Critical Messaging Best Practices for Reliability and Security

As your trusted provider of critical messaging services, American Messaging wanted to take this opportunity to provide you with an outline of best practices for connecting and sending messages to our wireless paging network.

To reduce the risk of delays, outages and SPAM related message failures, it is important to utilize the most secure, reliable and redundant message delivery protocols to the American Messaging network. The following is an overview of available industry technologies and our recommendation's for best practices.

American Messaging accepts TAP, SMTP, SNPP and WCTP protocol messages, using IP, VPN or PSTN connections. Below are explanations of each of these options and our suggested method of sending for optimum network performance.

Sending Protocols

TAP – Telocator Alphanumeric Protocol - (TAP) is an industry-standard protocol for sending short messages via a land-line modem to a provider of pager and/or SMS services, for onward transmission to pagers and mobile phones. TAP relies on ASCII protocol (clear text) transmitted over modems to a phone line. Because the protocol relies on modems, processing transactions is inherently slower and there is an ever-present danger of modem failure or lock-up on either end. Messages are not secure. This is not a desired protocol for sending critical or secure messages, unless connected internally to a local CMS (on-campus Critical Messaging System).

SMTP - Simple Mail Transfer Protocol - SMTP is the least preferred method for delivery of messages. SMTP pages ride the email highway to American Messaging, which may include numerous ISP's along the way to message delivery. Potential for delays exist within each ISP's network and at transfer points between providers. Because SMTP is the main vehicle for SPAM, customers open the door to random attacks. While American Messaging makes every effort to protect our subscribers from unwanted SPAM and the effects of "denial of service" attacks, the SPAM world continues to reinvent itself with new and different methods of getting around even the most sophisticated SPAM filters. If feasible, non-dialable PIN's can be used as addresses for mission-critical messages. Because the PIN's are not open to the public, unwanted SPAM attacks are avoided.

SNPP – Simple Network Paging Protocol - The SNPP protocol remains the preferred, primary method of message transmission in the secure environment (VPN to American Messaging). This will provide the fastest delivery of pages, even in a high-traffic, emergency situation. To install diverse redundancy, a customer may opt to deliver messages in SNPP protocol via a VPN, with back-up delivery in SMTP or TAP protocol over the secure VPN tunnel.

WCTP – Wireless Communications Transfer Protocol - The WCTP format offers a high level of message security. Customers send encrypted messages from their WCTP client, over port 443 to our WCTP gateway, in HTTPS (Hypertext Transfer

Protocol Secure), over SSL (Secure Sockets Layer) protocol. We can create a VPN tunnel to provide end-to-end security from the customer's environment to American Messaging for that important "first hop" in message delivery.

Connection Options

IP – Internet Protocol - The **IP** is the principal communications protocol or relaying datagrams across network boundaries with the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers.

VPN – Virtual Private Network - Used to extend a private network across a public network (i.e., the Internet), while maintaining the security of the private network. Dedicated connections are used to establish a point-to-point "virtual tunnel" between the sender and receiver (customer and American Messaging). This is a highly secure, dedicated (fast) connection that can be encrypted.

PSTN – Public Switched Telephone Network - The **PSTN** is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication.

Suggested Method of Sending

The recommended solution for secure, fast and reliable delivery of critical messages includes SNPP as the primary protocol sent via VPN from the customer to American Messaging. Redundancy can be established using a different protocol (such as any of those listed above) over the VPN, or for further diversity, the WCTP protocol can be added using any other local Internet Service Provider.

Dispatching Messages

Legacy dispatch systems are acceptable as long as the connection is secure. Secure web applications such as Message Manager allow custom message management for sending, receiving and managing messages.

Future Development for SMTP Messaging

American Messaging is currently developing a new system to aid customers who can only send messages using SMTP. This system will be based on a "known sender list". Customers will advise American Messaging of the IP addresses in use to generate pages. Additionally, the system will capture IP addresses sending to the same pager or PIN number over periods of a few days, and then assign those IP addresses to the customer's list based on the pager/PIN number. In the event of a denial of service attack, IP addresses on the list will not be randomly blacklisted. During a denial of service attack, we will shift to only accepting inbound messages from the Known Sender List, discarding all other traffic. This should greatly reduce the load on our SPAM filters, allowing Known Sender

messages to move through the system quicker. We plan to have this new system ready for beta-testing before the end of April 2015. This will not eliminate the potential for other SMTP delays that are outside of American Messaging's control.

Secure Critical Messaging

In order to provide encryption from the message origination point to the message receive point, both the application that is sending the message and the application that is receiving the message must be able to encrypt and decrypt the message.

The CUE

The CUE can receive and save encrypted messages from the AMS system on a per capcode basis. The CUE Secure Messaging System uses a version of the Secure Paging Layer (SPL) protocol to *encrypt* and *decrypt* messages. SPL messages consist of a header followed by an encrypted payload. The payload consists of a CRC32 checksum, a type code, a random byte field used for spoiling and aligning the message, and the message. The payload (CRC, type and spoiler data, and the message) are encrypted using AES-128 in CBC mode, prepended with the header. The CUE Secure Messaging System also uses multiple Encryption Keys that are used in a rotating sequence. The CUE device automatically detects the encrypted messages; and therefore, does not have to be configured/programmed for encryption.

The Network

All message content is stored within an American Messaging Data Center, which is physically behind locked doors that require security clearance access. The network servers located in American Messaging's Data centers are behind firewalls with restricted access. Message content is retained for a period of no more than seventy-two (72) hours depending upon system capacity limitations. The message content is retained as a resource for solving system issues. Message content at rest is encrypted on American Messaging's servers that process paging traffic. While in storage, at no time is message content accessed by American Messaging except, as indicated above, for network problem detection and resolution. In dealing with network problems, American Messaging may access an offending message that has distressed the network. This is done to protect our network from excess traffic that could have an adverse impact on all our customers.

In summary, our objective is to provide the most reliable, redundant and secure connection options to our wireless messaging network. As your trusted provider of critical and secure messaging services, we would be happy to schedule a call or personal visit to further discuss these options and begin the process of implementing best practice solutions. Please contact your Account Manger to set up a meeting.