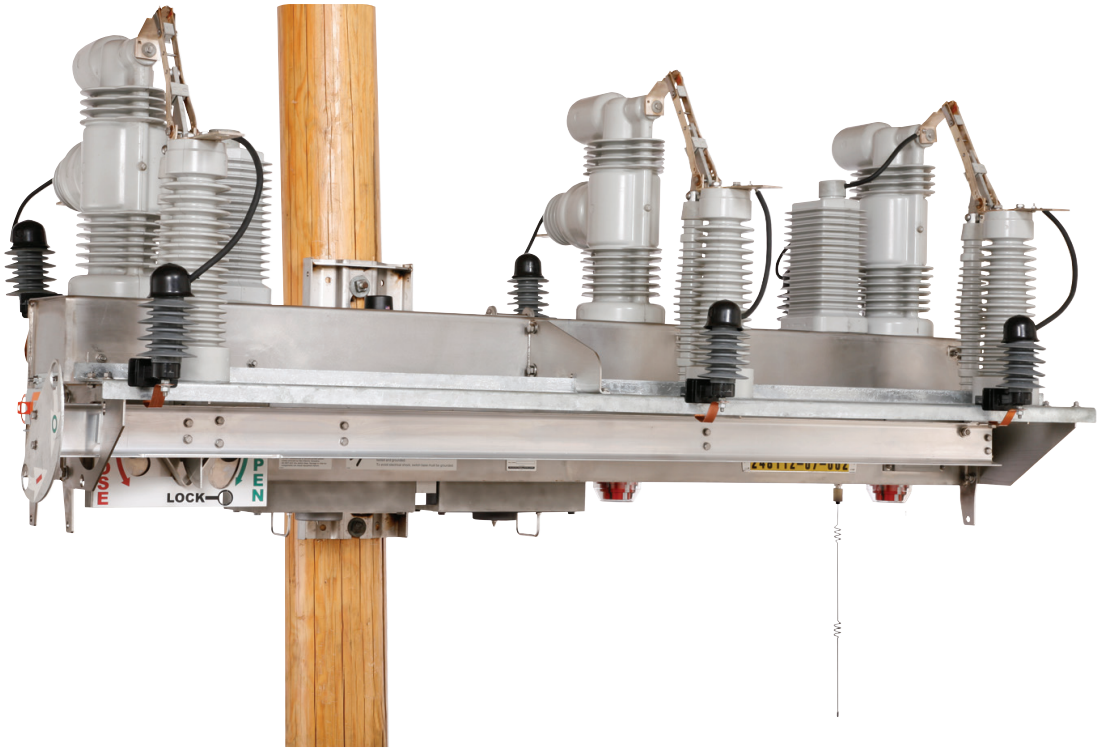
Wi-Fi and Security Administration

Table of Contents



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 non-live 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 publication is available online in PDF format at **sandc.com/Support/Product-Literature.asp**

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 it.

Proper Application

⚠ CAUTION

The equipment in this publication must be selected for a specific application. The application must be within the ratings furnished for the selected equipment.

Special Warranty Provisions

The standard warranty contained in S&C's standard conditions of sale, as set forth in Price Sheet 150, applies to 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: Seller warrants to 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 ten 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 seller's option) by shipment of necessary replacement parts.

Replacement control groups and S&C SpeedNet Radios provided by seller or repairs performed by 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 immediate purchaser or end user all manufacturers' warranties that apply to such major components.

Understanding Safety-Alert Messages

There are several types of safety-alert messages which may appear throughout this instruction sheet as well as on labels attached to the IntelliRupter PulseCloser Fault Interrupter. Familiarize yourself with these types of messages and the importance of the various signal words, as explained below.

⚠ 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 or product or property damage 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 your 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 PulseCloser Fault Interrupter.

Replacement Instructions and Labels

If you need additional copies of this instruction sheet, contact your 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.

Wi-Fi Features and Benefits

The IntelliRupter fault interrupter uses short-range wireless Wi-Fi communication for setup and operation. You can establish a connection to the IntelliRupter fault interrupter using a laptop computer without leaving the security of your vehicle—a great benefit, especially in inclement weather. The control module is housed in the IntelliRupter fault interrupter base to enhance surge protection. There's no need for a separate pole-mounted control enclosure, and its associated control, power, and communication cables.

The Wi-Fi connection between an IntelliRupter fault interrupter and the computer is a direct point-to-point network, with no internet connection, routing capability, or access to other networks. The Wi-Fi module conforms to IEEE Standard 802.11b, the most reliable and widely used choice for Wi-Fi communication. Its modular design allows easy migration to newer technology if required. See Figure 1.

