

SedonaOffice Server Upgrade, OS, and Migration Frequently Asked Questions

Last Modified on 10/22/2026 9:26 am EDT

At this time our Development & Product teams are not aware of any issues using SedonaOffice or SedonaWeb on any current versions of SQL Server or Windows OS 2019 or later. Not all SQL/OS combinations have been QA'd and certified. If this is standard OS patching or security/cumulative updates, your team will only need to ensure that the updates are not interrupted, as that can have impacts on the OS and DLL library integrity.

Typically, the only consideration you may need to factor in is if the upgrade/migration causes your Unique Program ID of SedonaOffice to change; if it does you will need a relicense of SedonaOffice by supplying the new Unique Program ID from the Server Utility License Activation wizards during support hours for a new license key.

If you are upgrading your SedonaWeb/API servers' OS, you will need to ensure that your DNS, IIS, and IPs configured remain the same and that their connection to your SQL Data is not impacted by your environment changes. If you do not have a rollback option and/or have issues following your in-place server upgrade, it will require a quote for a reinstallation/redeployment of impacted services.

There is not a specific order recommended between OS and SQL; however, priority is usually determined by which is most needed either in security or function. They should not be done in tandem and should have appropriate regression testing between the two based on your company's critical workflows. SQL tends to be faster of the two.

In-place Server upgrades have better success rates if the upgrade is not spanning more than 2-3 versions [e.g., upgrading from SQL2012 to 2025 would be considered higher risk]. Customers have reported issues upgrading from anything under 2012 R2 *or* more than 3 versions tend to result in various permissions/security and data variances. We recommend testing your desired changes/updates on a Test/UAT server with the latest server version you wish to go to and then migrating your data to that server. This will allow you to compare configurations in the event of any issues before completely archiving or removing the original server.

Whether your servers are virtual/cloud-based or physical, we recommend ensuring you have snapshots/images of them before proceeding with either the server upgrade or migrating Sedona DBs to a different server with the new SQL version. Customers using virtual systems reported they were able to clone their existing server and test the server upgrade prior to deployment in production to assess any potential issues, such as configuration or relicensing.

Frequently Asked Questions:

What are your current recommended hardware specifications? / Do you have a Hardware and Software Requirements document?

Minimum requirements are based on the number of users and environment type can be found here:

<https://sedonaoffice.knowledgeowl.com/help/sedonaoffice-minimum-hardware-software-requirements>

There is not a publicly available spec sheet for our hosted environments as they are offered either in Communal or Dedicated versions and typically provisioned to the access and needs of the business

What Microsoft OS versions does SedonaOffice currently support?

There is not an exhaustive list of compatible Microsoft Server and OS versions. Our current testing has not shown any issues through to Server versions 2025 and Windows 10. We have received reports of a visual issue with Workstations using Windows 11, utilizing multi-monitor (SedonaOffice may have visual tearing/artifing when moving sliders and internal Sedona windows).

Do you have any Network Provisioning Recommendations?

We recommend ensuring your Application Server(s), Workstations, and Web/IIS servers have SQL standard and dynamic port access. Beyond that, ensure that all machines can appropriately resolve the SQL server via DNS and IPv4 connections

<https://sedonaoffice.knowledgeowl.com/help/network-provisions-for-sedonaoffice-primary-integrations>

Are there any known issues with migrating all Sedona Office servers from VMware to Azure or Hyper-V?

There are no known issues with migrating server Hosts between VMware to Azure or Hyper-V. These specific tools are not currently employed by our Development or Infrastructure engineers, so Bold does not have the ability to certify functionality in these configurations. It is recommended that you test your migrations with all required stakeholders before full production deployments, as there can still be items in the environment that can impact use post-migration unique to your setup.

Does SedonaOffice support encryption at rest / TDE?

Transparent Data Encryption is a SQL Server feature and is described by Microsoft as encrypting/decrypting SQL Server data and log files at the I/O layer, transparent to the database application(without requiring application-level changes)

From the SedonaOffice side, our Development team has not specifically fully certified/QA'd all TDE use cases. We do not currently have a broadly certified standard deployment model for TDE across customer-hosted Enterprise environments or confirmation of its utilization, and thus would not expect TDE itself to change how SedonaOffice queries the database, as it works on the underlying SQL service. That said, TDE is still a SQL Server administration/security configuration item, and TDE can introduce measurable overhead(general performance hit) depending on workload, storage, CPU, and backup activity, so it is recommended to verify the disk IO resources and speed to maintain processing speeds, and may need server monitoring software in addition to workflow validation in your rebuilt environment before you go-live.

