# Customer Has Inquiries Around TLS 1.2 and Disabling TLS 1.1/1.0

09/19/2025 11:08 am EDT

***Will it affect its operation?***
This is largely dependent on which version of SedonaSync you are using and if you are utilizing any other applications running on the same server that are dependent on those TLS ciphers. The SedonaSync application is created by ECI, and they have confirmed that version 9 of the product will not support newer versions of TLS. However, Version 10 will.
You can confirm which version you have by how it is accessed. Applications based is version 9 [Monitor, Event Viewer, etc], Web portal via browser is version 10.

As long as you are on Version 10 of Sync and do not have any other 1st or 3rd party software relying on TLS 1.0 on the server in question, you should not have any issues disabling that specific cipher/protocol on the server.

For reference, the latest versions of SedonaOffice and SedonaWeb 1.0 and 2.0 are TLS 1.2 compatible and do not rely on TLS 1.0. compatibility if properly setup. TLS updates were noted in the following releases.
SedonaOffice version 6.2.0.19 released Q1 2025 https://dyzz9obi78pm5.cloudfront.net/app/image/id/67c0ce75dfbfb316a50aef8a/n/sedonaoffice-62019-rev-4-release-notes.pdf
SedonaWeb 1.0 version 2.7.82 released Q1 2024 https://sedonaoffice.knowledgeowl.com/help/release-notes-sedonaweb-10-0f50811
SedonaWeb 2.0 version 1.44 released Q2
2023 https://dyzz9obi78pm5.cloudfront.net/app/image/id/66194bfcdd21e73bb321e959/n/sedonaweb20-release-notes-1440-ver2.pdf

Deprecated items such as Legacy FSU, SedonaAPI 1.0, etc would need to be migrated to their newer variants Sedona X, Sedona Web 2.0 and ensure the entire environment from SQL Server to any dependent servers are all compliant TLS 1.2 where applicable.

***Do you think you'll be able to disable it?***
BoldGroup does not configure/change Windows Security/OS Options in Enterprise environments. The best way for your team to test the change is to assess what applications are running on the impacted server and the stakeholders who access/update/validate applications on the server:

- Clone the desired server virtually if possible
    - Simulate the change
        - If all validations pass on the virtual system for a set monitoring period, proceed with production
        - If any validations fail, list and assess if they present a go/no-go scenario for your team

Alternatively

- Plan a maintenance period
    - Ensure you have snapshots and backups of all data - Disable the ciphers temporarily
        - Reboot the required server(s) /workstations
            - Have your stakeholders test their reporting/automations configured within SedonaSync and any other dependencies on that server
            - If all validations pass for the set monitoring/maintenance period
            - If any validations fail, list and assess if they present a go/no-go scenario for your team to rollback using your snapshots

Please note: Test Servers/ Migrations are not covered under support. If you need assistance spinning up a test server outside of temporary licensing, you will need a quote with your Account Manager for project review.

Regards,