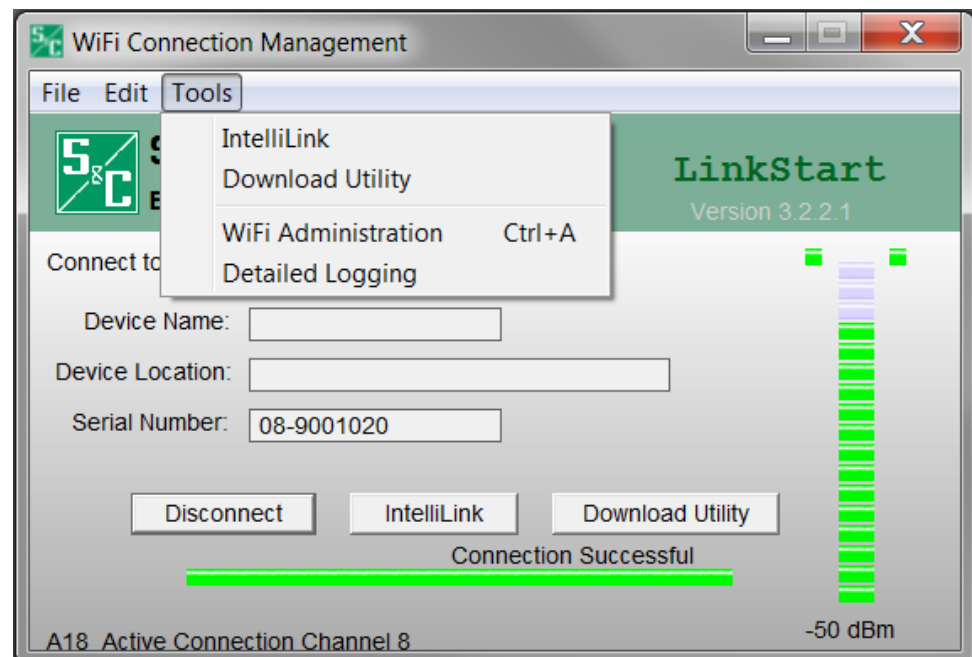


Figure 36. The Tools option and the Wi-Fi Administration selection.

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

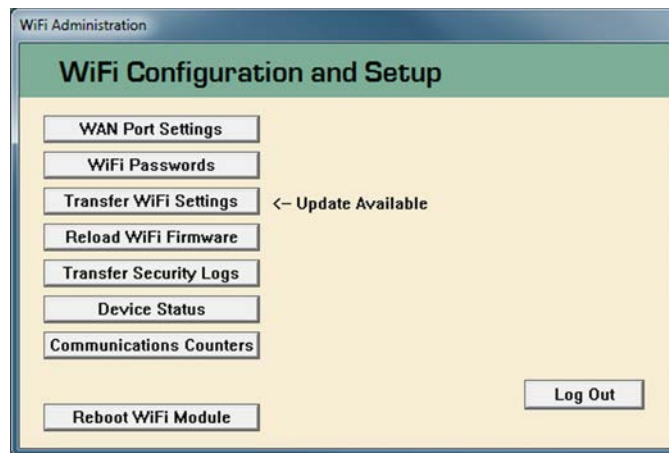


Figure 37. The Wi-Fi Configuration Setup Dialog Box.

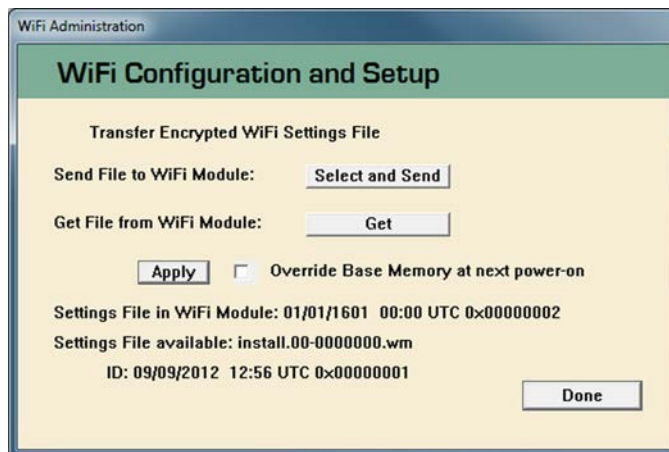


Figure 38. The Wi-Fi Configuration Setup dialog box after clicking on the **Transfer Wi-Fi Settings** button.

Notice that **install.00-0000000.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-XXXXXXX.wd**, where XX-XXXXXXX = 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.

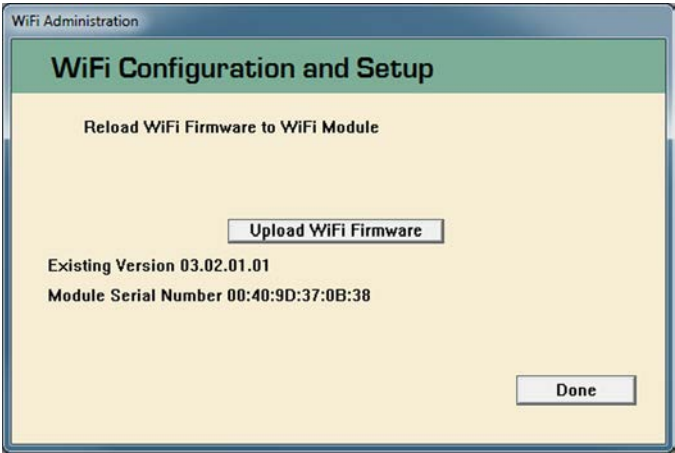


Figure 39. The Upload Wi-Fi Firmware button on the Wi-Fi Administration dialog box.

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.

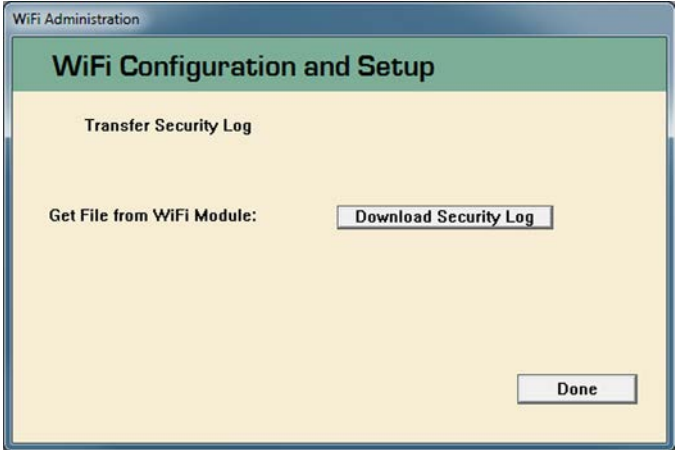


Figure 40. The Download Security Log button on the Wi-Fi Administration dialog box.

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 **SecurityLog.<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 27.



**Table 1. Security Event Log Entries**

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 establishment.
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.

### 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.

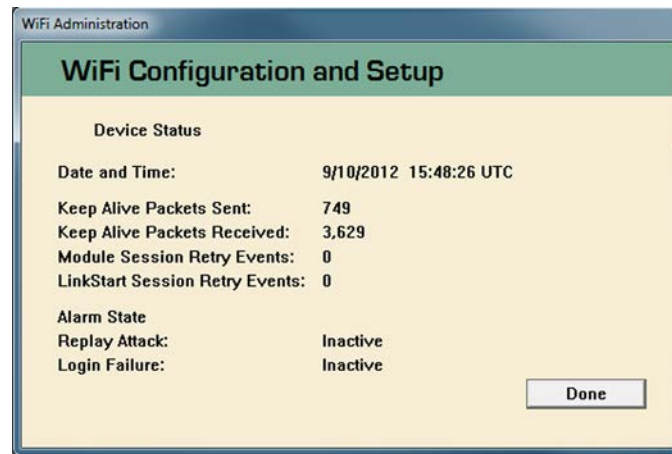


Figure 41. The Device Status dialog box.

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 LinkStart 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.

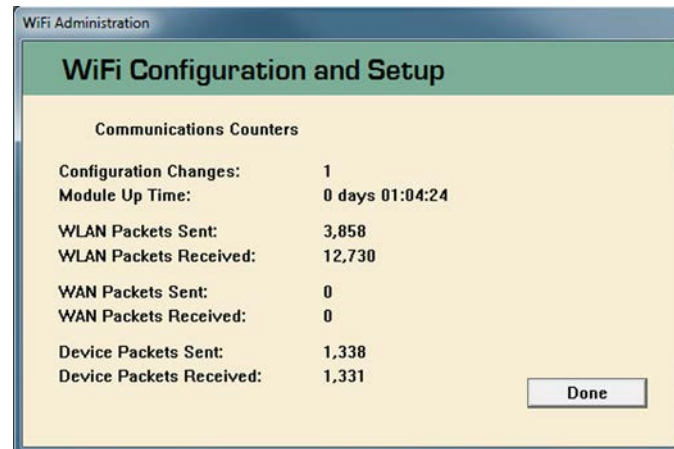


Figure 42. The Communications Counters dialog box.

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.

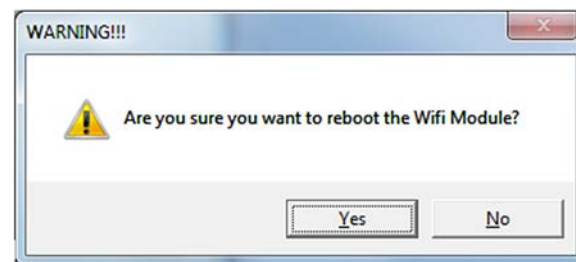


Figure 43. The Reboot Wi-Fi Module dialog box.

### 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.

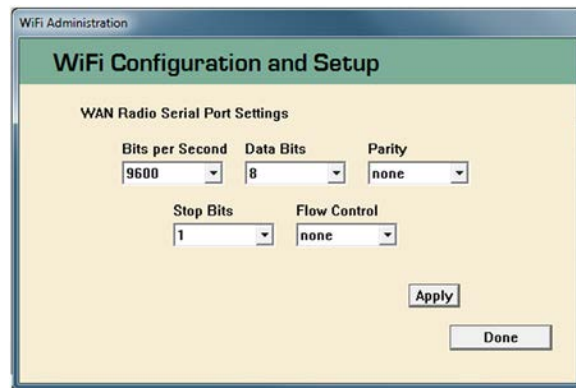


Figure 44. The WAN Radio Serial Port Settings dialog box.

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 adaptor to communicate with the IntelliRupter fault interrupter control modules. Optionally, a security dongle is required to deploy the security keys on the user PC.

## Software Installation

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 higher is required. The **IntelliRupter Screensets**, **LinkStart**, and **Wi-Fi Module Firmware** options must be checked. See Figure 45.

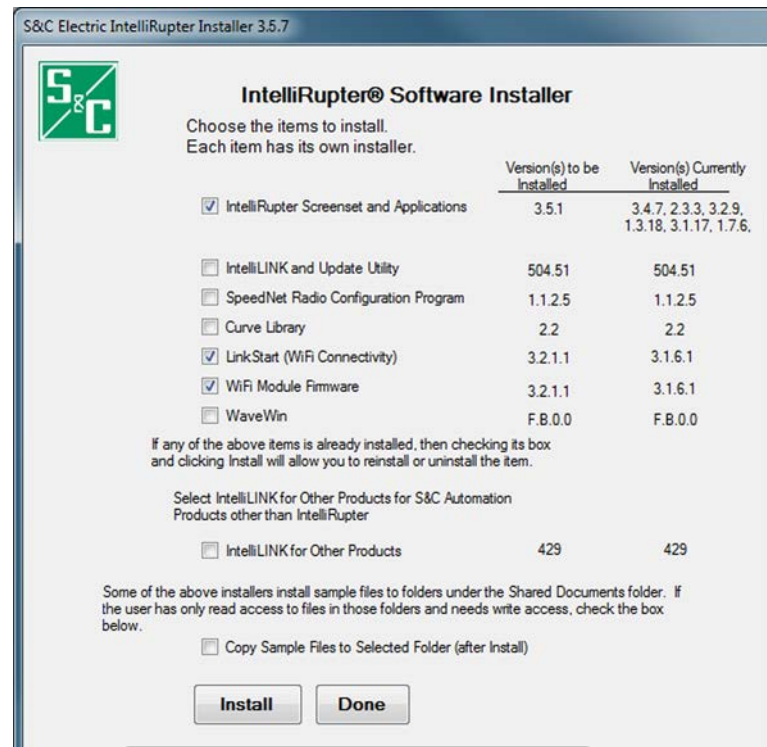


Figure 45. The IntelliRupter Software Installer dialog box.

If necessary, upgrade the Wi-Fi module firmware to version 3.2.0.0 or higher 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.

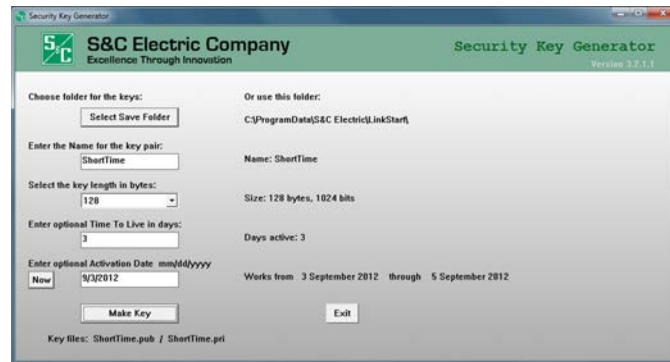


Figure 46. The Security Key Generator dialog box.

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 entered, 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 XP the folder is C:\Documents and Settings\All Users\Application Data\S&C Electric\LinkStart\, and for Windows 7 it is \ProgramData\S&C Electric\LinkStart\. See Figure 47.