The connection can be made only within the approximate 150-foot range of the Wi-Fi module.

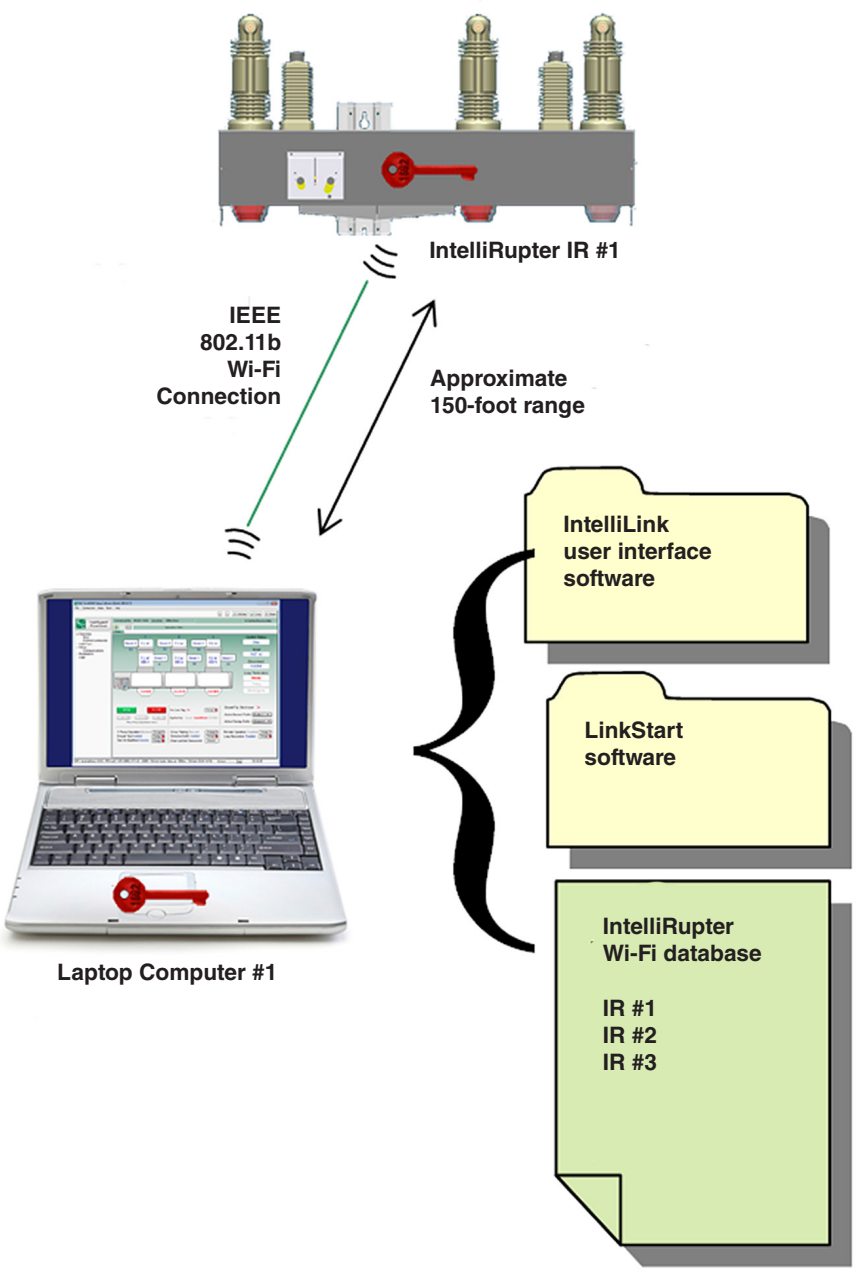


Figure 1. Laptop to IntelliRupter fault interrupter communication with 802.11b Wi-Fi.

The requirements for establishing a Wi-Fi connection to a particular IntelliRupter fault interrupter are:

- A laptop computer with a Windows® XP or Windows® 7 operating system, and Wi-Fi capability.
- S&C IntelliLink Setup Software, and LinkStart Software installed on the computer.
- Matching Wi-Fi security key files in the computer and IntelliRupter fault interrupter.
- An IntelliRupter Wi-Fi Database file resident on, or accessible from, the computer. This IntelliRupter fault interrupter must be included in the file.
- The Wi-Fi-equipped computer must be within 150 feet of the IntelliRupter fault interrupter.