If you wish to enable TDE on any upgraded or rebuilt on-prem SQL Server, your IT and/or your MSP/DBA would need to own the SQL Server configuration, certificate/key management, backup strategy, recovery testing, and operational procedures. In particular, the TDE certificate and private key must be backed up and protected, because they are required for database restore/recovery.

- Without the key, if any type of server loss, corruption, ransomware event, or disaster recovery scenario happens beyond that point, your data cannot be restored in any other environment.

Does SedonaOffice support encrypted SQL connections / TLS 1.2

SedonaOffice release guidance for current versions indicates TLS 1.2 can be used when the environment meets the documented requirements, including supported Windows client/server versions, TLS 1.0/1.1 disabled, TLS 1.2 enabled,

required Microsoft .Net versions, and SQL Server configured to force encryption for SedonaOffice versions 6.2.0.14 and beyond. <https://sedonaoffice.knowledgeowl.com/help/sedonaoffice-release-notes-6201x>

To Use TLS 1.2 – Consider the following:

- All computers running SedonaOffice client must be on Windows 10 with the October 20, 2020 build, version 17763.1554 or later; the server must be on Windows Server 2019 or later.
- TLS 1.2 must be the only TLS version enabled in the Registry. TLS 1.0 and TLS 1.1 must be disabled. Verify they are disabled and TLS 1.2 is enabled.
- The SQL Server must be set to force encryption.

Supported Environments

Minimum System Requirements

- Server is on Microsoft .NET 4.6.1
- If used, SedonaWeb/SedonaAPI version 1.44.0 (or higher)

The larger risk is not usually SedonaOffice alone. It is anything else that connects to SQL Server. Before making encrypted connections mandatory, your team should inventory and test all SQL-connected use cases, including but not limited to:

- Reporting tools
- ODBC/OLE DB connections
- SedonaOffice client workstations
- SedonaWeb / SedonaAPI, if used
- Sedona Sync, especially older versions
- Legacy FSU or other legacy services, if present
- WeSuite, Vivid, QuoteWerks, or other third-party integrations
- Custom queries, jobs, linked servers, or automation
- Any MSP monitoring/backup tools that connect to SQL

Microsoft's SQL Server encryption guidance requires a SQL Server to have a valid certificate available for all encrypted connections and trusted on all machines/clients on the network accessing SQL data. The certificate procurement, installation, renewal tracking, DNS/name alignment, trust validation, and testing forced encryption in a non-production or staged environment first [using the same client versions, connection strings, DNS names, integrations, and workflows expected at go-live] would need to be handled by your IT or your MSP.

Does SedonaOffice Support SSO or Microsoft Entra?

SedonaOffice is an intermodal VB6 app and does not support Single Sign-On in any capacity in its current form. If SSO is enabled for the 1st/server login, it will not work for the 2nd login into the client app. This has been explored previously with Duo, Azure/Entra, and other avenues by Development. SSO for SedonaOffice has been raised with our Product Management team and is in discussions for the next generation of the application that will not be reliant on older .Net/VB6 code stacks.

Does BoldGroup provide the SQL license or do we need to provide that on our own?

We are not able to resell or provide a SQL license if you are migrating from one Enterprise Self-Hosted to another Enterprise Self-Hosted server. If you are migrating to our hosted AWS Cloud Solutions, SQL licensing is configured in

the server/instance spin-up.

How do we go about coordinating this upgrade or migration with you? / Is there any additional support cost to help upgrade or migrate to the new server?

OS/SQL Server Upgrades & Migrations & after-hours assistance, are not covered by support and require a quote for a project with your Account Manager in order to ensure SedonaOffice and your business-critical 1st-party integrations [e.g. SedonaWeb, Sedona X, Sedona Sync etc] are properly assessed, licensed, and scoped for the changes, along with any 3rd-party ones are coordinated [Blackleaf, OPT, WeSuite, QuoteWerks, Vivid, etc].