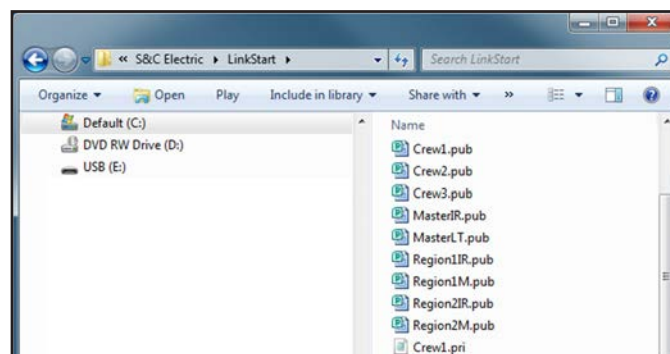


Figure 47. The LinkStart folder.





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

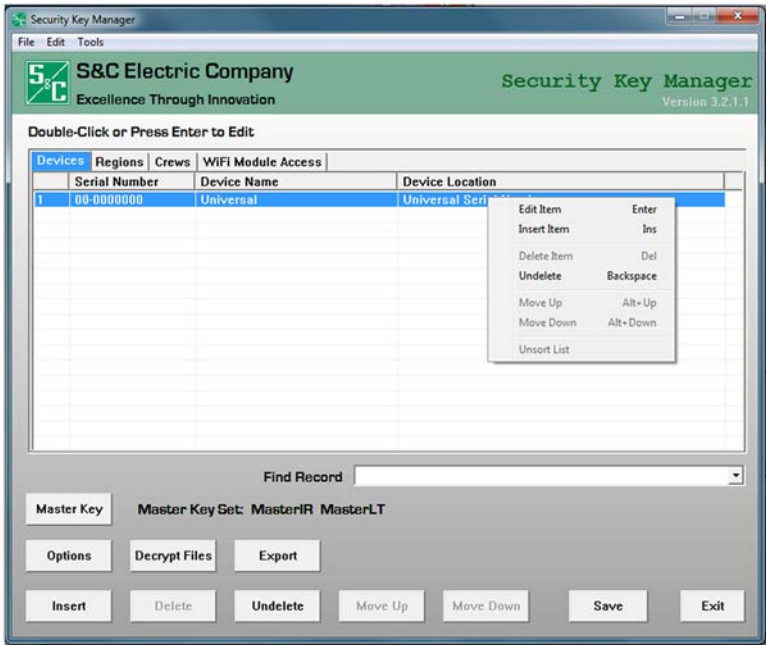


Figure 50. This menu opens when the universal serial number line is selected.

Click on the **Insert Item** option, enter the serial number for the first device, 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.

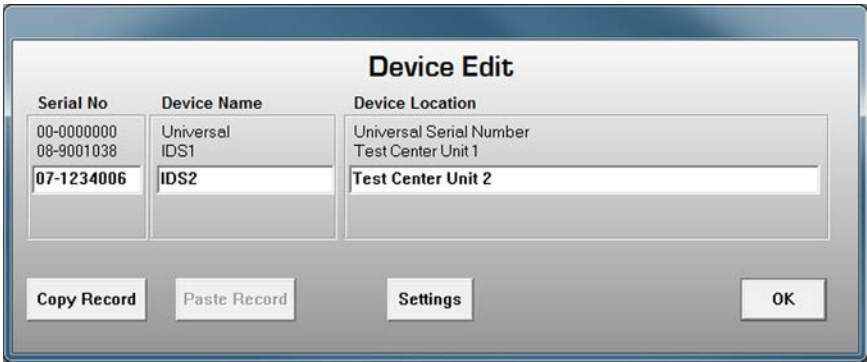


Figure 51. The Device Edit dialog box.

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 35.

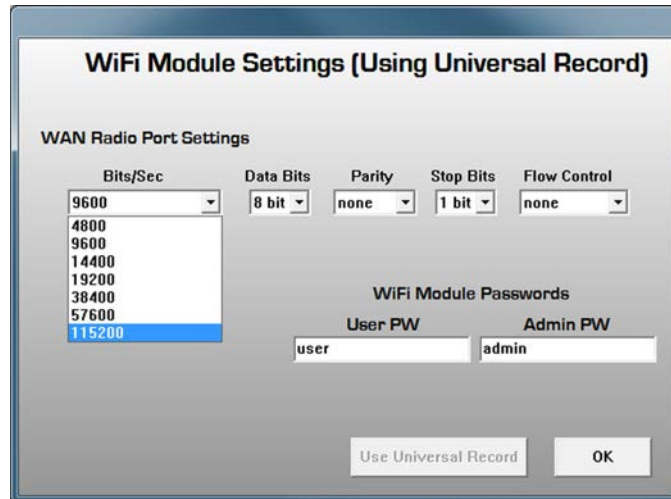


Figure 52. The WAN Radio Port Settings dialog box.

## 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.

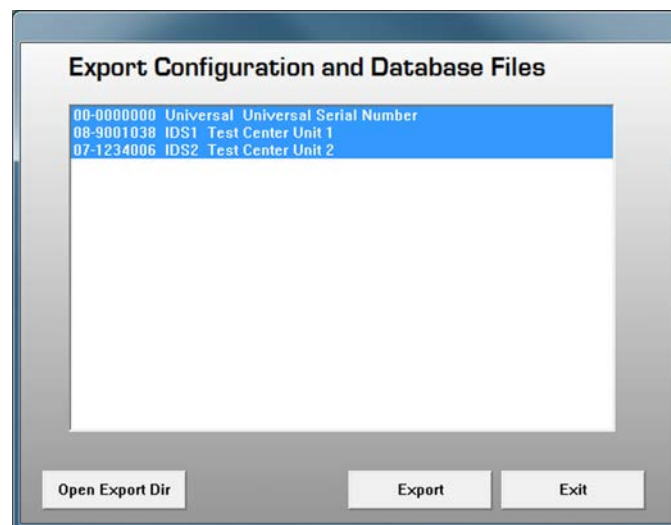


Figure 53. The Export Configuration and Database Files dialog box.

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.

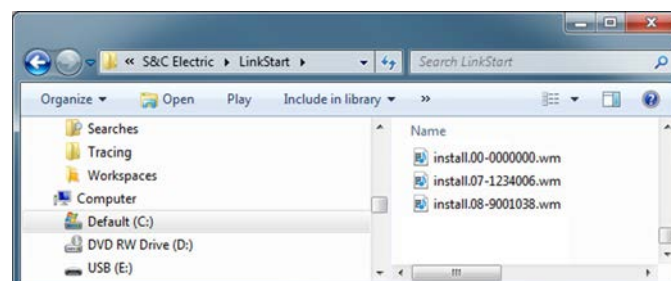


Figure 54. The *LinkStart* folder.

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.

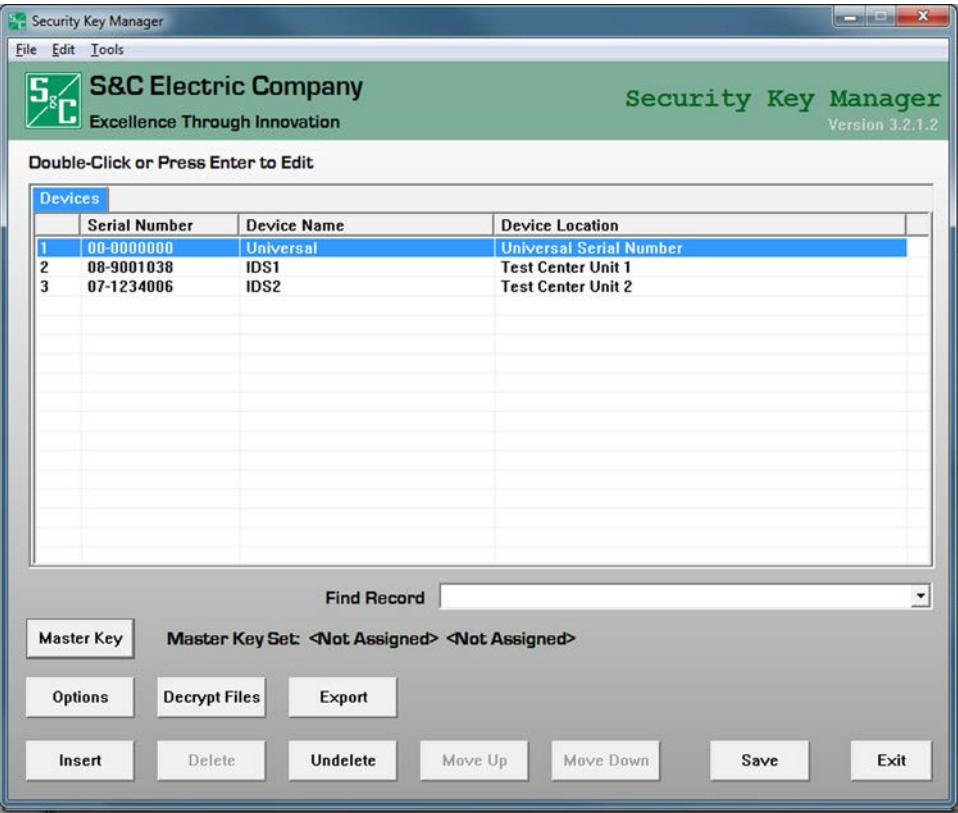
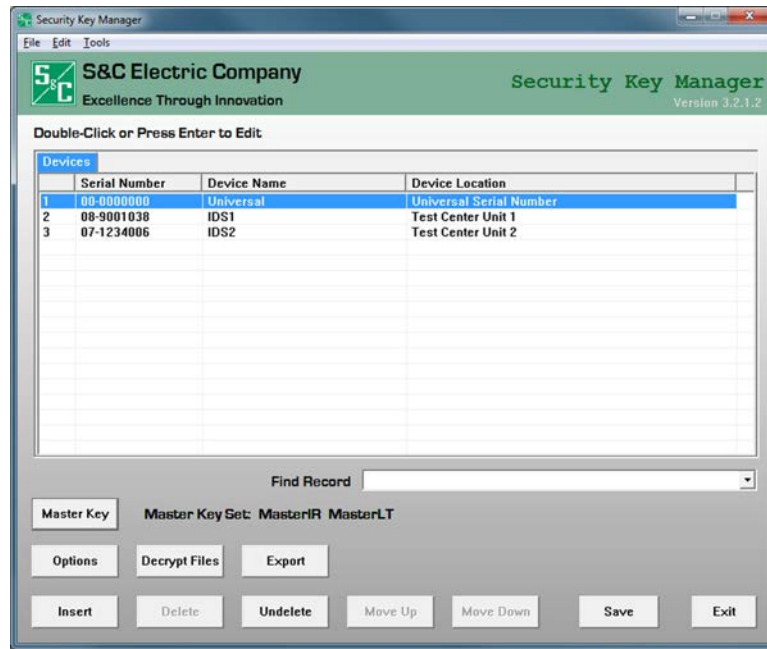


Figure 55. The *Security Key Manager* Main screen.

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.



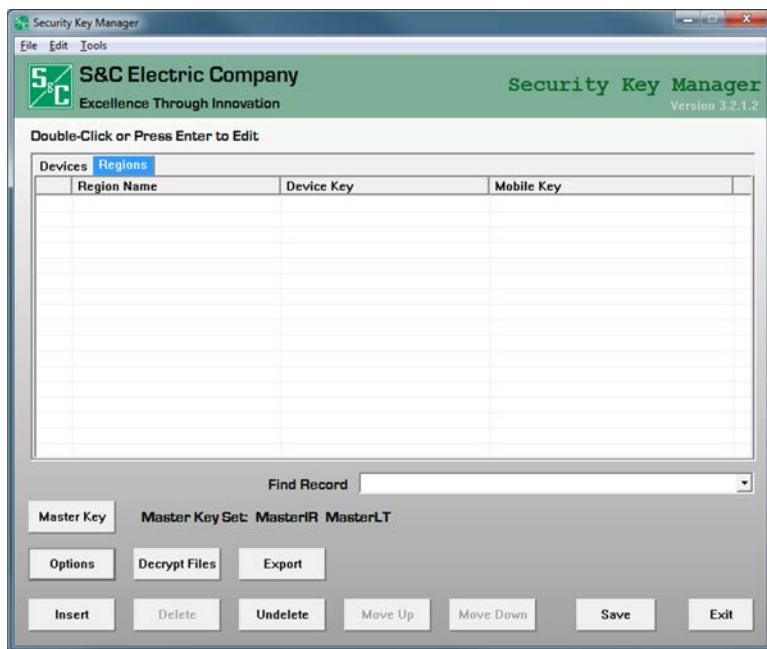
Figure 56. The Master Key Set dialog box.



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

Click on the **Options** button, check the Provide for Regional Specific Keys check box, and click on the **OK** button.

Then, click on the **Regions** tab followed by the **Insert** button on the *Main* screen. See Figure 58.



**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 ↔ 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.

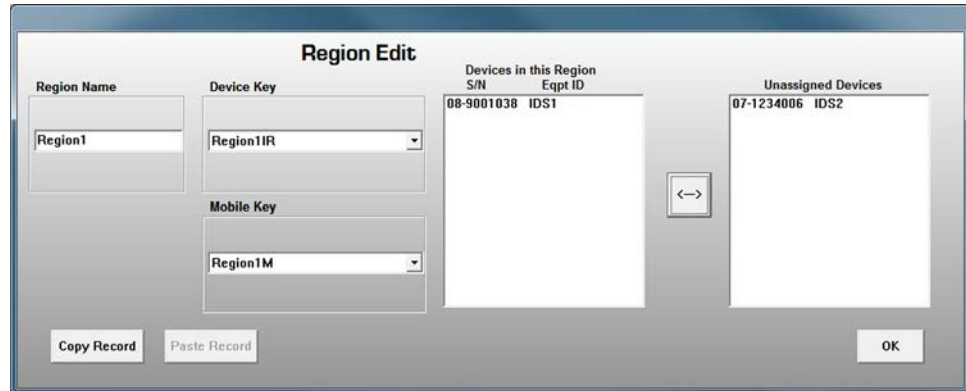


Figure 59. The Region Edit dialog box.

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.

