Fannie Mae

Uniform Closing Dataset (UCD)

Fannie Mae to Disable TLS 1.0/1.1 for UCD Environments

Fannie Mae will implement changes to only allow TLS 1.2 (and strong cipher suites) in the UCD Production Environment on **January 26th, 2019**. Shakeout testing recommendations are below.

> **NOTE:** *Shakeout testing is mandatory in both UCD CLVE Test and UCD Production environments.*

- TLS 1.2 enforce the following cipher suites below.

    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Testing: All are expected to perform shakeout testing and communicate results. Details of timing for change and shakeout windows will be communicated soon.

- You may be required to make a configuration change in your systems/applications to enable TLS 1.2 and strong ciphers,
- You will need to disable TLS 1.0 and 1.1

No action is needed if you are able to submit files into the new UCD CLVE Test Environment successfully.

> **NOTE:** *Failure to support TLS 1.2 (and ciphers) will not allow you to connect to the B2B Gateway. We strongly encourage you to test in the B2B UCD Test Environment to determine the scope of changes they will need to make in UCD Production.*

Contact integration_support@fanniemae.com for questions.