Updating to TLS 1.2 for Eval25

Last Modified on 09/21/2023 12:59 pm PDT

In March of 2017, some Eval25 Users were notified that CollegeNET's security auditors require us to eliminate the use of outdated encryption standards TLS 1.0 and 1.1. In the near future, we will no longer support TLS 1.0 or 1.1, and only support the use of TLS 1.2.

Your institution may potentially be affected by this change, particularly in relation to the use of Eval25 and the Eval25 GradeHook web service. Please perform the following to continue to successfully connect to both Eval25 and the Eval25 GradeHook:

1. Upgrade to Java 8

https://www.java.com/en/download/

2. Ensure Your Users are on a Recent Browser Version

The following browser versions support TLS 1.2:

- Android 5 (or 4.1 with non-default configuration enabled)
- Chrome 30
- Firefox 27
- Internet Explorer 11
- Opera 17
- Safari 7 (5 for Safari Mobile)

3. Verify That Your Client Encryption Software Supports ECDHE Ciphers

If not, you will need to upgrade it.

4. Use one of the Following Acceptable TLS 1.2ciphers

This is recommended for safety and performance reasons,

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  ECDH secp256r1 (eq. 3072 bits RSA) FS 256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  ECDH secp256r1 (eq. 3072 bits RSA) FS 128
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
  ECDH secp256r1 (eq. 3072 bits RSA) FS 256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
  ECDH secp256r1 (eq. 3072 bits RSA) FS 128

If you have any questions, please contact the Eval25 Support Team. The Support Team can be reached directly from

within Eval25 by clicking on the Help link in the upper right corner of the application header. Search the help articles and community conversations for answers to common questions, or email support@collegenet.com to initiate a support ticket with us.