Network Provisions for SedonaOffice & Primary Integrations

Last Modified on 04/03/2025 7:08 pm EDT

SedonaOffice Client

https://sedonaoffice.perennialsoftware.com/resources/reference-documents/system-requirements/

SedonaOffice uses a ‘Client /Server’ architecture (also called Fat, Thick or Heavy Client). Due to the network requirements of the SedonaOffice client (~20Mb per client, TCP/IP ports 1433/4992, Named Pipes, latency <100ms to the SQL Server), direct operation of the application is NOT supported over ANY type of VPN. This includes web-based services like Amazon AWS and Microsoft Azure. The workstation(s) must be on the same local network as the SQL Server.

Note: SedonaService is required to initiate sessions between the Software and SQL. After the initial client session is started on 4992, the client server connection takes an available port base of 6000 and port range of 250 ports [6001-6250] as listed in in the registry HKLM\SOFTWARE\WOW6432Node\Sedona Development Company\Sedona Office Server

Note: If you are using SQL Aliasing/Instancing [c:\windows\SysWOW64\cliconfg.exe] or Microsoft SQL is set to manage connectivity, those settings are going to override the default 1433 SQL server port connection for the client machines reaching out to the SQL server. In most aliased/instanced/newer configurations, Microsoft/SQL will dynamically assign a port which can be 49000-65535. For those arrangements in virtual environments, our recommendation is to configure the firewall rule to allow the activity from your terminal server(s) private IPs, webserver IPs, and any in-scope network ranges of machines to the SQL Server Service instead of ports to account for the variance.

SedonaOffice > Alarmbiller [eforms, Time & Attendance, Sales Automation, etc]

URL/Site requires a valid and current SSL certificate bound to the site in IIS. You may use a wildcard.

[We recommend having the intermediaries for the SSL cert installed as well]

There needs to be public access to your SedonaWeb API URL that is hosted on your IIS server via port 443 for integrations to test and connect

SedonaSync

SedonaSync is preferably installed on an IIS server separate from the Sedona SQL server. If it is installed on the same IIS server where SedonaWeb is also housed, it will communicate back to the SQL server over the following

All versions: TCP 1433 back to SQL Server - v10 uses SSRS port 80 or 8085 via http back to SQL Server for report creation/auditing

- If the server Sync is installed on is migrated or server name changes this will require a relicense. Plan accordingly

[visible in configuration manager]

Enterprise Legacy SedonaWeb /SedonaWeb 2.0/Sedona X

It is not recommended to run your IIS server on the same server as your Sedona SQL server due to the need to communicate with the public internet. SedonaWeb should be on its own dedicated standalone server. SedonaWeb, SedonaSync, and BoldNet can be installed on the same server as long as it has greater than IIS 7 installed.

Note: SedonaWeb will not run properly under a subfolder of an existing site; please plan on dedicating a site, IP address and host header bindings strictly for SedonaWeb.

OS/System

- Microsoft Server 2019 Edition or better
- 5GB available hard drive space in addition to OS needs
- 2.5 GHz multicore/CPU
- 6GB Ram or greater for additional for multi-product/purpose IIS
- Microsoft .Net Framework 4.8 [3.5,4.5, WCF Services]
- ASP.NET 2.1.3 Core Hosting Bundle https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-2.1.30-windows-hosting-bundle-installer
- Redis https://github.com/MicrosoftArchive/redis/releases/download/win-3.2.100/Redis-x64-3.2.100.msi
- Internet Information Server (IIS) for corresponding Server/OS edition https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis

Networking & Configuration

- Your SedonaWeb/X/API url/site requires a valid & current SSL certificate bound to the site in IIS that matches your DNS entry.

[We recommend having the intermediaries for the SSL cert installed as well especially if using a wildcard certificate]

- Static public IP tied to DNS entry with corresponding Host File entry for SW2.0/API site

You MUST have your public IP address routed to the IIS Server and DNS Entries in place prior to installation

- TCP Port 443 HTTPS out to public [nonstandard HTTPS ports may require additional configuration needs]

[Public traffic via HTTPS is required to have customers/field techs reach the portal or use API calls externally]

VPN configuration is not supported

- TCP Port 1433 between Web Server and the primary SQL Server for database access
- TCP Ports 8080 & 10943/10944 For Octopus Tentacle API pushes and communication with our Deployment server 12.174.58.69
- SMTP Traffic 25/465/587 based on your current SMTP email server settings and or relay provider needs

Note: You may have other 3rd party integrations with web services such as WeSuite or OPT. You will want to confirm with their respective support teams on any specialized web configurations when making firewall/network changes or planning a migration.

WeSuite - wesupport@wesuite.com

OPT - support@optbusinessservices.com

*If SedonaSync is on the web server and it is migrated or server name changes this will require a relicense of Sync, plan accordingly

Enterprise Legacy FSU/Hosted Legacy SedonaWeb

OpenVPN should be running on your Enterprise SQL server. The following traffic needs to be allowed through your Firewall/Network Security:

- Traffic via OpenVPN firewall rule 10.242.242.0/24 UDP Port 9194 or 10.42.42.0/24 UDP Port 9194 [specified in client config]

1. This address would have a subnet mask of 255.255.255.0 and does not require a gateway address or DNS assignment

Inbound traffic allowed from our backend server Ips – Should allow all traffic including TCP 1433

- 12.174.58.69 = FSU Web /OpenVPN Server
- 12.174.58.64/29 or 12.174.58.64/255.255.255.248 = Originating IPs for our backend SQL server Legacy FSU & SedonaWeb

1. This address would have a subnet mask of 255.255.255.248 and does not require a gateway address or DNS assignment

*Note if OpenVPN is not installed on your server you must review for a custom setup

- If Sync is installed with SedonaWeb and is migrated or server name changes this will require a relicense. Plan Accordingly

Troubleshooting Legacy FSU

Cannot Login

This typically means that the connection between your SQL server and our FSU backend is interrupted. This can be caused by:

- OpenVPN Tap adapter is disabled or blocked on the SQL server
- Traffic via UDP Port 1194 or Port 9194, 10.242.242.0/24 or 10.42.42.0/24 [specified in OVPN Client config]
- OpenVPN service needs to be restarted

1. If restarting the OpenVPN service does not restore FSU, stop the service and completely exit the GUI
2. Confirm OpenVPN Tap adapter is not disabled or blocked
3. Run the open VPN GUI as an administrator and connect
4. If issues persist submit a case via contacting sedonaoffice_support@boldgroup.com or 719-593-2829

Can Login but Schedules will not Load

- 12.174.58.66/12.174.58.69 is being blocked

1. Ensure your Hardware/Software firewall is not blocking traffic from these IPs as there are our backend SQL server attempting to communicate with your SQL server
2. If issues persist submit a case via contacting sedonaoffice_support@boldgroup.com or 719-593-2829

If you are still unable to get schedules to Load you may also require Firewall rules to allow traffic to SQL on ports 1433 to the corresponding service IPs

- 12.174.58.69 = FSU Web OVPN Servers - 12.174.58.64/29 or 12.174.58.64/255.255.255.248 Originating IP range for our backed SQL server