PACKETFUSION
Connecting the Dots to the Cloud™

Mitel Connect and TLS 1.2

TLS 1.2 is supported in Connect as of release 19.2 - 22.13. 4800.0 which was Generally Available (GA) November, 2020. Packet Fusion is currently running this version of code and has enabled TLS 1.2 with no issues.

What do you need to do to take advantage of TLS 1.2?

1. Upgrade to the current connect build.
2. Make sure there are no older SG vintage switches in your environment as they do not support TLS 1.2: (SGT1K, SG30, SG50, SG50V, SG90, SG90V, SG220T1, SG220T1a, SG24a).
3. Mitel's initial stance is that MGCP will not support TLS 1.2, so all MCGP phones will not be supported (IP110, IP115, IP230, IP230G, IP265, IP560, IP560G, IP565G, IP655). We have requested confirmation as to whether TLS 1.2 and MGCP can run simultaneously and we will provide additional information as it becomes available.
4. The physical switches that support TLS 1.2 are: ST1D, ST2D, ST24a, ST48a, SG50A, ST100A, ST100DA, ST200, ST500
5. All virtual switches support TLS 1.2

TLS 1.0, while not as secure as 1.2, will be supported in Connect until the SG switches reach End of Support which is slated for some time in 2024.

Connect will auto-negotiate TLS 1.2 and if all is good, TLS 1.2 is adhered to. If there is something in your network that doesn't support TLS1.2, it will then try TLS 1.0. There is no way to turn off TLS 1.0 in the current release. There will be a check box in the next release due out in Q1 2021 that will turn off TLS 1.0.

TLS 1.2 is not new to Mitel as both the Edge Gateway and Mobility Router utilize it.

If you have any questions, please reach out to us for a one on one discussion about the topic.

Are you a ShoreTel customer? Get more info here. https://www.packetfusion.com/shoretel-phone-system/

Get more info on Mitel Connect: https://www.packetfusion.com/mitel-support/