The Wi-Fi connection "opens the door" to an IntelliRupter fault interrupter. Once the link has been established, the control module can be configured, file uploads and downloads can be performed, and the IntelliRupter fault interrupter can be operated. See Figure 2.

If the communication module includes an S&C SpeedNet™ Radio, or other communication device with a serial configuration port, that communication device can also be configured over the Wi-Fi connection. Some other SCADA radios can be configured in this manner as well. Each configuration application has its own security keys, and/or requires a user ID and password.

As will be discussed later, each application has its own security keys and/or requires a user ID and password.

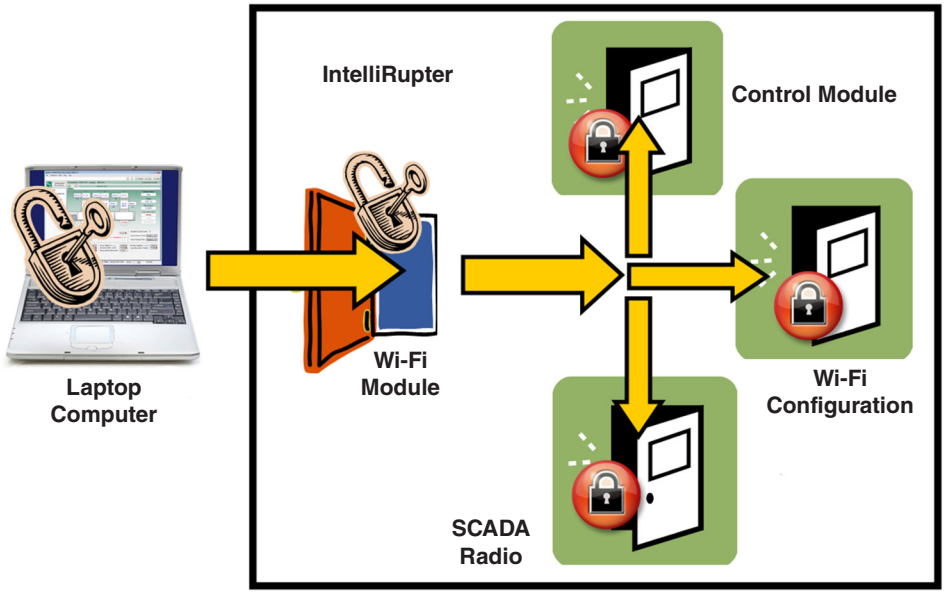


Figure 2. Security keys restrict Wi-Fi communication with the IntelliRupter fault interrupter.

System Security

Your company security administrator can implement a variety of measures at the Wi-Fi level, and in IntelliLink software, to achieve the desired balance of security and convenience.

- Operation of each company computer is password-protected.
- IntelliLink User Interface Software and LinkStart Software are installed only on authorized computers.
- The Wi-Fi Security Key Generator program is used to create, name, and manage security keys on authorized computers. A common security key is simple to use and provides full access for all authorized users. Unique security keys, on the other hand, provide increased security by defining specific IntelliRupter fault interrupters that can be accessed by the authorized user. The access logs and counters in IntelliRupter fault interrupters can be viewed only by the security administrator.
- The security administrator can create a master security key, that permits emergency access to any IntelliRupter fault interrupter on the system.
- The IntelliRupter Wi-Fi Database Editor is used to create a database file for all IntelliRupter fault interrupters on the system, or for just a subset of IntelliRupter fault interrupters, that a technician is responsible for. A common database file may be located on a central server, or a file of specific IntelliRupter fault interrupters can be stored on each user's computer. The user can only wake-up and connect to units listed in his or her database file. IntelliRupter Wi-Fi modules do not broadcast any signals until they receive the encrypted wake-up signal. The public is never aware that IntelliRupter fault interrupters have Wi-Fi capability.
- The administrator can assign one of eight different access levels for an IntelliLink software user.
- Wi-Fi security key files and IntelliLink software passwords in any or all IntelliRupter fault interrupters on the system can be changed by the security administrator using IntelliLink Remote.

Routine Operation

Your security administrator has probably pre-configured your laptop computer for use with IntelliRupter fault interrupters. If so, your computer has been assigned a security key(s), and the IntelliRupter Wi-Fi Database file has been installed on, or made accessible to, your computer.

