About Transport Layer Security (TLS)

Transport Layer Security (TLS) secures emails transmitted over the internet using standard encryption technology. Securing emails this way reduces the risk of interception, eavesdropping and mail forgery.

TLS has proved to be a stable and reliable service that requires no intervention by the email sender or receiver once it is available on both parties’ email servers. This means that both the sender and receiver can send and receive emails as they currently do today. For these reasons TLS is fast becoming an industry standard.

Enforced/Forced/Mandatory TLS is a configurable TLS policy setting which authenticates the destination email domain as a trusted source in addition to following the TLS process. This ensures the email is only sent if the email can be transmitted securely and the source is trusted.

How does TLS work?

To work, TLS needs to be enabled on the mail servers of both the sender and the receiver of the email. Any information exchanged between the servers is encrypted, including the subject line, text and any attachments. When sending encrypted messages, the mail exchange works as follows:

- When the sender connects to the recipient, the system automatically checks whether TLS is enabled on the client’s mail server
- If TLS is enabled at both ends, a secure TLS connection is established by using a ‘handshake’ procedure
- During the handshake, TLS certificates are exchanged. If the sender’s server trusts the certificate from the client mail server, the TLS session starts, and the email is sent via a secure internet connection

Checking a domain to see if they are TLS compatible

https://www.checktls.com/TestReceiver

GHX EIPP/OnDemand AP

TLS Email System Information

GHX IT Technical Contact (Name, title, email, phone number, etc.)	
Email Domain(s) that will require TLS	ghxinvoicing.com
Hostname/IP of GHX/FS Inbound[i] Email Server(s)	inbound-smtp.us-east-1.amazonaws.com inbound-smtp.us-west-2.amazonaws.com* *DR Instance configured in emergencies
GHX/FS Outbound[ii] Email Server(s) (Hostname/IP)	N/A
Certificate Authority that issued Certificate(s)	Amazon Web Services (AWS)
FQDNs fully qualified domain name(s) destination mail server(s); used to validate certificate(s).	inbound-smtp.us-east-1.amazonaws.com inbound-smtp.us-west-2.amazonaws.com
GHX/FS maximum permitted message size (MB)	30 MB

Customer Email System Information

Customer IT Technical Contact (Name, title, email, phone number, etc.)	?
Customer Email Domain(s) that will require TLS (Please specify if subdomains should be included)	?
Hostname/IP of customer Inbound[i] Email Server(s)	?
Customer Outbound[ii] Email Server(s) (Hostname/IP)	?
Certificate Authority that issued your Certificate(s)	?
FQDNs Please provide the fully qualified domain name(s) of your destination mail server(s); we will use these to validate your certificate(s).	?
Your maximum permitted message size (MB)	?