TLS with Insecure Ciphers and SSLv2/SSLv3 No Longer Supported

https://campus.barracuda.com/doc/91981918/

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 Various vulnerabilities in past years have exploited security issues due to insecure ciphers and outdated protocols. As a result, Barracuda Email Security Service (ESS) 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]

ESS also no longer supports SSLv2 and SSLv3 protocols.

If you are still using any of the above insecure ciphers, you will run into connections issues sending or receiving mail through ESS. Devices sending mail through ESS 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 ESS

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.