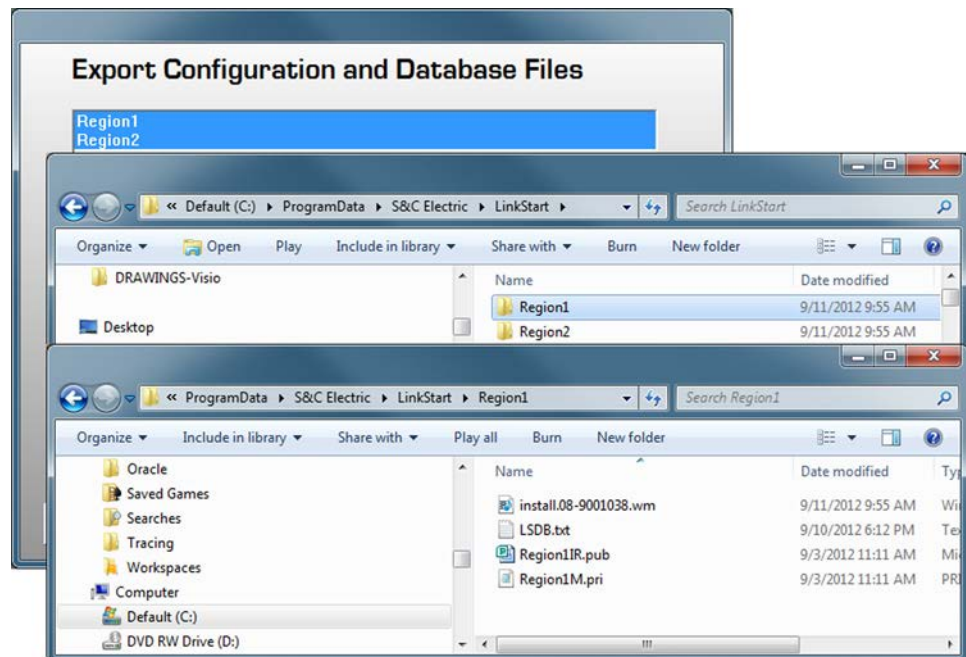


Figure 60. The LinkStart>Region1 folder contents.

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 that 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 **MasterLT.pri** key files and the **LSDB.txt** database file to the *LinkStart* folder of the target PC. See Figure 61.

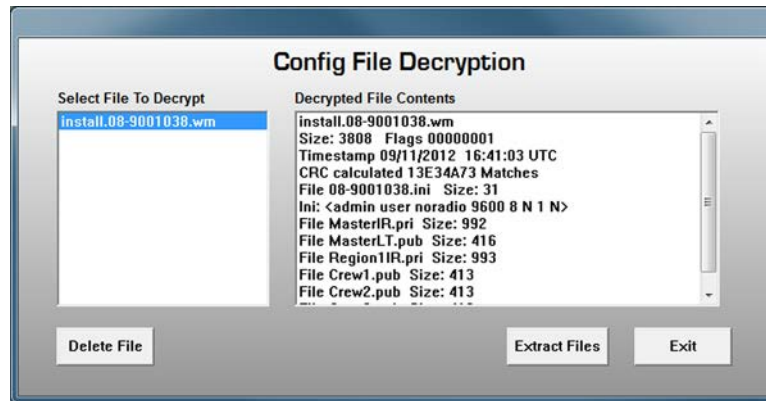


Figure 61. The Config File Decryption dialog box.

Click on the **Options** button on the *Main* screen and check the **Provide for Crew Specific Keys** check box. Leave 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 that 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.

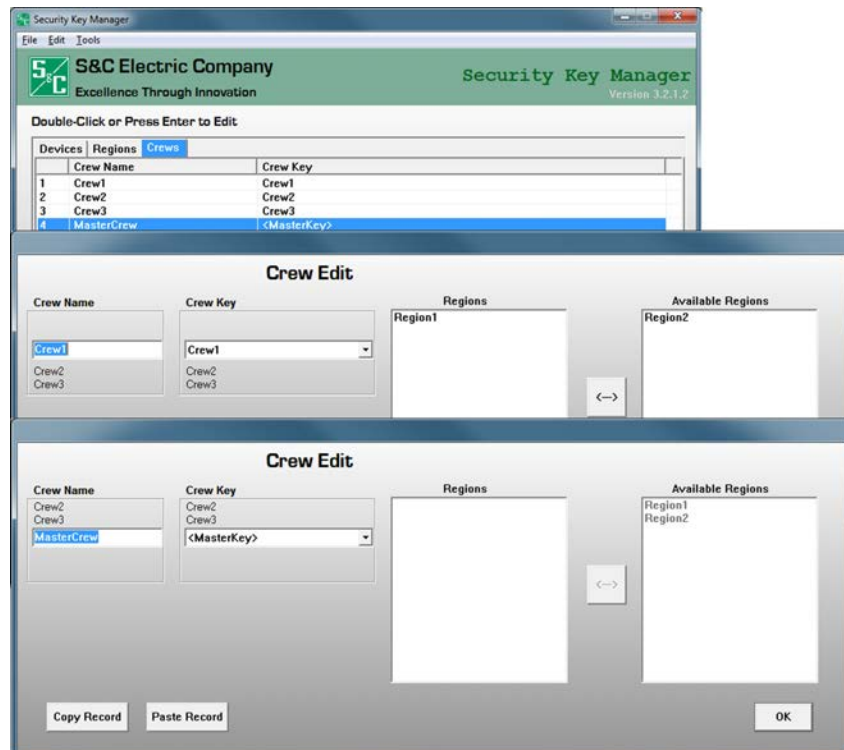


Figure 62 The Crew Edit dialog box.

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.

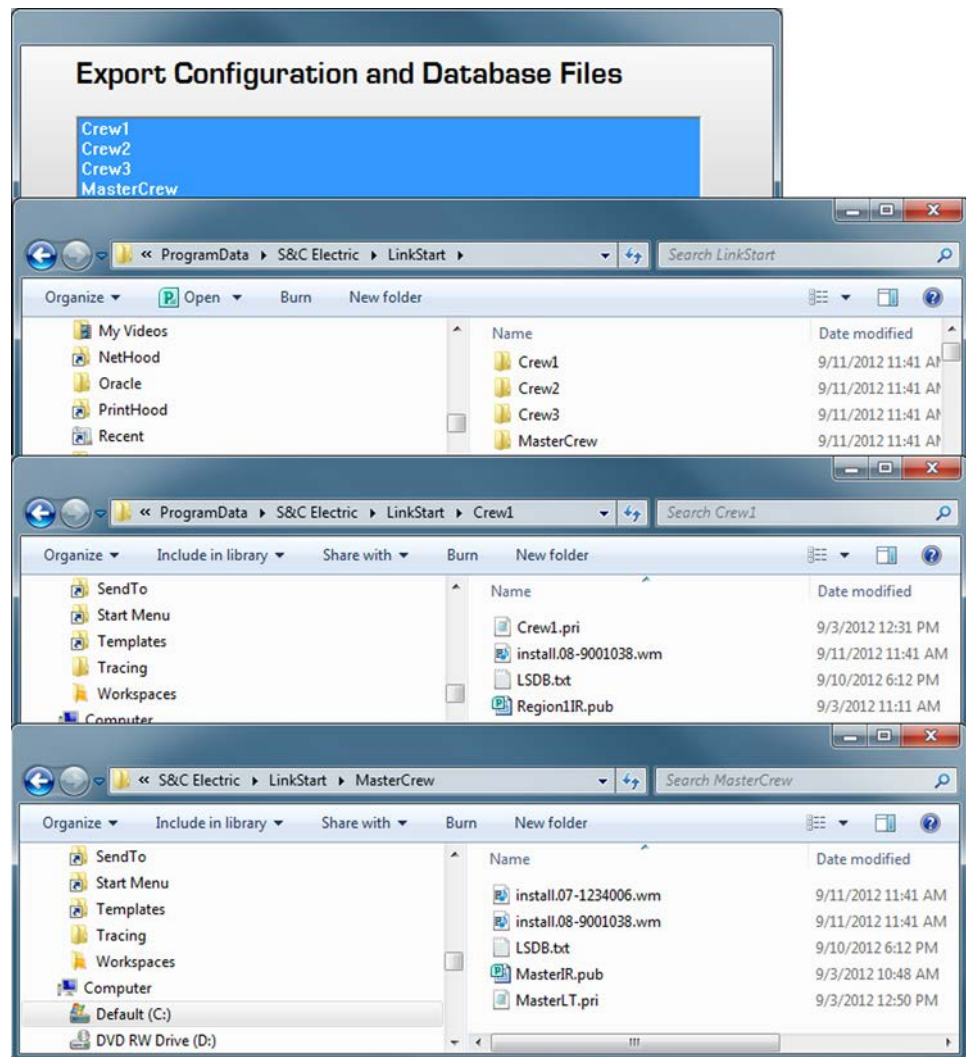


Figure 63. The expanded *LinkStart* folder.

The mastercrew 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 MasterCrew 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.

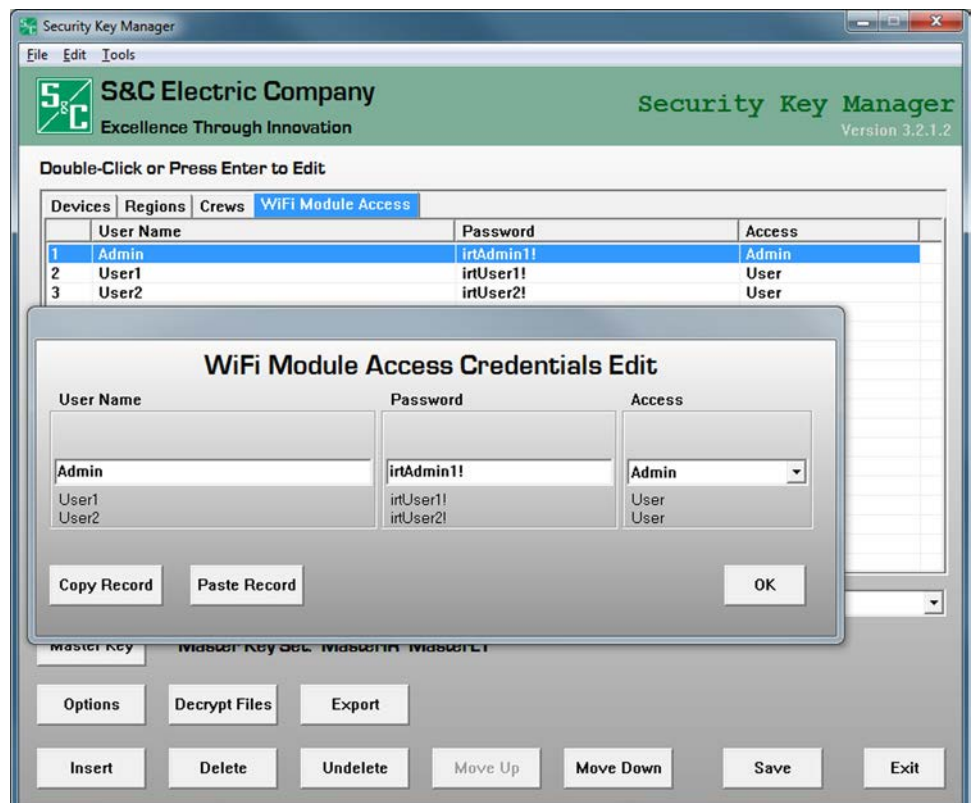


Figure 64. The Wi-Fi Module Access Credentials Edit dialog box.

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 that the **Wi-Fi Module Passwords** option is no longer available on the Wi-Fi Module Settings (Custom Settings) dialog box. See Figure 65.

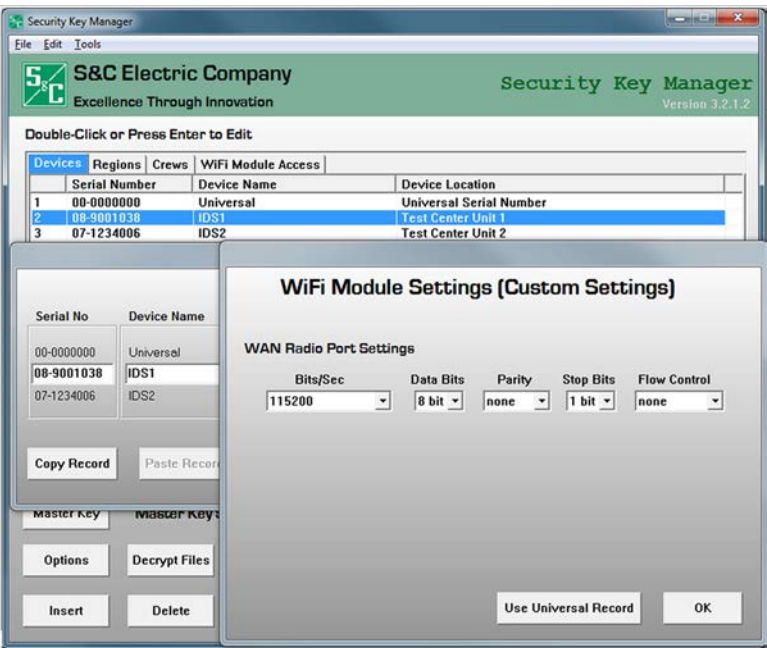


Figure 65. The Wi-Fi Module Settings (Custom Settings) dialog box.

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 that the first line below it contains file "MasterIR.pri Size:992." See Figure 66.

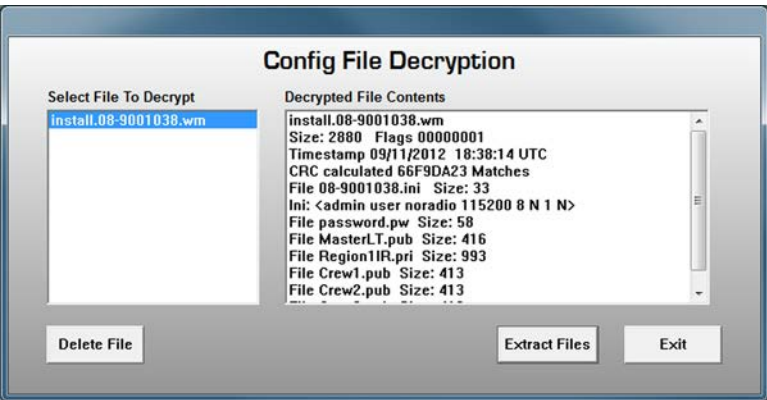


Figure 66. The Config File Decryption dialog box.

