KAKAPO SYSTEMS

TLS COMPATIBILITY OVERVIEW

Protocol or Cipher suite mismatch

When Unity Client connects to CTI/OCI over TLS, it is important that both client and server agree upon a common security protocol and cipher suite for secure communication. When a client machine and Broadworks server (CTI/OCI) do not have a common supported protocol or a corresponding common cipher suite, Broadworks server will sever the incoming connection as per the normal TLS handshake procedure.

TLS protocols and cipher suites must be configured on the XSP by the Broadworks provider. TLS protocols and cipher suites should be selected carefully to ensure maximum security, compatibility and performance.

When only the latest/strongest security protocols and cipher suites are enabled on the Broadworks platform, then some Unity clients running on old Windows machines may not be able to connect to the Broadworks platform over TLS. This is because the latest cipher suites may not be installed on the PC, and the server doesn't support the older cipher suites installed on the PC. *Configuration of cipher suites on the server side should be largely similar to how they are configured when securing a web server over TLS*. A link is provided in the references below which may have some pointers to select secure cipher suites.

If Unity Client is able to connect to Broadworks on the TLS port specified but the server severs the connection during TLS handshake, it may be due to a security protocol mismatch or a cipher suite mismatch. SSL analyzer tools such as https://sslanalyzer.comodoca.com/ can be used to confirm the TLS protocols and cipher suites enabled on the Broadworks platform, assuming public access is available.

We can also know the cipher suites enabled in the machine where unity client is running by referring following MSDN links.

Windows Version	Link
Windows Vista	https://msdn.microsoft.com/en-us/library/windows/desktop/ff468651(v=vs.85).aspx
Windows 7	https://msdn.microsoft.com/en-us/library/windows/desktop/mt767780(v=vs.85).aspx
Windows 8	https://msdn.microsoft.com/en-us/library/windows/desktop/mt762882(v=vs.85).aspx
Windows 8.1	https://msdn.microsoft.com/en-us/library/windows/desktop/mt767781(v=vs.85).aspx
Windows 10 v1507	https://msdn.microsoft.com/en-us/library/windows/desktop/mt767769(v=vs.85).aspx

Windows 10 v1511	https://msdn.microsoft.com/en-us/library/windows/desktop/mt767768(v=vs.85).aspx
Windows 10 v1607	https://msdn.microsoft.com/en-us/library/windows/desktop/mt490158(v=vs.85).aspx
Windows 10 v1703	https://msdn.microsoft.com/en-us/library/windows/desktop/mt808163(v=vs.85).aspx
Windows 10 v1709	https://msdn.microsoft.com/en-us/library/windows/desktop/mt813794(v=vs.85).aspx

Common Scenarios

Unity Clients running on a Windows Vista machine will not be able to connect to a Broadworks server over TLS if only TLS 1.2 is enabled on the server. This is because Windows Vista only supports up to TLS 1.0.

If the Broadworks server supports only a single cipher suite “TLS_DH_anon_WITH_RC4_128_MD5”, Unity client will not work on any Windows PC, as this cipher suite is not available on any windows version and cannot be added or enabled.

If the Broadworks server supports only a single cipher suite “TLS_RSA_WITH_RC4_128_MD5”, Unity client will work on all Windows versions except Windows 10 v1709. As described in the above link (Windows 10 v1709), this cipher suite is shipped with this version of Windows, but is not enabled by default. It can be enabled on client side by running a Powershell command as administrator on the local PC, although this will only resolve the issue for that PC. The Powershell command to run is

Enable-TlsCipherSuite -Name "TLS_RSA_WITH_RC4_128_MD5"

However, the best recommended practice is to ensure the below cipher suites are enabled on all OCI and CTI servers that are configured to use TLS for secure connectivity:

- TLS_RSA_WITH_RC4_128_MD5
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

This will ensure that the Broadworks servers are configured with sufficient flexibility to meet the security policies set on most Windows PCs, thereby allowing Unity client to connect over TLS. This recommendation is given without prejudice, you should consult with Broadsoft before making any changes on the server.

References

TLS handshake: - https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513(v=vs.85).aspx

Use Secure Cipher Suites: - https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices#23-use-secure-cipher-suites