



# **RFMS Core System Recommendations**

**Rev. 13/08/2024**

---

# General Information

There are several places in this document where we invite you to contact us. If you wish to open a support ticket with our IT department, you can do so in any of the following ways:

- Email [help@rfmsanz.com](mailto:help@rfmsanz.com)
- Call 1800 229 427 within Australia
- Call 0800 643 012 within New Zealand
- Fill out the contact form here: <https://rfmsanz.com/contact-us>

This document is intended as a guideline for clients with 15 users or fewer, and an RFMS database size of less than 2 GB. Regardless of your number of users and database size, we welcome you to reach out to us directly and discuss your specific requirements so that we can provide more tailored recommendations.

RFMS strongly recommends consulting with your local IT provider and SQL administrator for all SQL and server related purchases or changes because individualised adjustments based on your environment may be necessary.

Recommendations in this document are directed toward a server running Microsoft SQL Express for RFMS. The edition of SQL that you will need in order to run RFMS (Express, Standard, or Web) depends on your database size, number of concurrent connections, SQL management/reporting requirements, and other aspects specific to each client. Your IT provider is welcome to contact us to discuss any SQL recommendations or requirements.

This document does not take into account any other functions that your server may be required to provide, such as hosting other SQL instances, programs, or server roles. Please follow these recommendations at your own risk and with the guidance and advice of your local IT provider, who should be familiar with your environment, network, and business requirements. These recommendations are designed to provide you with the best RFMS performance possible; however, they do not guarantee optimum results as RFMS performance can be heavily affected by multiple environmental variables.

RFMS Core is comprised of two parts:

- RFMS Program Files
- Microsoft SQL Database

The RFMS program and database both run wholly off the server(s). Therefore, the server needs to have the hardware capabilities to support the inbound and outbound network connections and the memory capacity to support SQL database operations (and RD sessions if applicable). There is no client-side software for RFMS Core installed on the workstations. Instead, when accessed on a local network, the workstations use a shortcut pointing to the program on the networked server (via a mapped drive or UNC path). When accessed via Remote Desktop Services, the users typically execute the program from a local drive (on the RDS).

NOTE: RFMS has very specific requirements for the SQL configuration. In most cases, if you require SQL for another application or if SQL is already installed on your server, we recommend that you install a separate SQL instance for RFMS. We have documentation which details the specific SQL configuration required and we recommend that your IT provider contact us directly to review the SQL installation and configuration process.

- If you must use an existing SQL installation, you must ensure that it is set to Mixed Mode authentication (Windows Authentication and SQL Authentication) and that you know the password to the SQL SA account. Additionally, the SQL collation must be set to SQL\_Latin1\_General\_CP1\_CI\_AS. If SQL is used for another function or program, please confirm that it will not be detrimental to change the authentication mode and collation if they are not already configured this way.

- If a named instance is already installed, the RFMS database must be attached to a named instance. The RFMS database cannot be used on the default (MSSQLSERVER) instance if there is a named instance installed on the same server.

---

## Best Practices

### RFMS Core Software Updates:

Please DO NOT update your RFMS Core software without consulting with us first. RFMS is used in many countries around the world. Certain publicly available updates may not be suitable for the AU/NZ region. RFMS Australasia will always test updates internally to verify the update's compatibility with metric units of measure, GST accounting, financial reporting, and other AU/NZ-specific considerations. Please contact us directly so that we can advise you on the most suitable RFMS version for your circumstances.

### IT Provider:

Your IT provider should have a SQL-qualified technician on staff. Ideally, they would possess SQL certification or accreditation and have a qualified SQL DBA available.

### SQL Backups:

To minimise the amount of data loss in a disaster, we recommend configuring your RFMS database to use the Full Recovery Model. When the recovery model is set to Full, all database transactions are written to the transaction log file.

A SQL Maintenance Plan (if using SQL Server Standard or Web) or an external software utility should then be utilised to make at least nightly full backups and hourly log backups. These backups should be automatically uploaded to an off-site or cloud-based location. If you are simply storing your backups locally, they provide no value in the event of a disaster.

The benefit of the Full recovery model, combined with hourly log backups, is that your maximum amount of data loss should be limited to 1 hour's worth of changes.

For example, let's assume that your company performs a full database backup every night at 9:00 PM, and hourly log backups between 6:00 AM and 6:00 PM. You experience a hard drive failure at 11:25 AM. Your IT provider installs a new drive and restores your last full backup (from 9:00 PM the previous night) and then restores the incremental log backups from 6:00 AM to 11:00 AM. In this scenario, the only data that you would have lost is the changes between the last log backup (11:00 AM) and the time of the failure (11:25 AM), or 25 minutes.

