



Encryption and Secure Critical Messaging Devices

This document discusses message encryption for American Messaging Services secure critical messaging devices.

The American Messaging infrastructure provides message encryption for several critical messaging devices. For these devices, encryption is configured per address/capcode. A device can receive both encrypted and non-encrypted messages.

To protect the message, encryption and/or security methods (explained further below) must be used by the sending protocol, the received network and the protocol used over the RF transmission system (over-the-air).

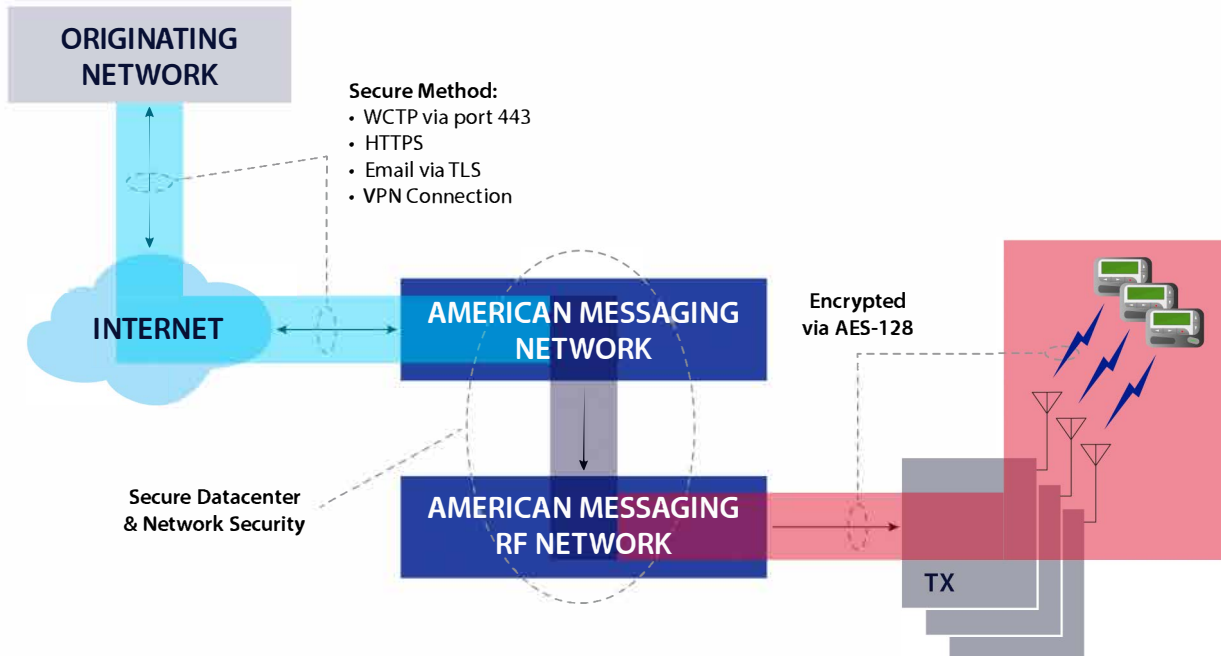
First, we will discuss the **methods for sending a message** to the American Messaging network. It is very important to know **how** the messages are being sent to the American Messaging network. The table below lists some of the various methods that can be used to send messages to all American Messaging critical messaging devices. Some of these methods are secure and some are not.

#	DESCRIPTION	METHOD	PROTOCOL (Port)	SECURE
1	Email	<10 digit #>@criticalmessaging.net	SMTP	No
2	Email using TLS*	<10 digit #>@criticalmessaging.net	SMTP (TLS)	Yes
3	Wireless Communications Transfer Protocol (WCTP) using port 443**	https://wctp.criticalmessaging.net	WCTP (443)	Yes
4	Send a page Website using SSL	https://criticalmessaging.net	HTTPS (443)	Yes
5	Simple Network Paging Protocol (SNPP) using port 444	snpp.criticalmessaging.net	SNPP (444)	No
6	VPN Connection	Any of the above methods	All	Yes
7	TAP	Modem	TAP	No

*SMTP via TLS requires auto negotiation from your email server. Please verify with your IT Department.

**This url only allows TLS 1.2 and 1.3. American Messaging recommends WCTP using port 443 as a best practice.

The diagram shown below illustrates the network components and the paths that the message follows.



To ensure that the message is secure over the internet, the **sending network must use a method that is secure**. This is shown in the light blue section of the diagram. There are four (4) methods listed in the table above that use encryption. Using one of these methods ensures that the messages are secure **between the sending network and the American Messaging network**.

Next, shown in the dark blue section of the diagram, the American Messaging data center, network and servers holding the messages must be secure. The American Messaging data center and network are secured by the following methods:

- 1) Internet facing connections are secured via firewalls
- 2) All network devices and servers are password protected
- 3) Servers where messages are stored have encrypted hard drives
- 4) Messages are deleted after 72 hours
- 5) Applications that are used for troubleshooting only display first and last five (5) characters of the message unless you have special system privileges
- 6) Data center facility has electronic key access with limited access
- 7) Data center has video monitoring

Lastly, shown in the red section of the diagram, the message must be secure over the RF transmission system. Once the message arrives at the American Messaging network, the critical messaging device number is looked up in the subscriber database and the configured subscriber attributes are applied. If the PIN is configured for encryption, then the message is encrypted, formatted for the device, and sent over our RF transmission system.

To encrypt the message for the RF transmission system, American Messaging uses a method called AES-128, which is a symmetric-key algorithm. This method uses the same 128 bit cryptographic keys for both encryption of the plaintext and decryption of encrypted text (ciphertext).

To summarize, in order to secure messages going to a critical message device, messages sent to American Messaging need to be encrypted, the message at rest in the American Messaging Data Center must be protected and messages sent over the RF transmission system need to be encrypted.