Configuring TLS 1.2

AVAILABLE IN 9.4 AND ABOVE

By default, all Verba services prefer TLS 1.2. For security or compliance reasons, administrators can choose to lock down the TLS version of the Verba system to 1.2, and therefore disable TLS 1.0 and TLS 1.1. This document provides an overview of how to enable TLS 1.2 and disable TLS 1.0 and 1.1 for the Verba product.

Component	How to Configure TLS 1.2
Internal communication between Verba servers and components	**Step 1 -** Ensure that TLS 1.2 is not disabled on the Verba servers **Step 2 -** Open the Web Application and navigate to **System\Servers** and select the server **Step 3 -** Select the **Change Configuration Settings** tab, **Server Certificate** - **Advanced TLS Settings** node **Step 4** - Set **Enable TLSv1** and **Enable TLSv1.1** to **No,** and **Enable TLSv1.2** to **Yes** **Step 5 -** Save the changes and click on the **click here** link to apply the changes
Additional configuration for the following services: Verba Avaya DMCC/JTAPI Service Verba Cisco Central Silent Monitoring Service Verba Cisco Compliance Service Verba Cisco JTAPI Service	**Step 1 -** Go to the Java home directory **Step 2 -** Open the **conf/security/java.security** or **lib/security/java.security** (JDK 8 and earlier) file using notepad with elevated permissions **Step 3 -** Change the jdk.tls.disabledAlgorithms property by appending ", TLSv1, TLSv1.1" As an example: jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize < 1024, \ EC keySize < 224, 3DES_EDE_CBC, anon, NULL**, TLSv1, TLSv1.1** **Step 4 -** Save the changes **Step 5 -** Restart the impacted Verba Service
HTTPS connection with the Web Application	Follow the instructions on all Media Repository Servers: **Step 1 -** Go to **C:\Program Files\Verba\tomcat\conf** **Step 2 -** Create a backup of the **server.xml** file **Step 3 -** Open the **server.xml** file using notepad with elevated permissions **Step 4 -** Change the value of the SSLProtocol from **"TLSv1+TLSv1.1+TLSv1.2**" to **"TLSv1.2"** **Step 5 -** Save the changes **Step 6 -** Restart the **Verba Web Application Service**
Encrypted SQL Server communication	Follow the information in the following article: https://support.microsoft.com/en-gb/help/3135244/tls-1-2-support-for-microsoft-sql-server To enable encrypted communication with the SQL Server in Verba, follow Configuring encryption for database connections
Communication between the installer and the Web Application during certificate generation	The installer uses TLS 1.2 by default when requesting certificates from the Verba CA.
Verba Microsoft Teams Bot Service's HTTPS listeners	

The TLS 1.0 and TLS 1.1 protocols need to be disabled OS level on the servers hosting the bot service. To disable the TLS 1.0 and TLS 1.1 protocols on Windows follow the instructions:
Step 1 - Add the following registries on all bot servers:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000
```

The following .reg file contains the above registries and it can be simply run on the servers:

Step 2 - Restart the **Verba Microsoft Teams Bot Service**