



Notification on Transport Layer Security (TLS) Version 1.2 Upgrade

1. What Is TLS

SSL stands for Secure Sockets Layer and was originally created by Netscape. SSLv2 and SSLv3 are the 2 versions of this protocol (SSLv1 was never publicly released). After SSLv3, SSL was renamed to Transport Layer Security and started with **TLSv1.0** which is an upgraded version of SSLv3.

2. TLS v1.2 Upgrade

Changes have been made to the test environment at:
(<https://tracsuat.hud.gov:9001/IMAX-WS/access>) to use the following ciphers:

- ∴ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and
- ∴ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

It is critical to upgrade, if HUD were to continue with the current TLS version, it will put HUD and our external business partners at risk, including financial transactions as there are unaddressed security vulnerabilities.

3. March 27, 2023 Deadline for TLS v1.2 Upgrade

TLS ciphers are scheduled for production implementation during the weekend of Saturday, March 25th and Sunday, 26th, 2023. To avoid potential rejection of TRACS electronic files without TLS v1.2, please upgrade your occupancy software to address this issue prior to March 27, 2023.

4. Multifamily Housing Help Desk Support 1-800-767-7588 or TRACS@hud.gov

You will be able to reach a Help Desk Analyst during normal business hours or you can leave a voicemail or email message requesting technical assistance.