It's quick and easy to access IntelliRupter fault interrupters for day-to-day operation—four simple steps are all that's required to connect and login to an IntelliRupter fault interrupter:

1. Start the IntelliLink software by clicking the desktop icon, or use the **Start** menu. IntelliLink will automatically launch LinkStart and initiate a Wi-Fi connection.
2. Click **Choose IntelliRupter**.
3. Select the name of the desired IntelliRupter fault interrupter from the dropdown list and click the **Connect** button. Watch the progress bars as LinkStart locates the IntelliRupter fault interrupter, authenticates your computer with the Wi-Fi module, establishes a secure-encrypted Wi-Fi connection, and then opens the IntelliLink User Interface login screen. The process takes 30 to 60 seconds.
4. Select your IntelliLink *Login Group ID* from the dropdown list, and enter your *Password*. The *Operation* screen opens, and shows IntelliRupter fault interrupter voltages, currents, fault targets, and other important data.

Cyber Security

IntelliRupter fault interrupters can be accessed and operated three ways:

- locally using a hotstick,
- locally with a Wi-Fi connection, and
- remotely over a wide-area network (WAN), using an S&C SpeedNet Radio, or other radios and fiber-optic transceivers that are compatible with electric utility applications. See S&C Specification Bulletin 766-31 for a list of devices commonly used with IntelliRupter fault interrupters.

Local access via hotstick provides the same level of security as any other field-operable switch or recloser. It requires the appropriate extendible hotstick, or a bucket truck and hotstick, plus the appropriate handling tool, all of which are generally available only to utility personnel.

Wi-Fi and WAN access, on the other hand, warrant a higher level of attention due to the perceived risk of cyber attack. S&C has addressed this issue by providing your company security administrator with the ability to manage the computer(s) that can access the system IntelliRupter fault interrupters.

The various IntelliRupter fault interrupter security types are shown in Figure 3.

