

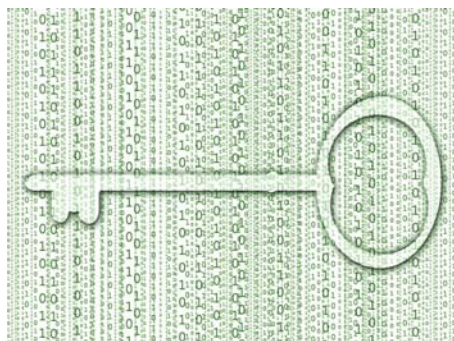
Red Condor's TLS Encryption Service

Available at No Cost on all MAG-Series Appliances and Hosted Service



Secure Email Communications with TLS Encryption

Although email is a key communications tool, it still involves risks and relies on insecure transport protocols. Intellectual property or other sensitive information such as contracts, transactions, social security numbers, birthdates, credit card numbers and bank account numbers may be intercepted and then read, deleted or altered before the email reaches its intended destination. Organizations can find additional security and privacy assurance by implementing the Transport Layer Security (TLS) encryption and authentication protocol.



TLS is a variation of the Secure Sockets Layer (SSL) protocol that is used to protect Web traffic. Using TLS to encrypt communications between two email gateways has a number of security benefits. First, each mail server authenticates to the other, making it harder to send spoofed email. Second, the contents of the emails sent between the two servers are encrypted, protecting them while in transit. Finally, the encryption of the conversation

between the two hosts makes it exceedingly difficult for an attacker to tamper with the email's contents.

Red Condor's TLS Encryption feature (now available at no charge) ensures the complete confidentiality of email communications and content. It works by establishing private email networks linking our users with their business-critical partners via the use of certificates. Every single email sent or received by these networks is fully and securely encrypted, and the encryption remains completely transparent to both sender and recipient.

How Does TLS Work?

A TLS client and server negotiate a connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish the connection's security including the CipherSuite, digital certificate and session keys. Once the handshake is completed the connection is secure and the session keys are used to encrypt and decrypt data until the connection is closed. If at any point during the handshake a step fails then the handshake fails and the connection is not created.

Red Condor's TLS Encryption benefits include:

- Secure email passage between sender and recipient networks
- Total data security with full compliance with privacy regulations
- Protection of the confidentiality of every part of every email message sent and received
- No effect on end users and no complicated message retrieval procedures needed
- The configuration flexibility you need with simplicity and ease of use

**TLS now available at
no additional charge!**

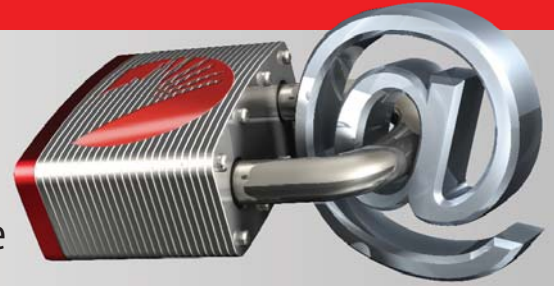


Security | Service | Simplicity

888-9NO-SPAM
www.RedCondor.com

Red Condor's TLS Encryption Service

Available at No Cost on all MAG-Series Appliances and Hosted Service



Important Steps to Establishing TLS with Red Condor

- Get a digital certificate to identify your email server
- Designate the mail domains you want encrypted
- Identify the partners you want to exchange encrypted communications with
- Enable boundry encryption and have Red Condor set up a secure private email network that uses TLS encrypted tunnels
- All emails sent between your mail server, Red Condor and your designated partners travel via this network
- Red Condor authenticates mail server certificates, with messages only sent to authenticated servers
- Red Condor ensures the integrity of the encrypted communications and applies any additional service settings that are needed

TLS Features and Benefits

Features	Benefits
TLS encrypts the email connection between sender and recipient network boundaries.	Secures email passing between sender and recipient networks, facilitates compliance with privacy regulations.
Can be configured to not send the message if a secure connection cannot be established. Can use TLS by domain and do not have to enable across the board.	Gives you the configuration flexibility you need.
Fully encrypts every email sent and received.	Ensures total data security with full compliance with privacy regulations.
Encrypts email header, subject, body and attachment.	Protects the confidentiality of every part of email messages sent.
Encrypts email only as it passes between mail servers, the most vulnerable stage of transmission.	End-users are completely unaffected and no complicated message retrieval procedures are needed.
TLS authentication of mail servers is based on genuine authority-signed certificates.	Ensures that encrypted email is only sent to the correct destinations.
Automatically and consistently applies your encryption policies.	End users do not need to take any special actions.
Simpler than other solutions in the marketplace.	Don't need a large IT Staff to have encryption enabled.
Works seamlessly with Red Condor email security services.	Meet all of your email security needs with one provider – at no additional charge.

Learn more about how Red Condor's TLS Encryption can help your organization by calling 1-888-9NO-SPAM or emailing us at info@redcondor.com!



Security | Service | Simplicity

888-9NO-SPAM
www.RedCondor.com