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 that the first file below the line beginning with “Ini:” now contains “File password.pw Size 58.” The password pw 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 thumb drive. See Figure 67.

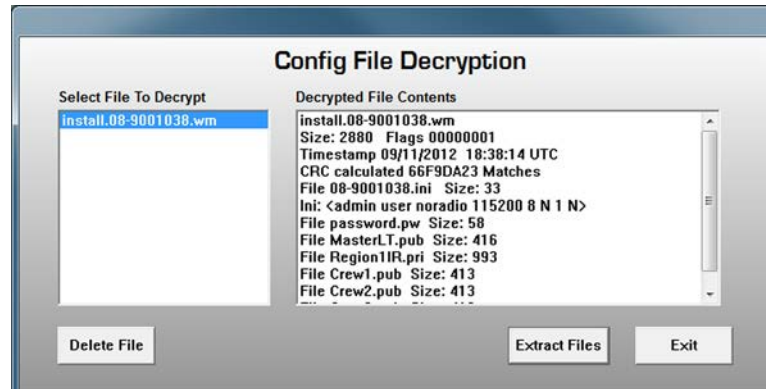


Figure 67. The Config File Decryption dialog box.

## 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 that 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. Reformating the dongle erases its contents and passwords, making it available for new data. See Figure 68.

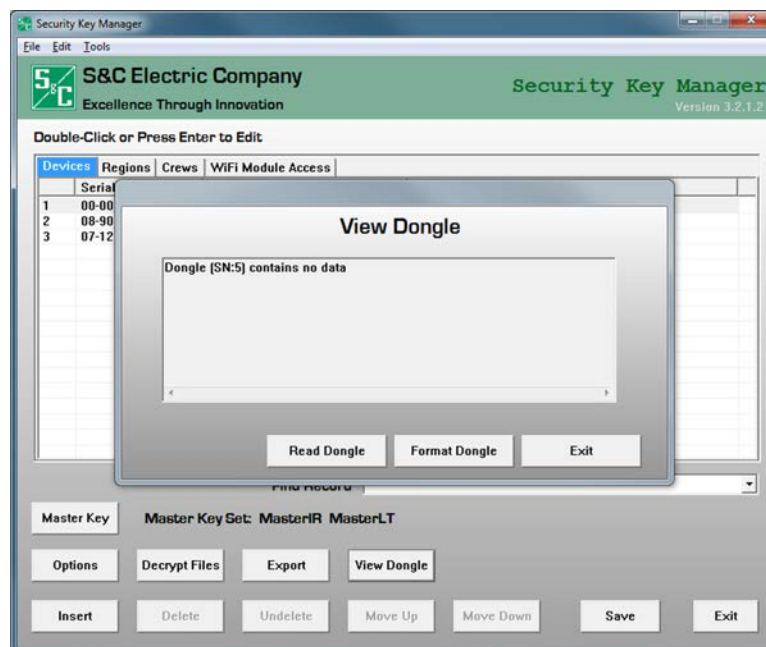


Figure 68. The View Dongle dialog box.



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.

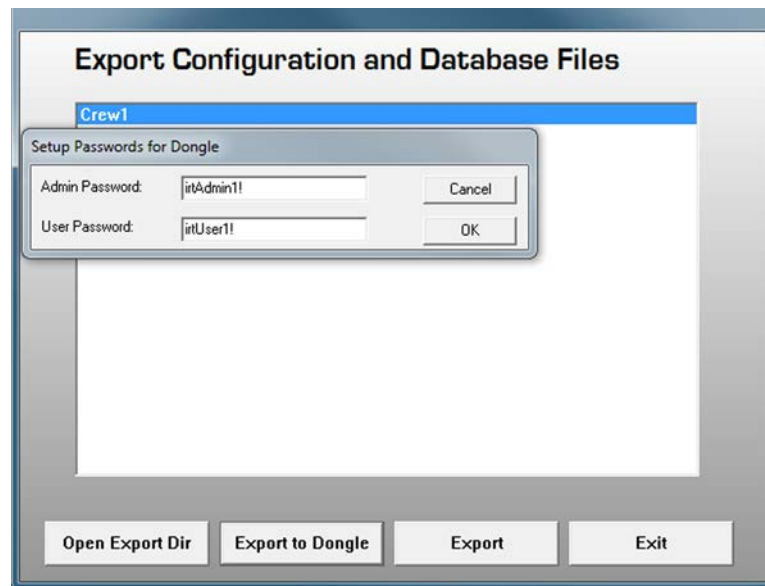


Figure 69. The Setup Passwords for Dongle dialog box.

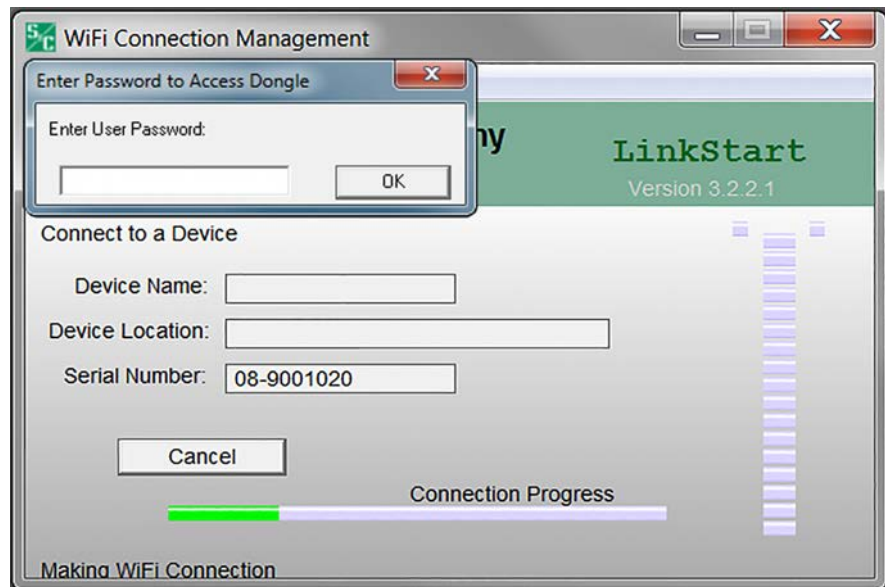
Exit the Export Configuration and Database Files dialog box, and click on the **View Dongle** button on the *Main* screen. Enter the admin password “irtAdmin1!,” when prompted, and the contents of the dongle will be displayed. See Figure 70.



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.



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

Now that the configuration files, corresponding keys, and the dongle are set up, IntelliRupter fault interrupters can be connected through the LinkStart program.

To use the keys, Wi-Fi firmware version 03.02.01.01 or higher 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 26, 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 that 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 that 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 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 \ProgramData\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.

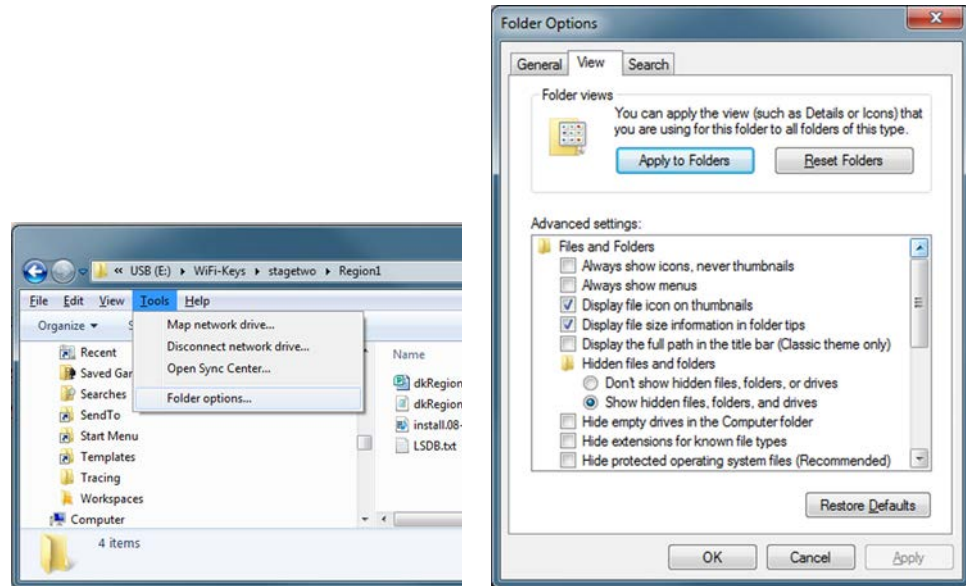


Figure 72. The Folder Options dialog box.

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.

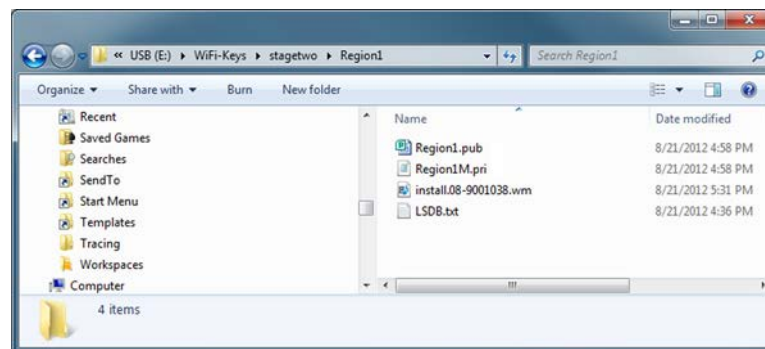


Figure 73. The Wi-Fi Key Generator screen.

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

Connect to the first IntelliRupter fault interrupter by launching the LinkStart program, select the **Tools** tab, and click on the **Wi-Fi Administration** option on the *LinkStart Main* screen. See Figure 74.

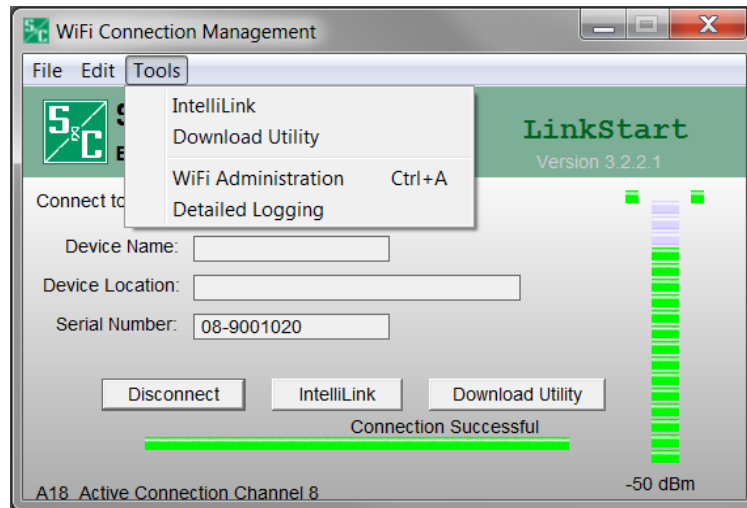


Figure 74. The *LinkStart Main* screen.

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.

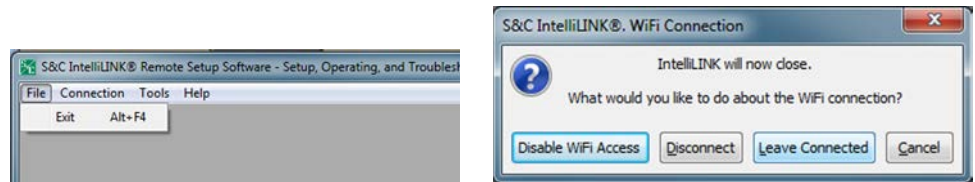


Figure 75. The IntelliLink will now close dialog box.

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. 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**.



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

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.

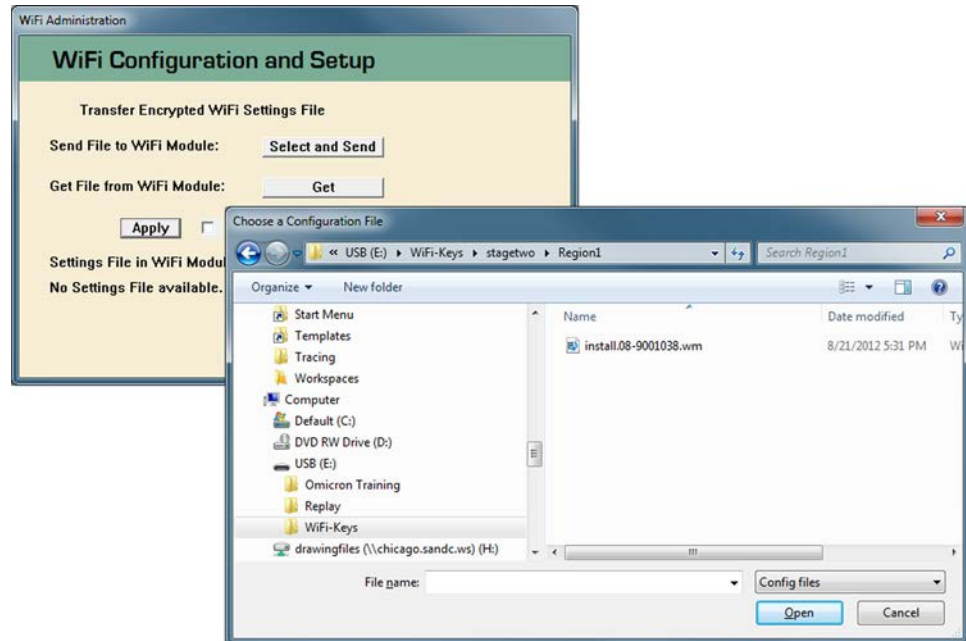


Figure 77. The Transfer Encrypted Wi-Fi Settings File dialog box.

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. 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.

Disconnect and exit the LinkStart program.

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.

Got to \Users\Public\Documents\S&C Electric\LinkStart for Windows 7 or \Documents and Settings\All Users\Documents\S&C Electric\LinkStart for Windows XP, 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.