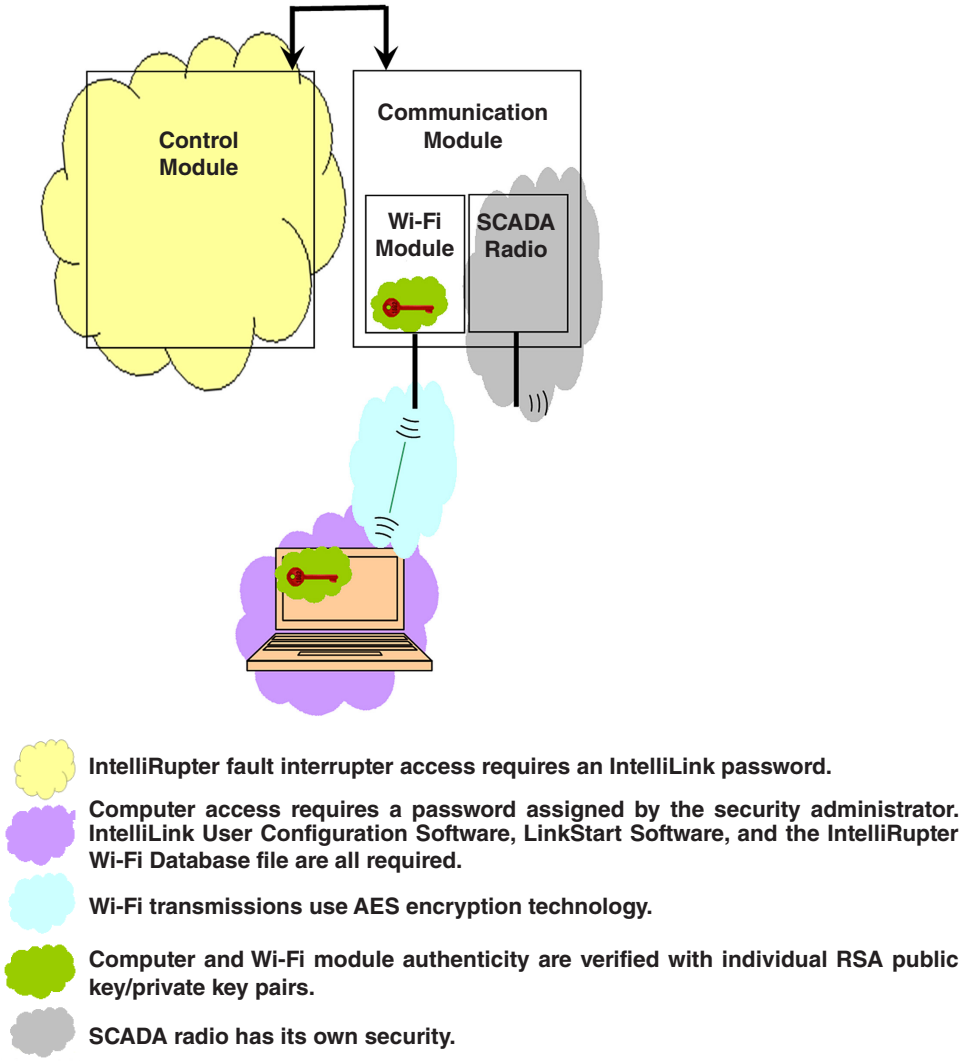


Figure 3. IntelliRupter fault interrupter communication cyber security.

Wi-Fi Security and Encryption

IntelliRupter Wi-Fi uses the latest 256-bit encryption technology from Wi-Fi Protected Access Version 2 (WPA2). WPA2 addresses security problems with the original Wireless Equivalent Privacy (WEP) encryption. It provides government-grade security by implementing the National Institute of Standards and Technology FIPS 140-2 compliant AES encryption algorithm.

Additional S&C features (some patent-pending) have created a unique security system that is easy to use—yet extremely difficult to circumvent:

- Every time a connection is initiated from a user computer, a time-stamped sequence number is generated. This sequence number can never be reused, thus preventing a playback attack, where a hacker records a wireless message and then plays it back.
- Authenticity of both the user computer and the Wi-Fi module are verified using dual-asymmetric public key/private key pairs, known as RSA encryption. The algorithm is split into two parts: encryption and decryption. When a message is encrypted with a public key, it can only be decrypted by another device that has the associated private key. Not even the machine that encrypted the message can decrypt it. One key pair is used to authenticate the computer; a separate key pair is used to authenticate the Wi-Fi module.
- The Wi-Fi module transmitter is turned off, maintaining total radio silence, until a specific message is received, that incorporates an encrypted version of the IntelliRupter fault interrupter serial number, and the appropriate time-stamped sequence number. The Wi-Fi module will never appear in a list of available networks during a Wi-Fi network scan, and the Wi-Fi module will not reply to probe requests. The Wi-Fi Module can reply only to a properly constructed access request from an authenticated utility computer.
- When the Wi-Fi module acknowledges a connection, it generates an AES session key which is securely passed to the computer using RSA encryption. Only that specific computer can decrypt the 256-bit session key. The session key provides authorization to start Wi-Fi communication.
- Once established, the Wi-Fi link between the user computer and the IntelliRupter fault interrupter is direct. There is no internet connection or routing to attract a hacker.
- The Wi-Fi module stores an access log, and if a replay attempt is received, it will generate a DNP alarm for the intrusion event.
- All unused ports, addresses, interfaces, and other back doors, have been disabled.

S&C engineers have worked hard to balance security with ease of use. Most Wi-Fi connection details are handled automatically by software. Reducing the amount of human security interaction makes the IntelliRupter fault interrupter more user-friendly.

Master Keys

Many utilities find that common or Master security keys provide an adequate level of security, allowing access to all system IntelliRupter fault interrupters by authorized users, while preventing any unwanted access. Master keys make it easy to add additional IntelliRupter fault interrupters, users, and computers. The password and key files can be updated once-a-quarter, once-a-year, or never—determined by the security administrator.

All IntelliRupter fault interrupters and computers shown in Figure 4 on page 9 share the same security keys. So each computer is authorized to access every IntelliRupter fault interrupter in the system. If the computers can access a corporate server through a cell phone link, the IntelliRupter Wi-Fi Database can reference the central file that contains the latest IntelliRupter fault interrupter list. Or the latest version of the Wi-Fi Database can be saved on each authorized computer.