It is essential that your SQL backups are executed via SQL and not by copying the database files themselves. If you use a SQL Maintenance Plan or a third-party program that is specifically designed to make SQL backups, the backup will be created properly. Simply backing up the .mdf and .ldf database files will often result in files that cannot be restored in an emergency. A proper SQL backup creates a .bak file for full backups and a .trn file for log backups. Additionally, if you aren't creating proper SQL backups but your database is set to the Full recovery model, your transaction log will grow continuously until the server drive is full. When a proper full or transaction log backup is executed, the transaction log file is truncated.

### SQL Backup Integrity:

Database backups that aren't usable do not offer any protection. Therefore, it is important to regularly test the integrity of your backups. Your IT provider should periodically perform restoration tests of your database backups to ensure their integrity. They should also perform a DBCC CHECKDB on the restoration test. It may also be beneficial to compare the table record counts between a recent backup and your live database. The record counts will not match exactly between the backup and live database since the backup is static, but the record counts should be reasonably close.

### RFMS Directory Backups:

Do not store your production RFMS directory in a cloud-sync folder (like Dropbox or OneDrive). Do not configure backup software to synchronise RFMS folder changes continuously. Either of these options will cause significant performance issues as there will be constant reads, writes,

and network traffic involved in this backup/sync process. Instead, we recommend backing up your RFMS directory nightly, outside of operating hours. All of your RFMS trading data is stored in the SQL database. The only things stored in the RFMS directory are the program files, attachments, logos, user dictionaries, etc, as well as any documents that you choose to save within the directory. These files are relatively static and do not require the same backup frequency as the SQL database.

#### **SQL DBA Review:**

We recommend a biannual review of your RFMS database by a qualified SQL DBA. They should follow Microsoft's best practices in checking the integrity and performance of your database and SQL configuration. Here are some examples of tasks that a DBA would typically perform:

- Configure SQL Maintenance Plans
- Check the database and tables for integrity and abnormalities
- Check for data fragmentation or any indexes that need to be rebuilt
- Verify the integrity of the database backups
- Ensure that the edition of SQL is still appropriate for your database size and other circumstances
- Check the compatibility level of the database
- Review the SQL logs for errors or other concerns
- Ensure that all relevant updates and service packs for your version of SQL have been applied
- Ensure that your SQL version is still supported by Microsoft and RFMS, and upgrade if necessary
- Verify the SQL network configuration (within SSCM) is still optimised for your environment

#### **Network Review:**

We recommend an annual review of your local network by a network analyst. Your local network is a critical part of your IT infrastructure. Since RFMS is a database application with constant client-server-client communication, it is especially sensitive to network disconnects, poor performance, and dropped packets. A network review should analyse the speed, consistency, and quality across your network. The analyst should also evaluate the hardware and cabling, and the security of your network. If you use a local SQL server, then the analyst should also evaluate the ODBC and Cliconfg aliases/connections between each client and the SQL server.

---

## **General Requirements**

- **High-Speed Internet Connection**
- **Wired Ethernet Connections** are strongly recommended. Gigabit Network Cards, Gigabit Switches, and Cat 5 cabling are recommended at a minimum. It is not recommend to connect workstations through a physical IP phone (since their built-in network switch is typically only rated for 100Mbps), and it is not recommend to run RFMS over a wireless connection (unless using a remote desktop connection) due to potential performance issues.
- **Printer (Network or Local)** For more information about printers, please see the relevant section below.
- **Provision for Database and File Backups** (Consult with your local IT provider regarding the best method for your business.) RFMS requires that SQL database backups be performed using a SQL backup routine. Simply backing up the .mdf and .ldf database files is not sufficient and will result in warnings by the RFMS applications until properly registered SQL backups are performed at least daily. We can make specific recommendations to your local IT provider regarding database backups (such as the use of incremental log backups to reduce data loss in a disaster). Backups of your RFMS directory and your SQL database

should be stored both locally and off-site to protect them from a physical or environmental event (flood, fire, etc). There are numerous ways to accomplish off-site backup storage, with many companies opting to have backups automatically uploaded to a cloud storage provider like OneDrive, Dropbox, etc.

- **An Uninterruptible Power Supply (UPS)** (battery backup) is required on the server to allow for the proper shutdown of the SQL server in the event of a power failure. A hard shutdown of the SQL service during database operations could result in data loss or corruption.
- **Monitor(s) with a minimum resolution of 1920x1080.** Running RFMS at lower resolutions may create screen bleed issues, and the user may not be able to view all fields or buttons.