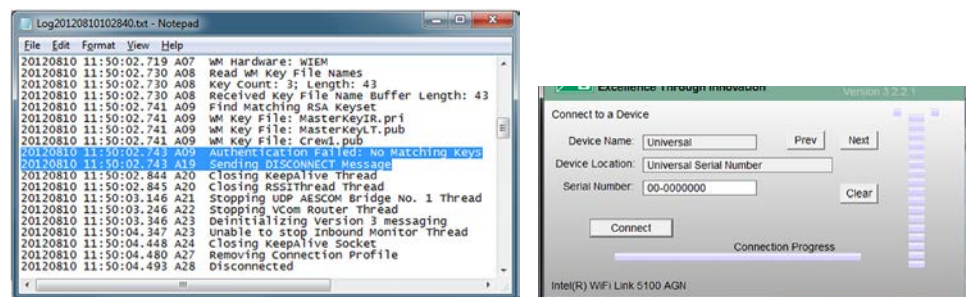


Figure 78. The Wi-Fi Connection Manager dialog box.

## 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.

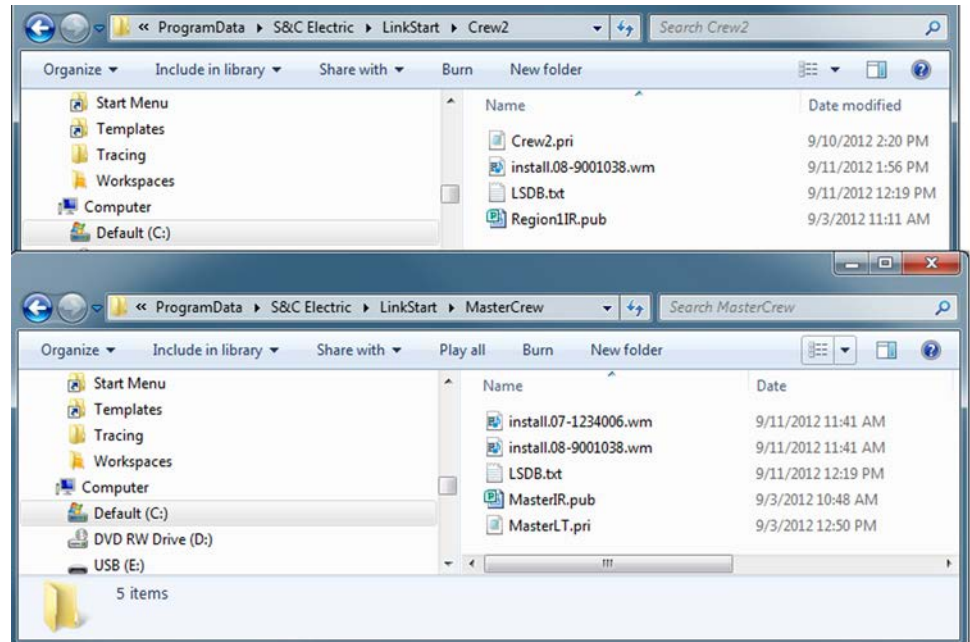


Figure 79. The Crew2 and MasterCrew folders.

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 AdminCrew 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.



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 that 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 to see that the credentials created above can be accessed. See Figure 81.

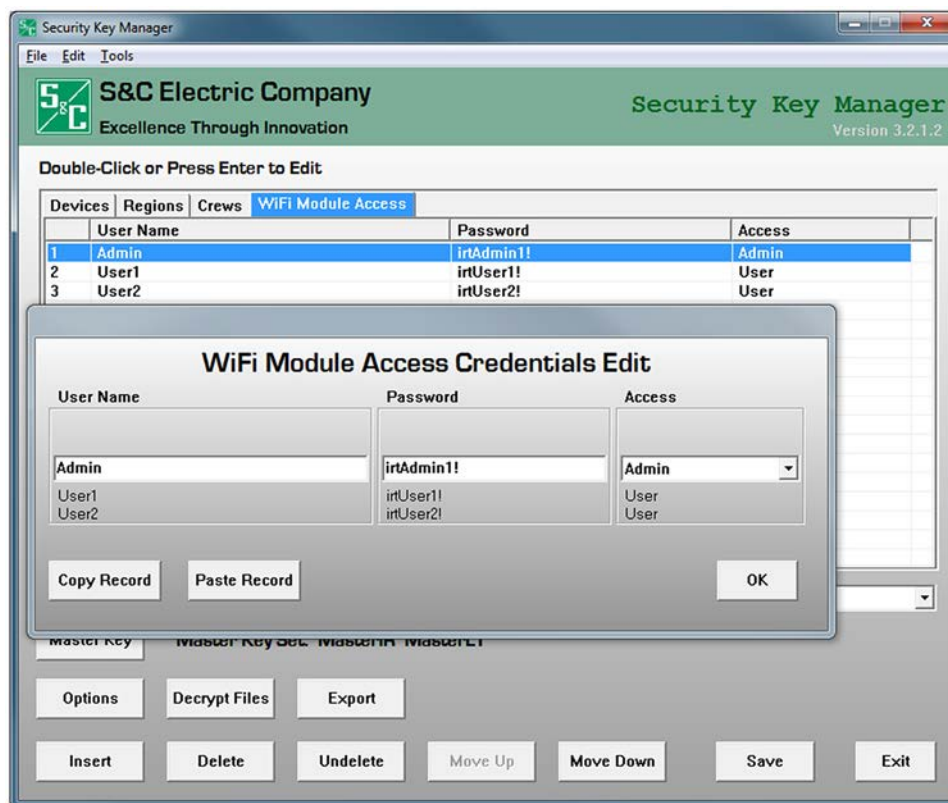


Figure 81. The Wi-Fi Module Access Credentials Edit dialog box.

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

Use the same re-keying approach discussed above, 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 that 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.





## Loading Wi-Fi Keys with IntelliLink Remote Setup Software

In the IntelliLink software menu, select Setup>Communications>Wi-Fi.

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.

Verify the transfer status has completed. See Figure 83.

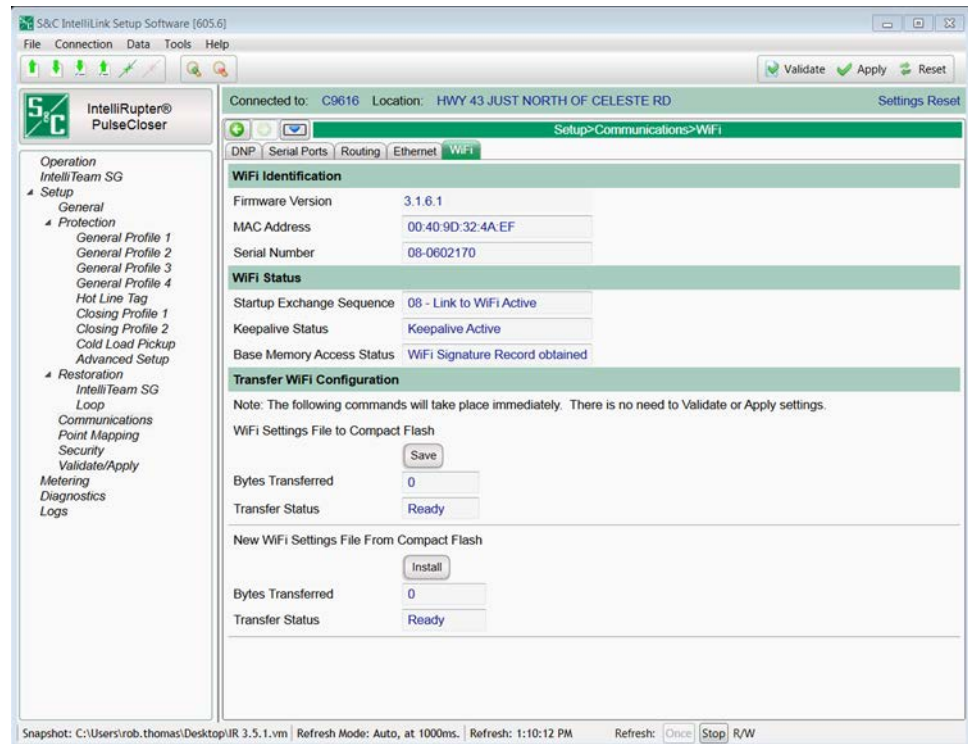


Figure 83. The Setup>Communications>Wi-Fi screen.

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.

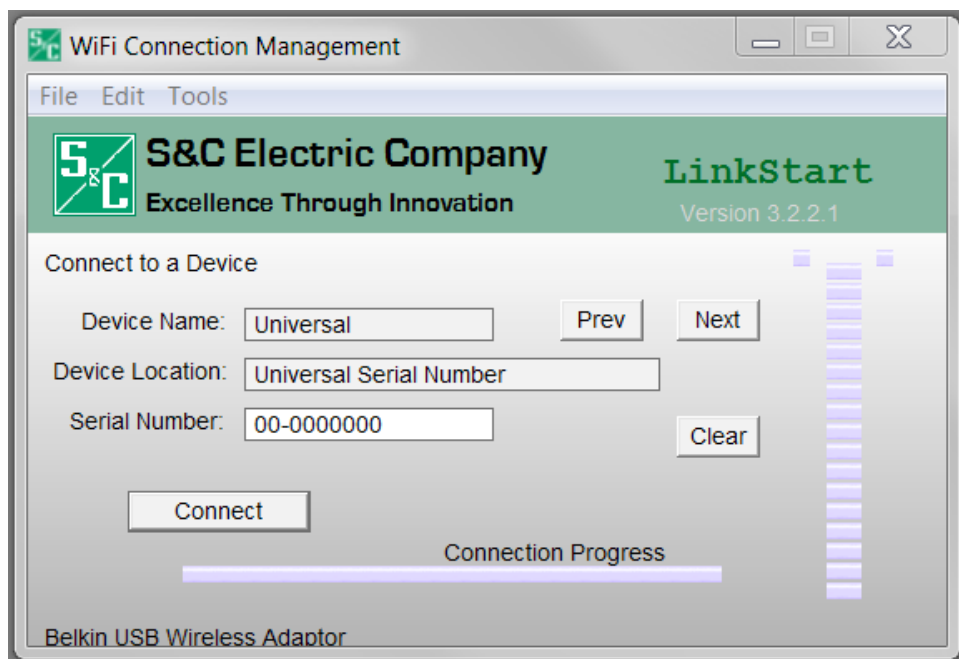


Figure 84. The Wi-Fi Connection Management dialog box.

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.

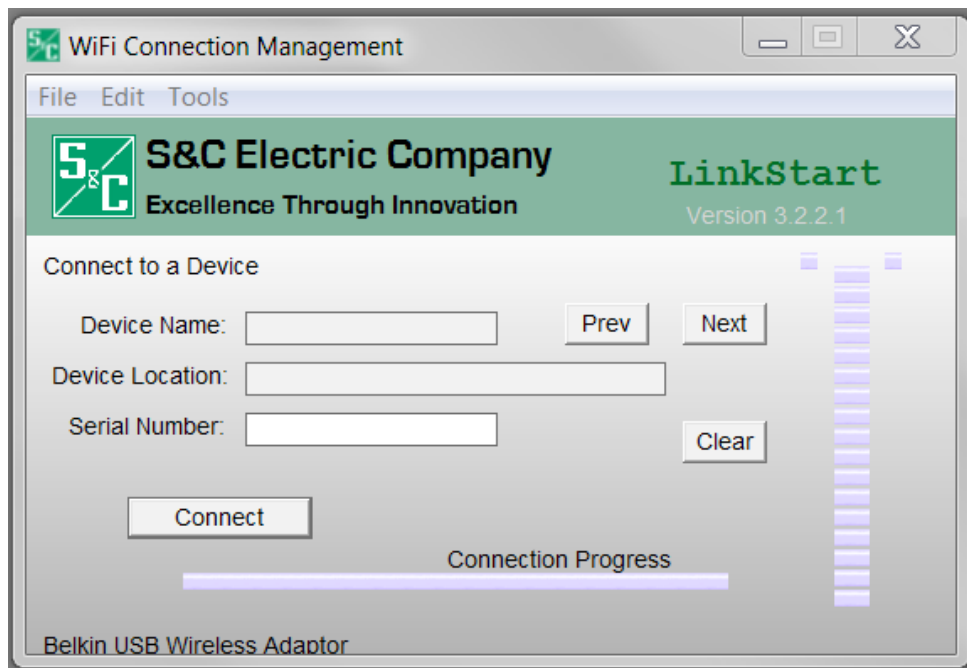


Figure 85. The Connect to a Device dialog box.

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

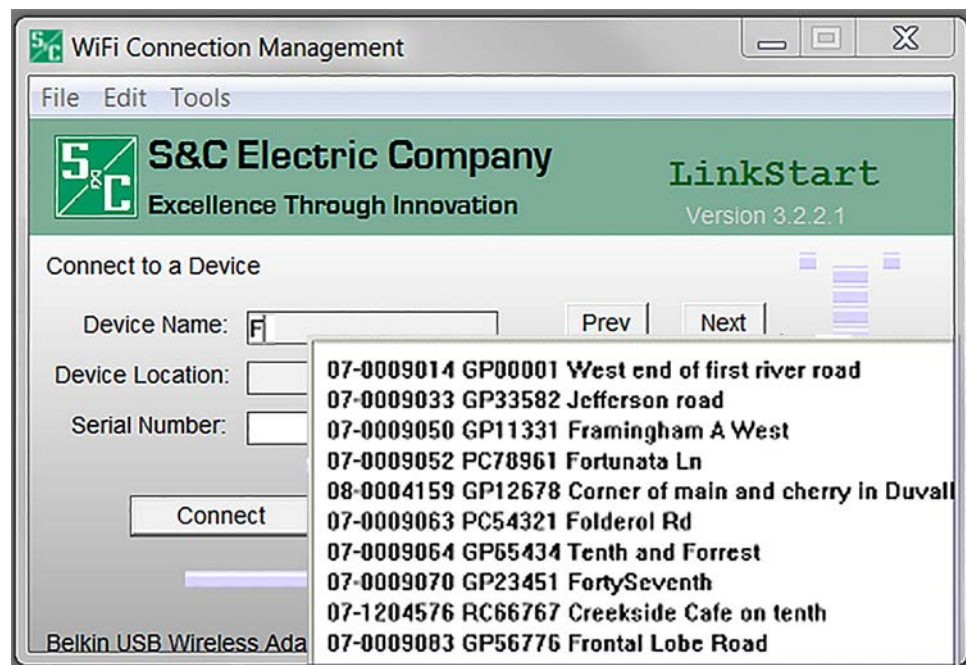


Figure 86. The drop-down list of matches.