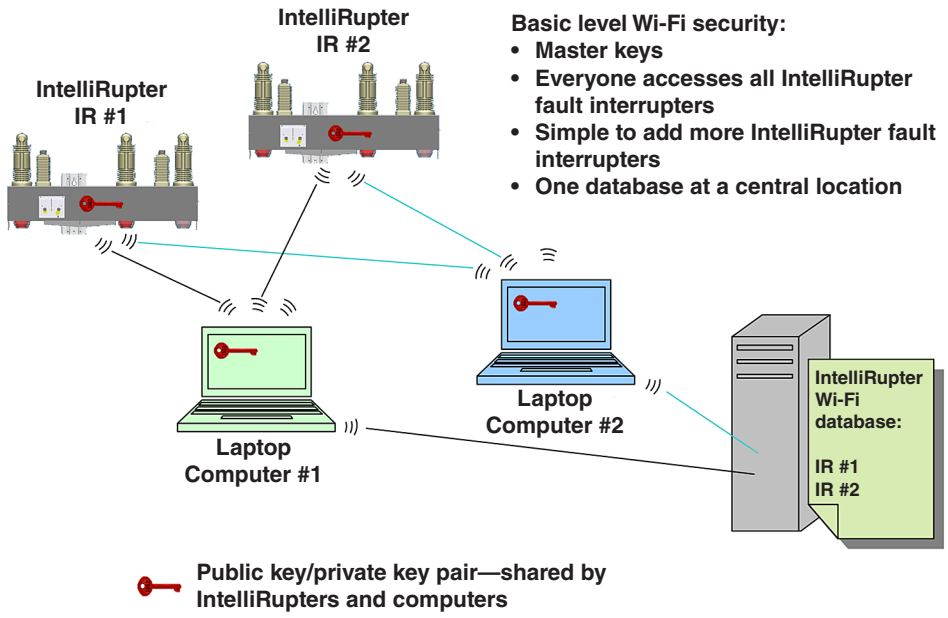


Figure 4. Master security key used by the system.

To add IntelliRupter IR #3 to the system, you must load the common keys into its control module. First, connect to it as the administrator using the default S&C-supplied security key files. Then use LinkStart to transfer the new security keys to IntelliRupter IR #3 the default keys are automatically deleted when new keys are added. Use Wi-Fi Database Editor to update the central database to include the new IntelliRupter fault interrupter. All authorized users can now connect to the new IntelliRupter fault interrupter. See Figure 5.

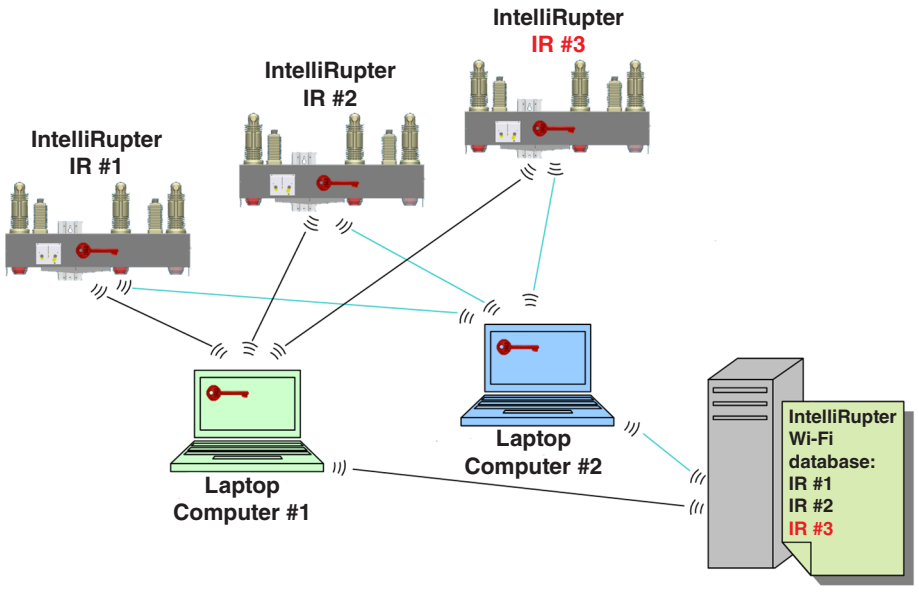


Figure 5. A third IntelliRupter fault interrupter has been added to the system.

Using common security keys does not affect the security of encryption algorithms. The Wi-Fi module will not broadcast until it receives a special encrypted message from the computer. Complex RSA encryption algorithms prevent access to users without the proper security keys. And Wi-Fi communication, as always, uses AES encryption and is very secure.

This basic level of security makes access by authorized users simple, while successfully preventing unwanted access to the system.

Regional Security Keys

An increased level of Wi-Fi security is easily attained by managing security key pairs and/or Wi-Fi Database files on a regional basis. Instead of using a common security key pair across the system, unique key pairs can be generated for each operational region or otherwise logically organized group of IntelliRupter fault interrupters.

A middle ground between common and unique Wi-Fi security keys can be achieved by assigning unique keys to groups of IntelliRupter fault interrupters. In the Figure 6 example, the IntelliRupter fault interrupters have been organized into to two regions and assigned region keys.

