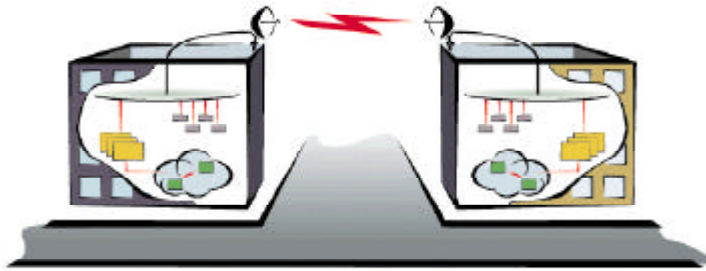


SecureLINK Software

Models RMG-105, 205, and 305



About SecureLINK

Wireless technology promises a world without boundaries and the convenience offered by wireless devices, but with wireless technology also comes security risks. Wireless transmissions containing valuable information are susceptible to interception and tampering by hackers; therefore, businesses have no choice but to ensure this information is protected and safe.

RadioLAN Marketing Group™ offers state-of-the-art security that will encrypt all the data sent on RadioLAN wireless networks to enhance the security of the network and keep transmitted information private. Encryption puts the data into a form that cannot be read and ensures privacy by keeping information hidden from anyone for whom it was not intended.

SecureLINK is based upon BSAFE™ Crypto-C from RSA Security™, the most trusted name in Security. Crypto-C, the most popular form of public-key cryptography, is a public-key/private key system where the public key is made public while the private key remains secret. Encryption is performed with the public key while decryption is done with the private key. This means you can communicate securely to just about anyone, anywhere.

RadioLAN's SecureLINK™ software provides this encryption capability on the wireless network. Each station encrypts/decrypts data at its local CPU, which means that on RadioLAN's Campus BridgeLINK™, for example, the process does not slow down the network. SecureLINK is available in either 40-bit or 128-bit from your Authorized RadioLAN Reseller.

Specifications

Model Numbers	RMG-105 SecureLINK/Card 128-bit encryption for Adapter products, Models 101, 130, 140, and 150 RMG-205 SecureLINK/Access Point 128-bit encryption for Access Point products, Model 208 and 218 RMG-305 SecureLINK/Bridge 128-bit encryption for Bridge Products, Models 3xx series.
Warranty	1 Year parts and labor (return to factory)
Technology	RSA Security's BSAFE Crypto-C cryptography
Security Standards	Supports ANSI X9.30, X9.31, X9.32, X9.42, X9.56, X9.62 and X9.63 financial standards; IEEE: P1363; PKCS: 1, 5, 8, 11, 186. NIST (FIPS): 46-2, 81, 180-1, 186

Features

- Based upon BSAFE Crypto-C from RSA Security, a trusted name in security technology.
- A highly secure method of keeping your data transmissions safe.
- Based upon the most popular public-key cryptography.
- Easy to install and set-up.
- Standards compliant.
- Provides peace of mind knowing your wireless network is safe.
- Available for all RMG Products.



RadioLAN
Marketing Group

www.radiolan.com

RadioLAN Encryption

Enabling Encryption on the RadioLAN network

To switch a RadioLAN network over to encryption mode requires two steps on each device.

- Step 1. Enter the encryption-string.
- Step 2. Select encryption mode of operation.

How-To: CardLINK Products

- Using RadioNet Manager, choose the Info panel, press the MODIFY button.
- Press the Encryption Key button, and enter the encryption-string into the pop-up window. The encryption-string will not be visible. You must enter it twice to verify it is correct.
- Now, select the Encryption checkbox to turn on encryption and decryption.

Note: The RadioLAN header information is not encrypted. This allows RadioNet Manager to display the station's signal levels, but does not allow the computer to send data. If you are using a BackboneLINK-II access point, you will not be able to select Access Point until it has been put into encryption mode.

How-To: BackboneLINK-II

To setup a BackboneLINK-II for encryption, you must have a management session established with a web browser or use the VT100 control port.

- From the BackboneLINK-II Manager window, select Configuration Settings.
- Select Encryption.
- Select Encryption settings.
- Enter the encryption-string (twice).
- Select the Encryption Mode checkbox.

How-To: Campus BridgeLINK-II

The Campus BridgeLINK-II provides a link between buildings. ***You MUST enable encryption on the remote CBL-II first,*** then enable encryption on the near CBL-II. Failure to do this can stop your CBL-II communication, and require that you go to the other side of the link before you can reach the remote CBL-II to change it back. Changing a CBL-II system to enable encryption will cause a short outage (approximately 1-minute).

- Step 1. Make sure your link is operating and transmitting data.
- Step 2. Use your browser to connect to the remote CBL-II.
- Step 3. Select Configuration Settings.
 - Select Encryption.
 - Select Encryption settings and enter the encryption-string (twice).
 - Select the Encryption Mode checkbox.
- Step 4. Use your browser to connect to the local CBL-II.
 - Repeat Step 3.
- Step 5. Using the Antenna Aiming screen, verify the link is correctly setup again.

Corporate Headquarters:

185 Lewis Road - Suite 30 Phone: 408-365-6200
San Jose, CA 95111 Fax: 408-365-7675



www.radiolan.com