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

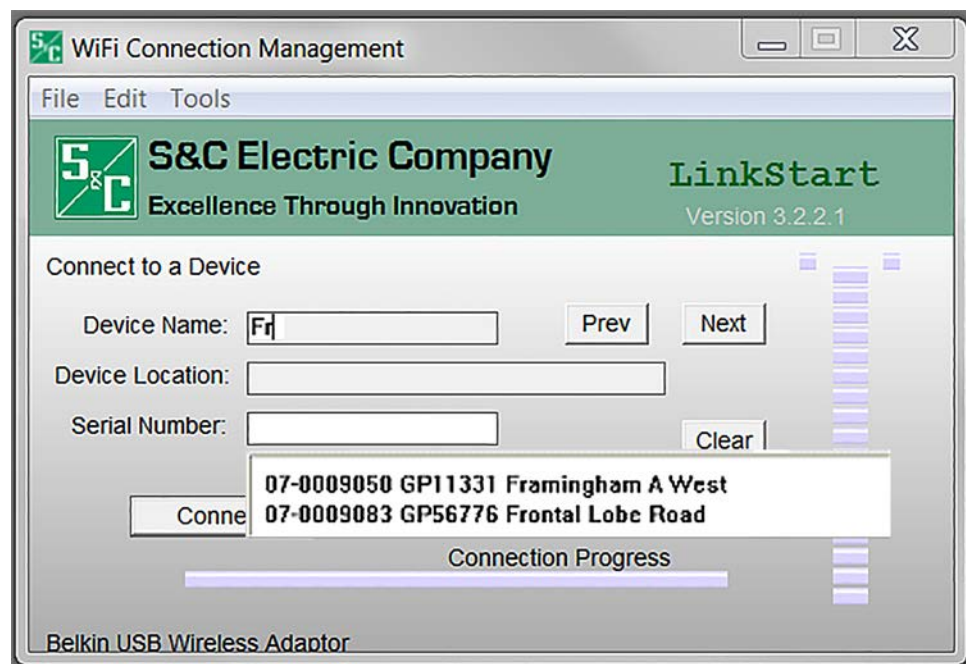


Figure 87. More typed characters narrow the search result.

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 89 on page 55.

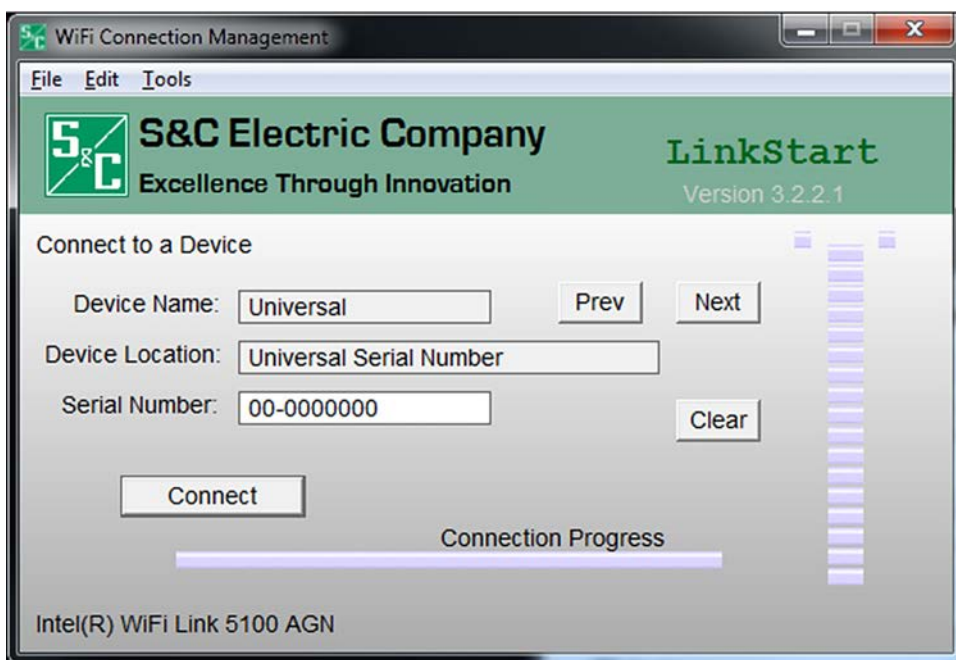


Figure 88. The Connect to a Device dialog box.

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 24 for each IntelliRupter fault interrupter to be configured. See Figure 88.

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.

# Removing Wi-Fi Security Keys

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 80. Click the **OK** button. Click the **Yes** button on the confirmation dialog box. See Figure 89.

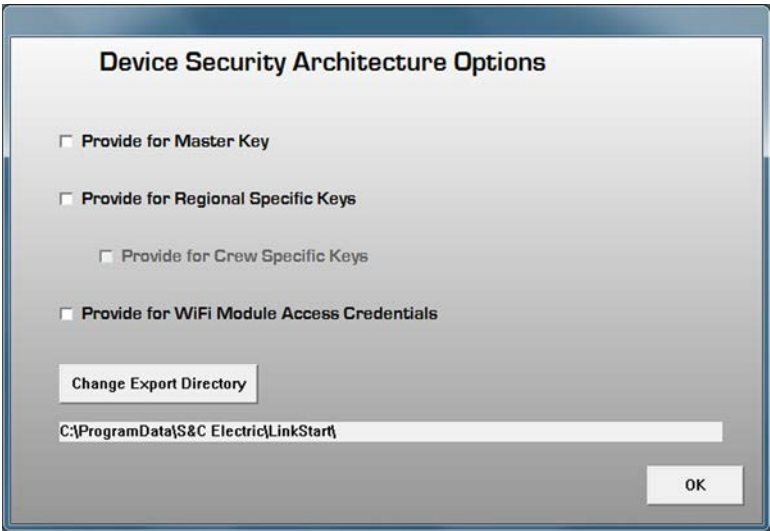


Figure 89. The Device Security Architecture Options dialog box.

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

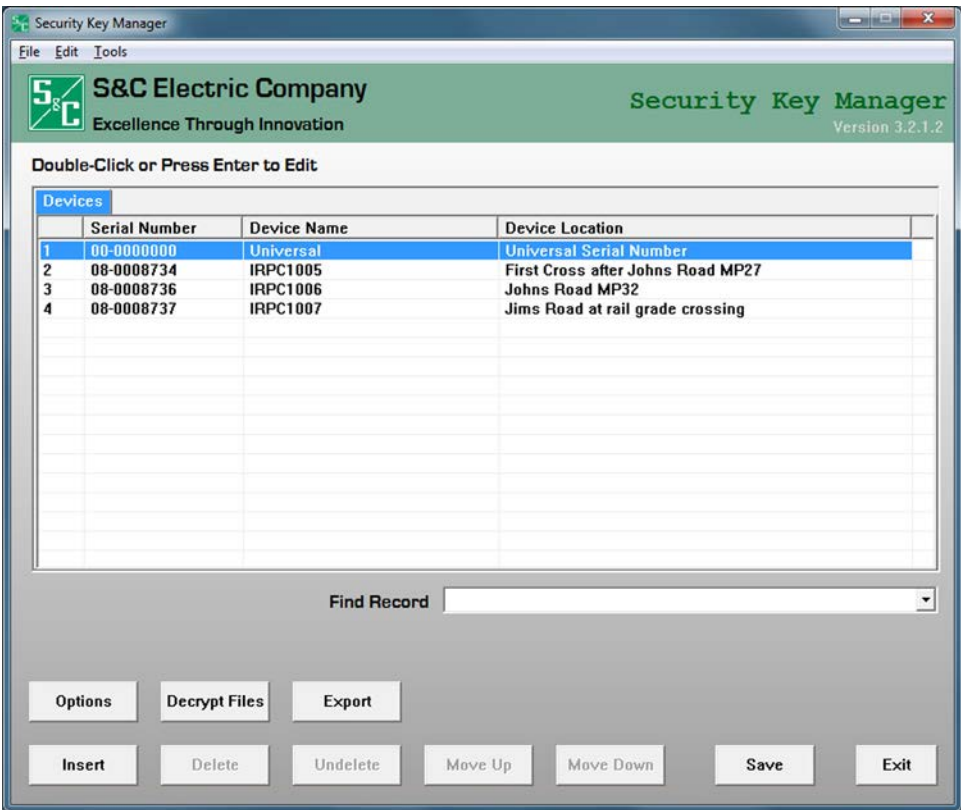


Figure 90. The Security Key Manager screen.



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.

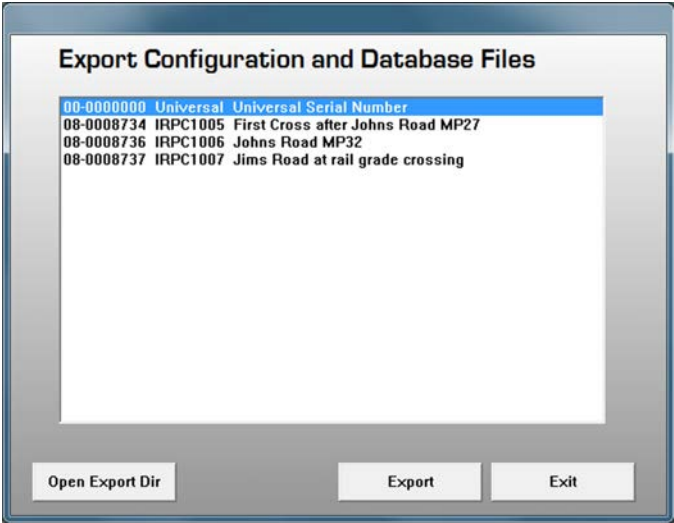


Figure 91. The Export Configuration and Database Files dialog box.

Examine the Universal Configuration File that was 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 93.

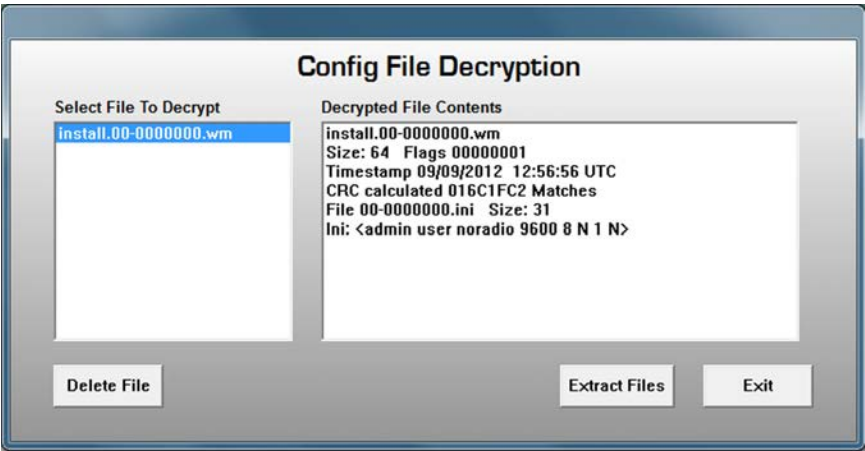


Figure 92. The universal configuration file generated.

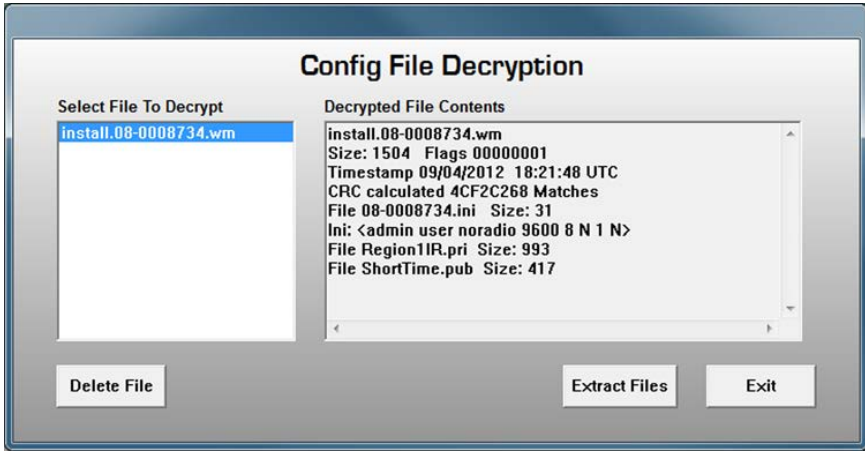


Figure 93. A serial number-specific configuration file.



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.

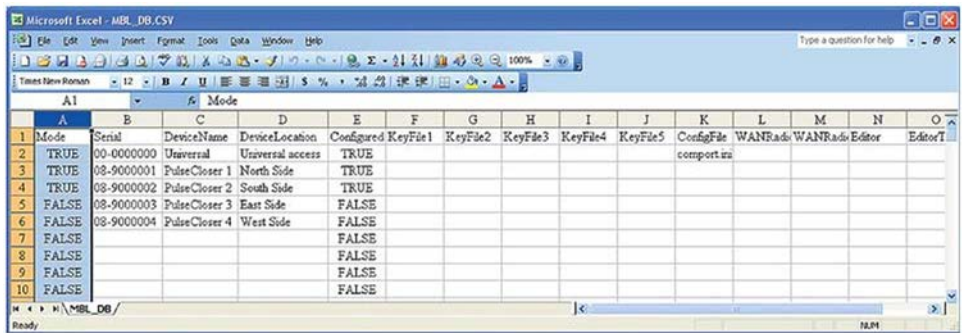


Figure 94. The Microsoft Excel data.

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.

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 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, DeviceName, and DeviceLocation columns remain. See Figure 95.