All computers for Region 1 will use Region 1 keys and all the computers for Region 2 will use Region 2 keys. Super users can be created by giving their computers multiple keys.

An administrator is a super user who's computer has every key.

Updating passwords and key files becomes more manageable because updates can be done region by region, so everyone doesn't have to be revised at the same time.

To add a new IntelliRupter fault interrupter to a region, load the region key into its control module. The process is the same as adding an IntelliRupter fault interrupter to a system that uses Master keys. Use the Wi-Fi Database Editor to update the central database to include the new IntelliRupter fault interrupter. Or alternately, the latest version of the Wi-Fi Database can be copied to each computer used in the region. Only the computers in the region with the new IntelliRupter fault interrupter need to be updated.

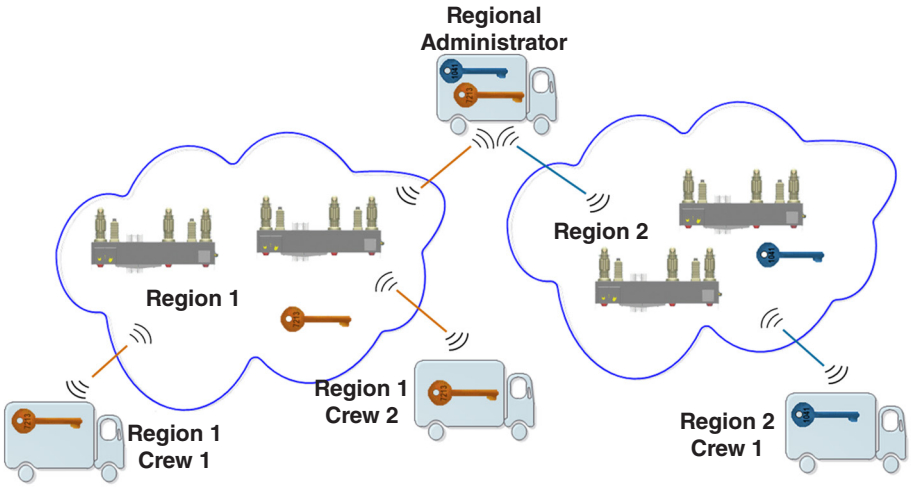


Figure 6. Regional security keys.

Regional and Crew Security Keys

Greater security can be obtained by adding crew keys to the region keys. More than 30 different security key pairs can be stored in the Base Memory Module of an IntelliRupter fault interrupter. Each time a successful Wi-Fi connection is made, the date, time, and name of the security key used is recorded in the Wi-Fi security log. Access to view, download, or clear the log is restricted to your company security administrator. The name of each security key is selected by the administrator; so it can be the employee name or another suitable descriptor.

With unique security keys and/or log-in passwords, it is possible for the administrator to record access for each individual or user group. See Figure 7.

