

A close-up photograph of a silver metal padlock resting on a laptop keyboard. The padlock is the central focus, with its shackle open. The background is a warm, reddish-orange gradient, and the laptop's keys are visible but slightly out of focus.







Radio IP MTG™

Mobile VPN Security Solutions

Giving a mobile workforce access to the corporate LAN will always preoccupy the minds of IT Managers across mission-critical organizations. Indisputably, IT Management’s primary concern will be that of: Security.

Radio IP MTG™, a mission-critical Mobile VPN, will ensure that all security breaches are eliminated when it comes to data transmission to and from your mobile workforce and head office. Radio IP MTG helps you protect your users, your LAN and the integrity of your data. You can select the security level that meets your organization’s unique requirements, and secure your wireless data transmission with any combination of networks you choose to leverage.

Radio IP Software’s End-to-End Secure Mobile VPN

 <p>Mobile VPN & Encryption</p> <p>Protect the integrity of your mobile data being transmitted over the air.</p>	 <p>Digital Certificates</p> <p>Validate the authenticity of the devices being used to access the network.</p>	 <p>Single Sign-on Authentication</p> <p>Simplify authentication by using one sign-on for both the device and the Mobile VPN.</p>
 <p>Security Audit Function</p> <p>Keep all security events on the server or send it to your syslog system.</p>	 <p>Two-Factor Authentication</p> <p>Validate the identities of your users attempting to log onto the network.</p>	 <p>Access Defender™</p> <p>Rethink the way your system establishes connections and protect your LAN in the process.</p>

Wireless Security at the Core of our Mobile Data Communications Solution

Mobile VPN & Encryption

Most VPN solutions were created for the wired world. Radio IP MTG™ provides a Mobile VPN designed specifically for wireless networks, allowing you to extend your network boundaries beyond the corporate firewall. Radio IP Software’s Mobile VPN is more stable than off-the-shelf solutions and simpler to manage than SSL VPNs. Destined for organizations transmitting sensitive, mission-critical data, your VPN connection is seamless and persistent even as you roam over disparate networks.

Since wireless network signals are broadcast and can potentially be intercepted, we offer the highest encryption standards assuring all data are transferred securely between the field worker and home office. The IT Manager is able to choose which level of encryption best fits the organization’s needs. Data can be encrypted with either AES (128, 172 or 256-bit) or Triple DES (112 or 168-bit) symmetric encryption methodologies, using FIPS 140-2 validated technology.

Alternatively, some organizations may choose to utilize the DES encryption algorithm. These symmetric secret keys will be exchanged using RSA FIPS 140-2 validated asymmetric encryption technology. Since our encryption meets and exceeds state and federal FBI/CJIS security mandates, you can be assured that all data passing to and from your organization, whether it is private citizen data, criminal history, medical records, line locations or financial data, is safe and secure.

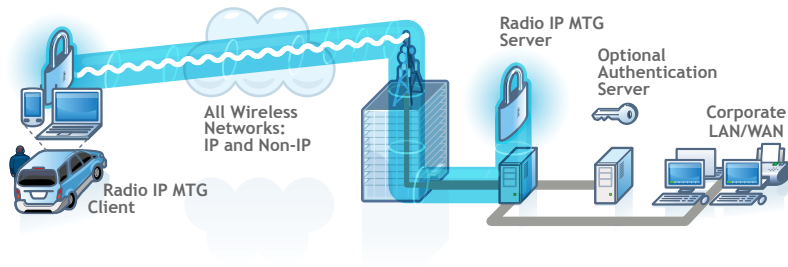
Digital Certificates

With Radio IP MTG, you have the tools to validate the authenticity of the device being used to access the LAN. By checking if the device's digital certificate is legitimate or not, the organization can protect against foreign devices attempting to break into the network. Moreover, even before a user can try to log onto the system, our Mobile VPN's encrypted tunnel will be

established and the authenticity of the device will be verified. This method is essential in ensuring that no critical data will be sent over the air in clear text (particularly usernames and domain names), a security breach that is commonly found in many other Mobile VPNs. The digital certificates used by Radio IP MTG are compliant with the ITU x.509 v3 standard.

End-to-End Secure Data Tunnel Using Radio IP MTG™

© 2006 RADIO IP SOFTWARE INC. / 200-00000236-0002



Single Sign-On Authentication

Is your organization looking for ways to save its field workers' valuable time? Radio IP MTG can help you to simplify the authentication process without creating a security breach on your network. On top of our application and session persistence, Radio IP MTG allows, via the use of 802.1x protocols, mobile workers to sign-on once and authenticate on the device and the Mobile VPN concurrently. Life can thereby be made easier for the end-user but still remain secure for the IT Manager.



Security Audit Function

For IT Managers, security is top-of-mind and they need to be aware of what is happening on their system. Using the Security Audit function in Radio IP MTG, IT Managers are able to log and store all security events in files on the server: Device authentication attempts, user authentication attempts, ghost detection, etc. Should you already be utilizing an external syslog server, simply identify its IP address in Radio IP MTG, which will send it the critical event information in real-time, allowing immediate action to be taken.

Supplemental Security Options

With wireless security at the core of Radio IP MTG and all of our mobile data communications software solutions, Radio IP Software has developed supplemental security options designed to meet more precise customer and partner requirements. In addition to the highest encryption and mobile device validation standards, your organization can choose to increase its security level to include user identity validation with the Two-Factor Authentication option and LAN architecture protection with our unique Access Defender™ solution.

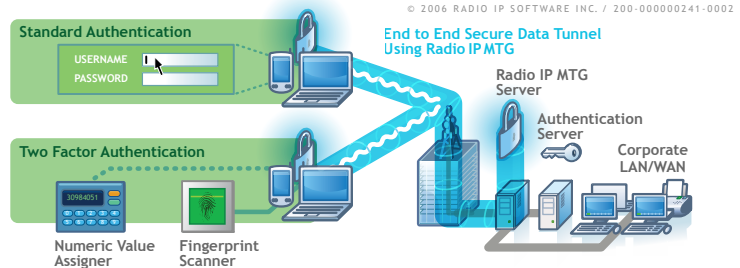
Two-Factor Authentication

As an additional layer of security on top of standard Windows logon authentication, Radio IP MTG can provide two-factor authentication to validate user identity. Typically, strong two-factor authentication mechanisms combine something that the user knows with something that the user has. A password is something that a user knows. After keying in their standard login credentials (username/password), which of course will always be sent over the air in an encrypted state,

users can now be equipped with a token key and software that assigns temporary keys. Radio IP MTG will communicate with a RADIUS server to confirm the key. Other methods

of two-factor authentication that you may choose to leverage include biometrics, which utilize a user's personal characteristics such as fingerprints.

User Authentication



Access Defender™

Is your mobile workforce connected to public networks such as cellular or public broadband networks? Are you concerned about intruders trying to negatively impact your LAN, using methods such as “denial of access” or “buffer overrun”? Access Defender is an additional security gate that removes the

vulnerability associated with using public IP networks. By residing between two firewalls, Access Defender scrutinizes and quarantines all incoming communication attempts, allowing the LAN to give access to your mobiles rather than letting the mobiles initiate the access to the LAN.



For more information on our security options, or other wireless connectionware solutions, contact us at: info@radio-ip.com

Toll Free: 877-717-2242 • Phone: +1 514-890-6070 • Fax: +1 514-890-1332

www.radio-ip.com