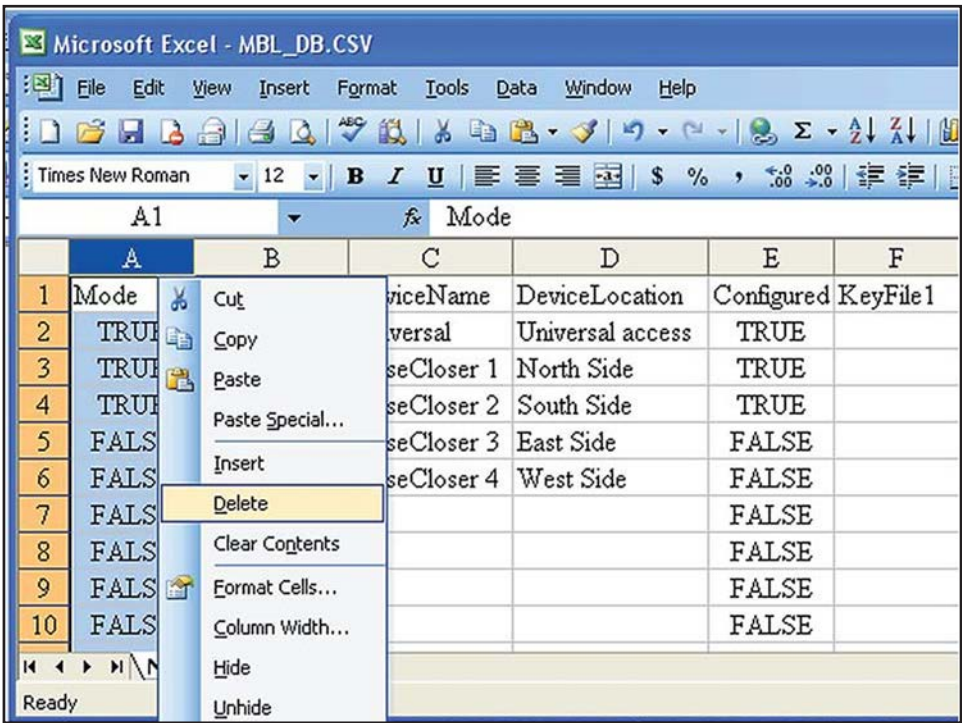


Figure 95. Deleting columns in the Excel program.

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.

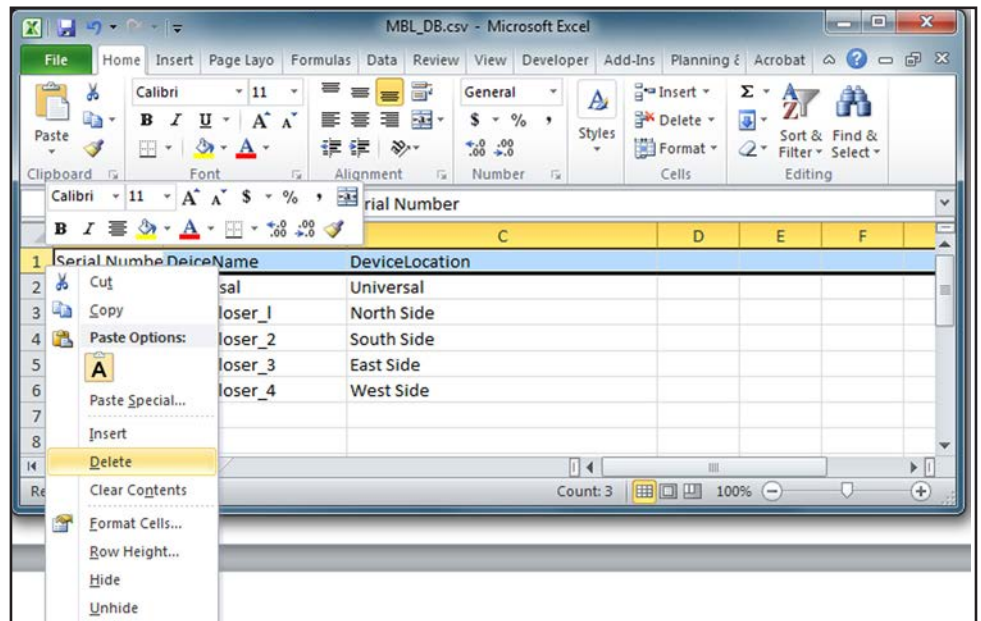


Figure 96. Deleting rows in the Excel program.

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.

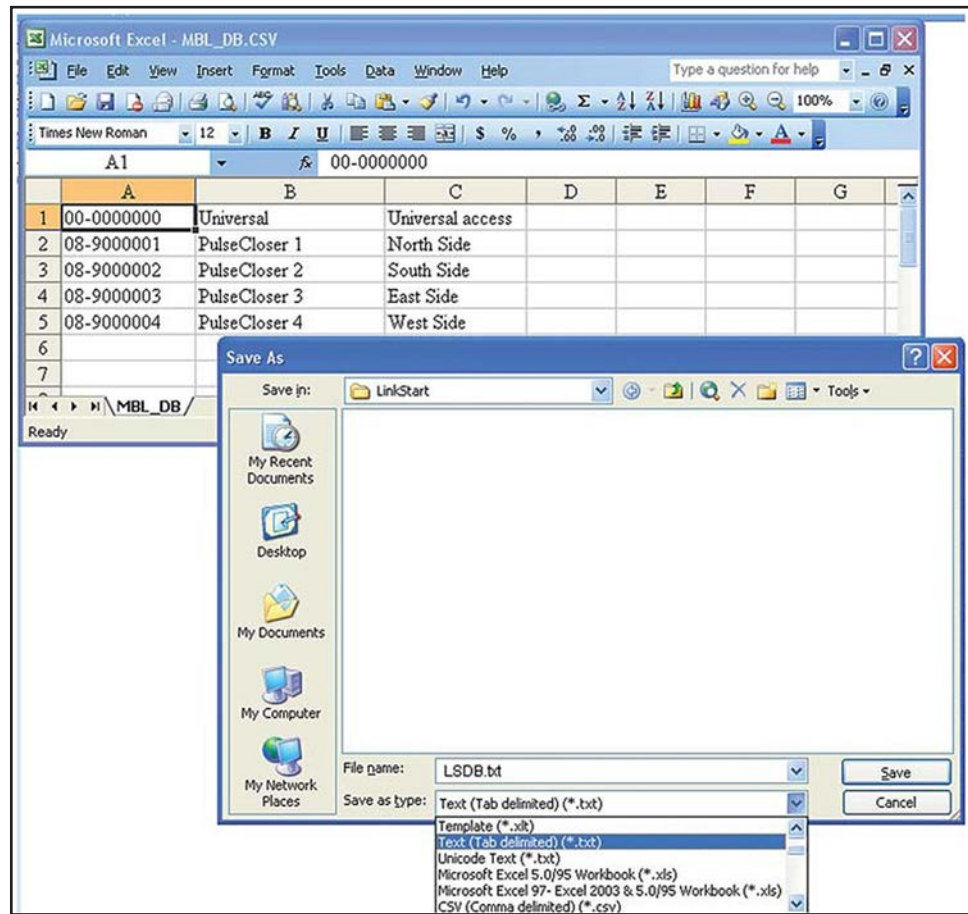


Figure 97. The Save As dialog box.

This dialog box opens. Click on the **Yes** button to close Excel. See Figure 98.

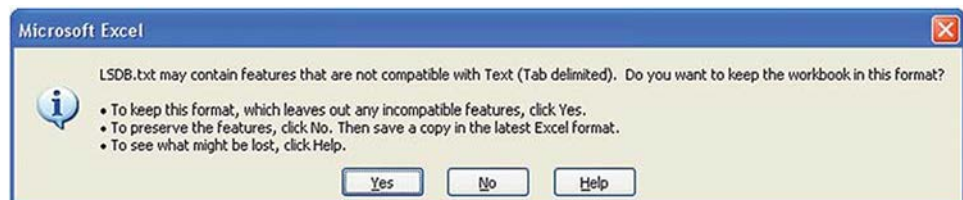


Figure 98. The Microsoft Excel Save As dialog box.

Figure 99 is an example of a converted database.

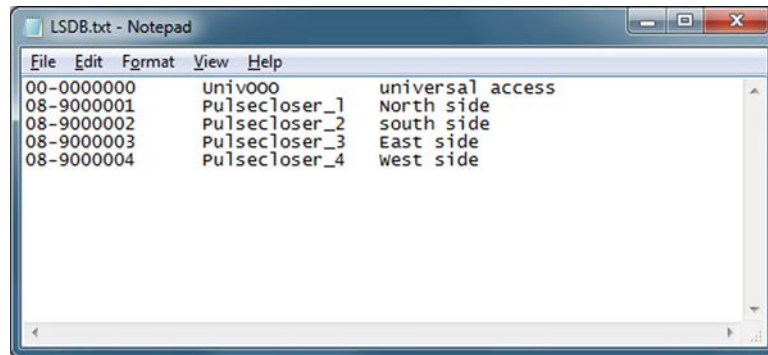


Figure 99. The converted database list.

### 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.

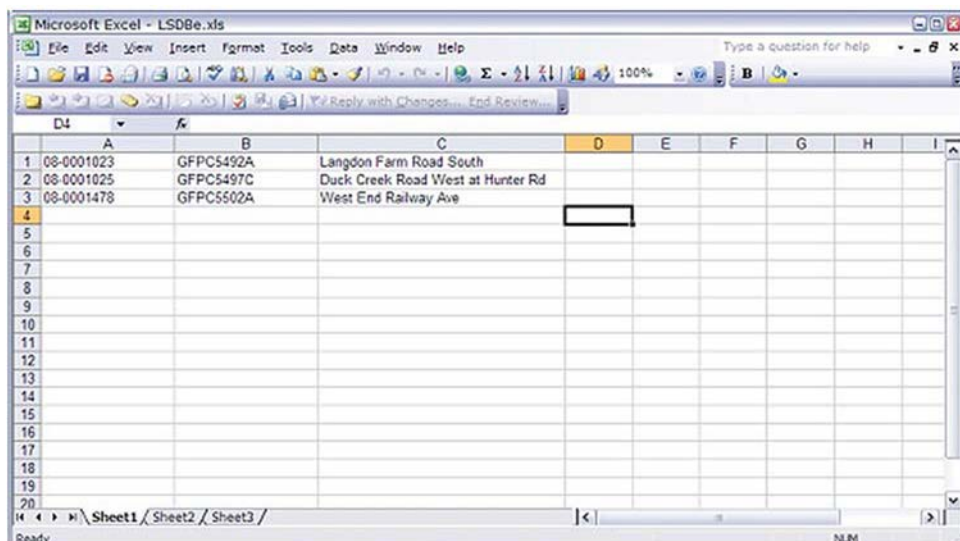


Figure 100. The new Excel file.

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.

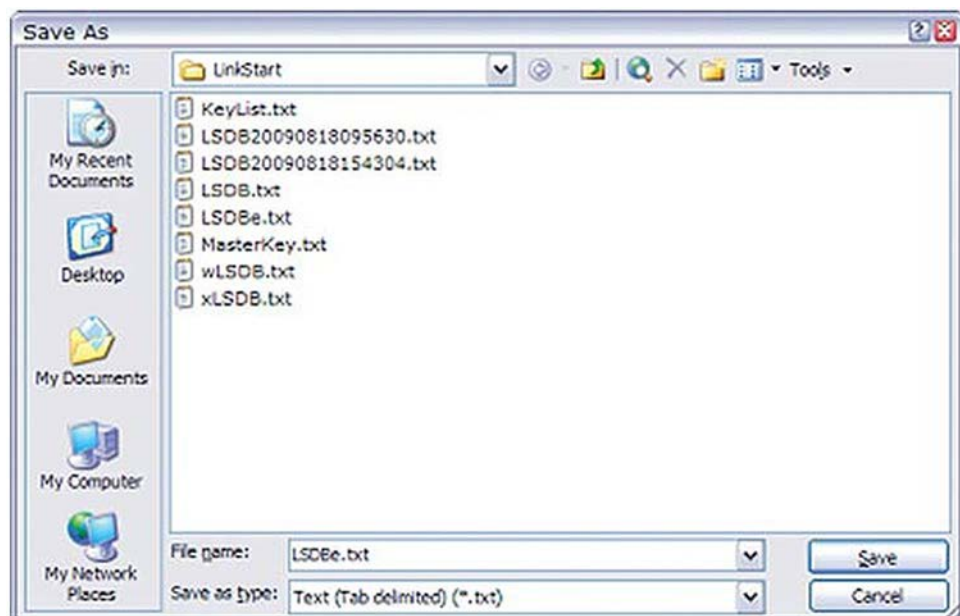


Figure 101. The new file name.

Excel then warns that it will only save one sheet—the active sheet. Click on the **OK** button. See Figure 102.

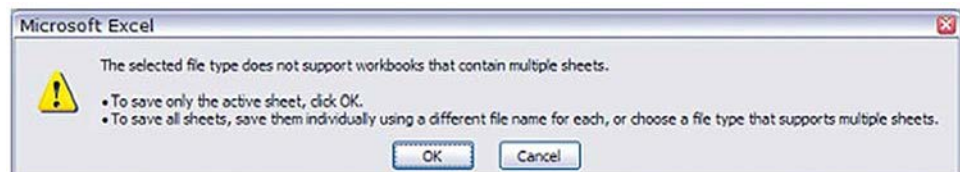


Figure 102. The Excel warning dialog box.



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

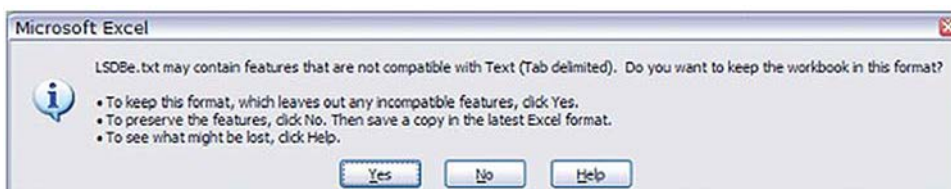


Figure 103. The Excel file save warning dialog box.