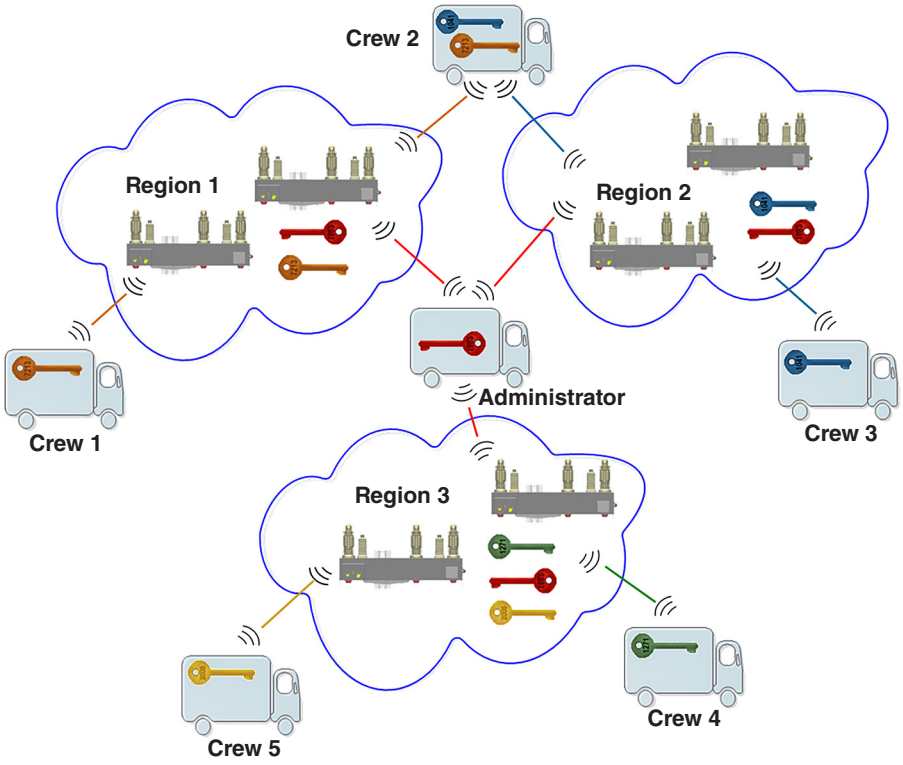


Figure 7. Region and Crew security keys.

To add a new IntelliRupter fault interrupter to a region, load the region and crew keys into its control module. The process is the same as adding an IntelliRupter fault interrupter to a system that uses region or master keys. Use Wi-Fi Database Editor to update the central Wi-Fi Database to include the new IntelliRupter fault interrupter. Or alternately, the latest version of the Wi-Fi Database can be copied to each computer used in the region. Only computers in the region with the new IntelliRupter fault interrupter need to be updated.

Administration Keys and Temporary Keys

If all keys for a commissioned IntelliRupter fault interrupter are lost, it will not be possible to establish a Wi-Fi connection to that unit. Security keys are stored in the Base Memory Module of the IntelliRupter fault interrupter and are not reset when the control module is changed. If a replacement communication module is inserted in the base, the Wi-Fi module receives the serial number and other security parameters from the Base Memory Module.

For systems using region and crew keys, the security administrator can also make a master key. It's a good practice for the security administrator to generate a master key pair permitting access to all IntelliRupter fault interrupters on the system. This secret key should be held only by the administrator.

In the event computers or security keys are lost or forgotten, the master key pair can

be used to connect to any IntelliRupter fault interrupter, so the security system can be rebuilt.

The security administrator can also issue temporary security keys for use by a visiting crew or consultant. An expiraton time limit can be assigned to these key pairs. If desired, each IntelliRupter fault interrupter can be pre-configured during commissioning to hold a number of temporary keys. Once the consultant establishes a Wi-Fi connection using the temporary security key, the timer starts, and the key eventually expires.

Shown in Figure 8 is an example of an IntelliRupter fault interrupter assigned a variety of master and temporary keys.

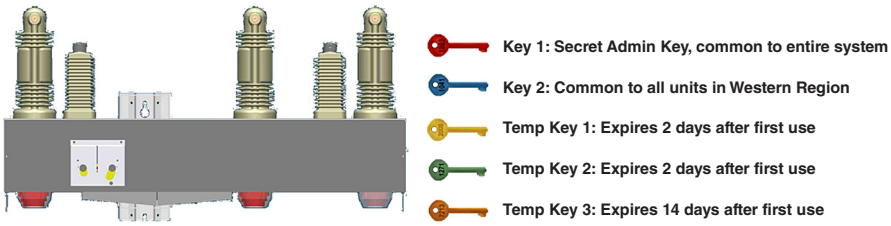


Figure 8. Administrator and Temporary security keys.

Access Denial

To deny Wi-Fi access for a specific user, the first step is to remove the Wi-Fi security keys from that user computer. If further action is warranted, Wi-Fi and/or IntelliLink security can also be changed.

If a common security key is used, the security administrator may need to create a new security key and update all IntelliRupter fault interrupters and computers accordingly.

A benefit of using region and crew security keys is that a single user can be de-authorized by disabling specific keys on the IntelliRupter fault interrupters that person has access to; there is no need to update the computers of other users.

Security keys and IntelliLink software passwords can be updated using IntelliLink Remote Configuration Software. IntelliLink Remote Setup Software allows the security administrator to login to one IntelliRupter fault interrupter and update other affected units over the radio network.

Computer security keys can be updated by a simple file update, via e-mail or a server download.

IntelliLink Setup Software Security

IntelliLink Software has eight user-definable access levels. Default group assignments include:

- Administrator
- Operator
- Protection Engineer
- Technician 1 (Restoration Technician)
- Technician 2 (Communication Technician)
- Technician 3 (Automation Technician)
- Additional User Group 1

All valid passwords allow the user to view operation screens. The security administrator can assign permissions to perform activities such as changing general settings, changing communications or protection settings, and operating the device.

IntelliLink passwords are stored in the IntelliRupter Base Memory Module, and can be updated when users are added to or removed from the system.