

## 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 your email domain to determine the email service provider being utilized. This information can be helpful to search for instructions on how to update TLS within your email service provider.

<https://mxtoolbox.com/SuperTool.aspx>

The screenshot shows the MX Toolbox SuperTool interface. The browser address bar displays `mxtoolbox.com/SuperTool.aspx`. The navigation menu includes **SuperTool**, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. The main input field contains `ghx.com` and an **MX Lookup** button. Below the input, there are two buttons: **Find Problems** and **Solve Email Delivery Problems**.

Pref	Hostname	IP Address
0	ghx-com.mail.protection.outlook.com	Microsoft Corporation (AS8075)

  

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓	DNS Record Published	DNS Record found

Your email service provider is "Microsoft Office" [Need Bulk Email Provider Data?](#)

Checking a receiving domain to see if they are TLS compatible

<https://www.checktls.com/TestReceiver>

# GHX EIPP/OnDemand AP

## TLS Email System Information

<b>GHX IT Technical Contact</b>  (Name, title, email, phone number, etc.)	GHX Support <a href="mailto:support@ghx.com">support@ghx.com</a> 800.YOUR.GHX (1-800-968-7449)
<b>Email Domain(s) that will require TLS</b>	ghxinvoicing.com
<u>Hostname/IP of GHX/FS Inbound[i] Email Server(s)</u>	<a href="https://inbound-smtp.us-east-1.amazonaws.com">inbound-smtp.us-east-1.amazonaws.com</a> inbound-smtp.us-west-2.amazonaws.com* <small>*DR Instance configured in emergencies</small>
<u>GHX/FS Outbound[ii] Email Server(s) (Hostname/IP)</u>	N/A
<b>Certificate Authority</b> that issued Certificate(s)	Amazon Web Services (AWS)
<b>FQDNs</b>  fully qualified domain name(s) destination mail server(s); used to validate certificate(s).	<a href="https://inbound-smtp.us-east-1.amazonaws.com">inbound-smtp.us-east-1.amazonaws.com</a> inbound-smtp.us-west-2.amazonaws.com
<b>GHX/FS maximum permitted message size (MB)</b>	30 MB