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

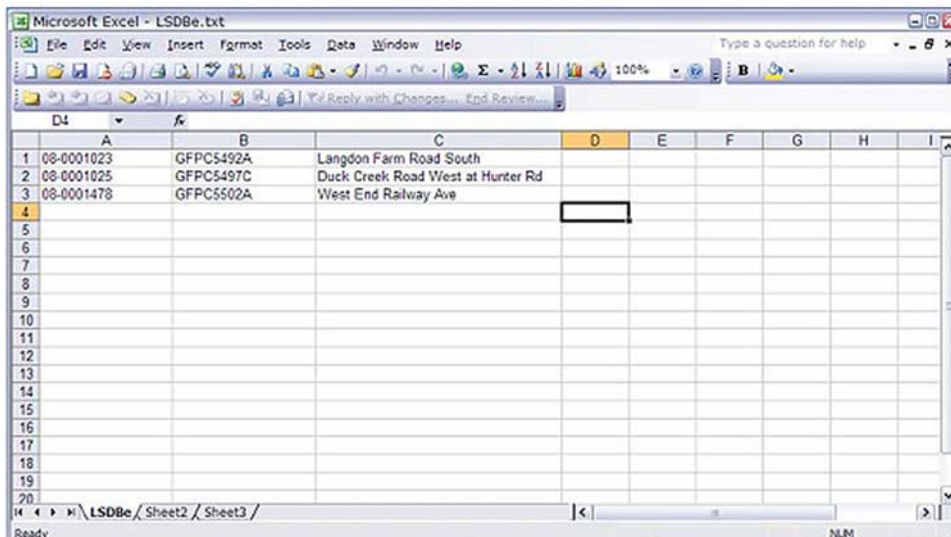


Figure 104. The new Excel file.

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

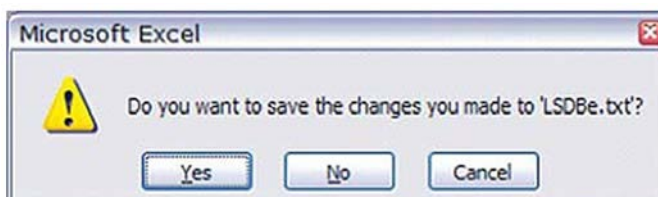


Figure 105. The Excel save changes dialog box.



Checking File with a Binary Viewer

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

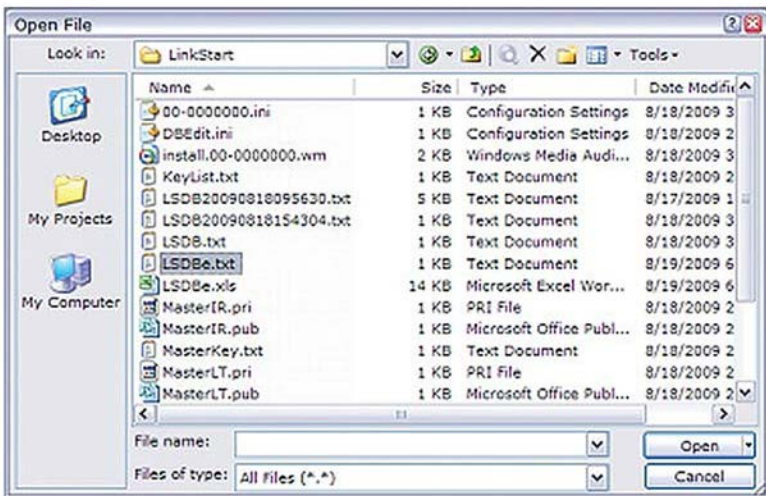


Figure 106. The Open File dialog box.

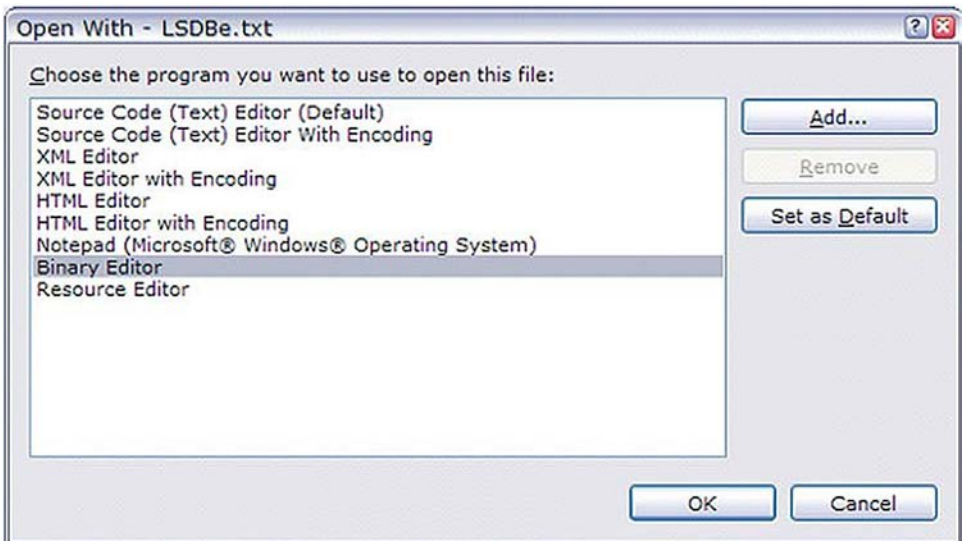


Figure 107. The Open With dialog box.

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

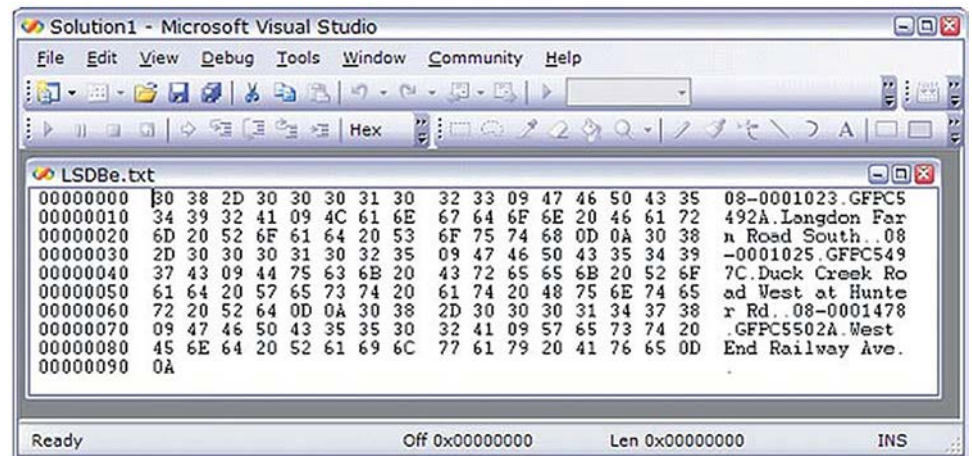


Figure 108. The hexadecimal display of file contents.

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.

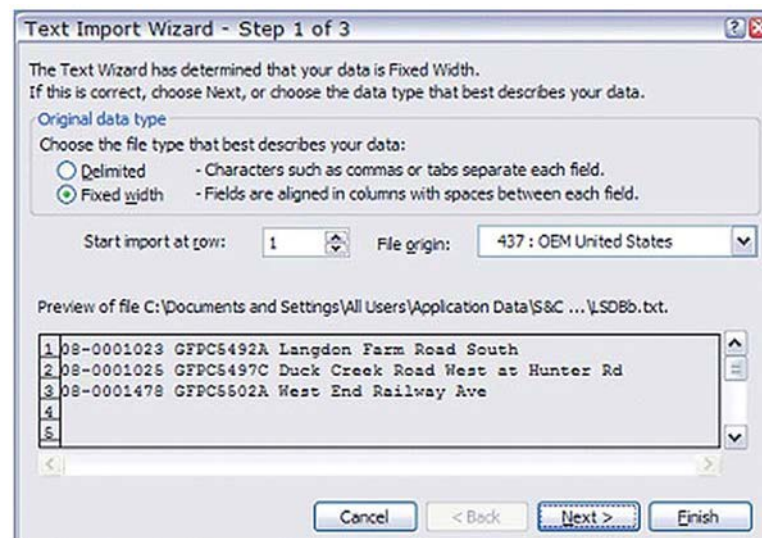


Figure 109. The Text Import Wizard dialog box.

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

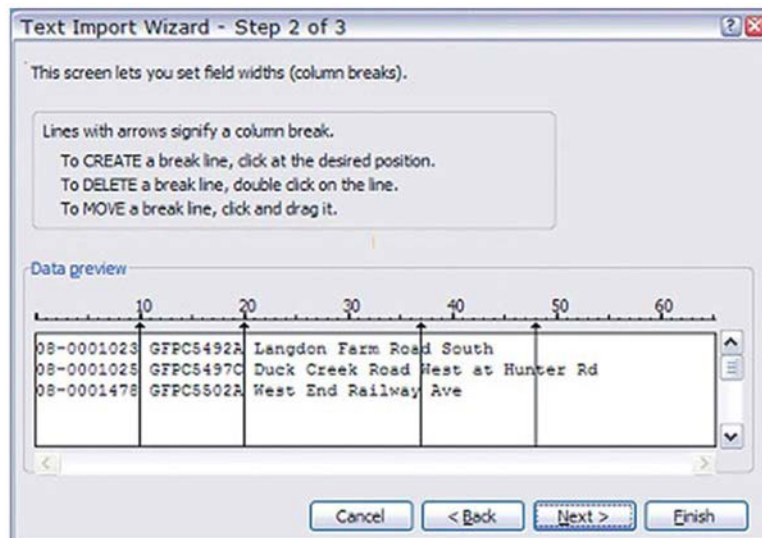


Figure 110. The Text Import Wizard dialog box.

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

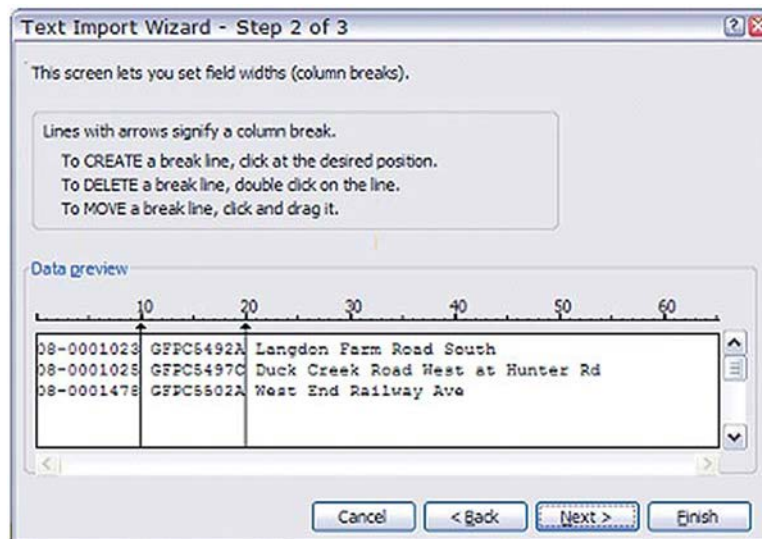


Figure 111. Double-clicking on the extra dividers to remove them.

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

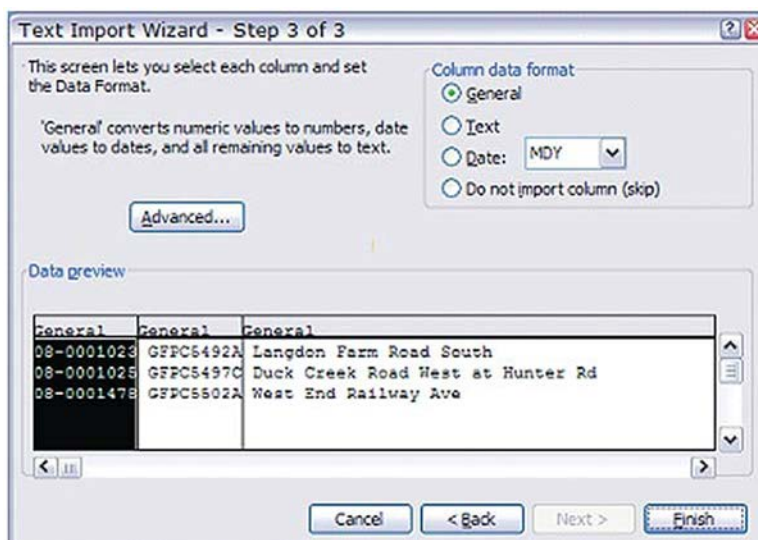


Figure 112. The last step in the Text Import Wizard dialog box.

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

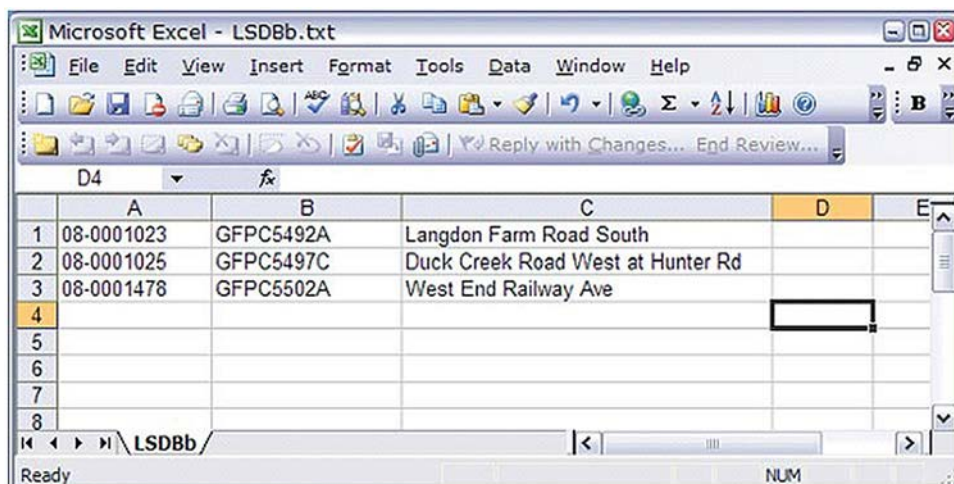


Figure 113. The new import in the Excel program.

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.

**1. What are the system requirements?**

The laptop computer should run Windows XP. The Wi-Fi module and the IntelliRupter control module must have the software components for Installer Version 1.6.9 or later.

Windows 7 can be used with IRInstaller-3.4.7 and later revisions, and 6800 Series Installers 3.4.3 and later revisions.

**2. 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.

**3. 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.

**4. 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.

**5. 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.

**6. 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.