TLS with Insecure Ciphers and SSLv2/SSLv3 No Longer Supported

https://campus.barracuda.com/doc/96022999/

In an effort to provide a more secure email environment, TLS 1.0 and 1.1 will be disabled on **November 30, 2020**.

Transport Layer Security (TLS) provides secure transmission of email content, both inbound and outbound, over an encrypted channel using the Secure Sockets Layer (SSL). Various vulnerabilities in past years have exploited security issues due to insecure ciphers and outdated protocols. Email Gateway Defense (EGD) no longer supports the following insecure cipher suites for TLS:

- ECDHE-ECDSA-DES-CBC3-SHA [1.0]
- ECDHE-RSA-DES-CBC3-SHA [1.0]
- DHE-RSA-DES-CBC3-SHA [1.0]
- AES256-GCM-SHA384 [1.2]
- AES128-GCM-SHA256 [1.2]
- AES256-SHA256 [1.2]
- AES256-SHA [1.0]
- AES128-SHA256 [1.2]
- AES128-SHA [1.0]
- DES-CBC3-SHA [1.0]

EGD no longer supports TLS v1.0 and v1.1.

EGD also no longer supports SSLv2 and SSLv3 protocols.

If you are still using any of the above, you will run into connections issues sending or receiving mail through EGD. Devices sending mail through EGD that are using TLS with insecure ciphers can encounter handshake errors on connect or general connection failures.

Possible solutions include:

- Updating your SSL services.
- Turning *OFF* TLS.
- Routing mail through a valid mail server before it comes to EGD.

As a best practice, you should configure your devices to use the latest protocol versions to ensure you are up to date on privacy, security, and performance improvements.

To disable TLS v1.0 for inbound connections on your Microsoft Exchange Server, use the Receive connector in the Exchange Admin Center interface.

To disable TLS v1.0 for outbound connections on your Microsoft Exchange Server, use the PowerShell command: `Get-SendConnector -Identity 'SendConnectorName' | set-SendConnector -IgnoreSTARTTLS: $true`

For more information on how to update your Microsoft Exchange version to support TLS v1.2, see the Microsoft article Exchange Server TLS guidance.

Contact Barracuda Networks Technical Support if you are unsure of the TLS version you are running.

> The plan to disable TLS 1.0 and 1.1 was originally scheduled for earlier this year with a notice posted on January 9, 2020. However, on April 20, 2020, we postponed this planned change due to the unprecedented circumstances surrounding the global pandemic.