---

## Hardware / Software Recommendations

- ARM (AArch64) Processors Are NOT Supported. (This includes the new Snapdragon X series processors.) Windows 11 comes with native support for ARM processors. Windows 11 has built-in x86 emulation which allows many programs that are designed only for the x86 architecture to run on ARM. However, RFMS will likely not work properly on ARM, even with the built-in emulation, due to the complex differences in the instruction set architecture and the programming language in which RFMS Core is written.
- The size of the database determines the amount of memory required for Microsoft SQL. Typically, the SQL memory requirement will be a 1:1 database size to memory ratio for data caching, with further memory required to support database operations.

## Workgroup System (For 2-5 Users)

### Server\*:

\* In a workgroup system, the server could be a dedicated machine or it could be used as a workstation in addition to hosting SQL and the RFMS Program.

- **OS:** Windows 11 Pro x64
- **SQL:** SQL Server 2022 (Express)
- **CPU:** Intel Core i7 or Core Ultra 7 (Tiger Lake or newer)
- **Memory:** 16GB/32GB RAM (depending on requirements);
- **Storage:** Business-Grade SSD (recommended) or 7200RPM SATA HDD

### Workstations:

- **OS:** Windows 11 Pro x64
- **CPU:**
  - Recommended: Intel Core i5/i7 or Core Ultra 5/7 (Tiger Lake or newer)
  - Minimum: Intel Core i3 (Kaby Lake or newer) or AMD Ryzen 3 (Zen series or newer)
- **Memory:**
  - Recommended: 16GB RAM
  - Minimum: 8GB RAM
- **Storage:**
  - Recommended: Business-Grade SSD
  - Minimum: 7200RPM SATA HDD

## Dedicated Server System (For 5-15 Users)

### Server:

- **OS:** Windows Server 2022 Standard;
- **SQL:** SQL Server 2022 (Express / Web / Standard - depending on requirements)
- **CPU:** Intel Xeon (Ice Lake or newer)
- **Memory:** 16GB/32GB/64GB RAM (depending on requirements)
- **Storage:** Server(Enterprise)-Grade SSD (recommended) or 7200RPM SATA/SAS HDD

### Workstations:

- **OS:** Windows 11 Pro x64
- **CPU:**
  - Recommended: Intel Core i5/i7 or Core Ultra 5/7 (Tiger Lake or newer)
  - Minimum: Intel Core i3 (Kaby Lake or newer) or AMD Ryzen 3 (Zen series or newer)
- **Memory:**
  - Recommended: 16GB RAM
  - Minimum: 8GB RAM
- **Storage:**
  - Recommended: Business-Grade SSD
  - Minimum: 7200RPM SATA HDD

## Hosted Servers

RFMS can be run in a cloud (off-site) environment. A remote connection client like Microsoft Remote Desktop Services is required to connect to a cloud server.

*When using a cloud environment, we recommend separate VMs for the SQL server and the Remote Desktop Server(s).* If SQL is installed on the RDS, resource conflicts between the RD session host and SQL service can cause performance and stability problems.

We recommend one of the following methods of remote connection:

1. RemoteApp deployment with a custom RDP Port
2. Remote Desktop Services (Protected\*)

\* The default RDP port (3389) must always be changed for security and connections to the RDS should be protected by a minimum of Multi-Factor Authentication (MFA). Additional security options include NLA and IP Whitelisting.

**Microsoft Azure:** Microsoft Azure (Azure Virtual Desktop [AVD] & Azure Server IaaS) has various specific configuration options, tools, drivers, and software utilities. While RFMS does work in Azure-hosted environments, your IT provider should be extremely proficient in the configuration, maintenance, and diagnostics of Azure VMs. We have seen unusual issues that required adjustments to Azure-specific group policy settings or server configuration options. Please note that it is the responsibility of your IT provider to manage your Azure environment, and, as Microsoft Azure is outside the scope of our support agreement, RFMS Australasia will be limited in the amount of assistance we can provide with regard to Azure diagnostics and troubleshooting.

**VPNs (Virtual Private Networks):** Running RFMS over a direct, site-to-site/IPSEC VPN connection is not supported and will cause significant latency and/or disconnects within RFMS. If using a VPN, you must access RFMS via RDP after connecting to the VPN.

# Operating Systems and SQL Server Versions

We follow Microsoft's Mainstream Support Cycle as closely as possible.  
[Please see Microsoft's current Product and Services Lifecycle Information.](#)

Product	Microsoft Mainstream Support End Date	Purpose
Windows 10 Pro	14 October 2025	Workstation OS; Workgroup Server OS
Windows 11 Pro	N/A	Workstation OS; Workgroup Server OS
Windows Server 2016*	11 January 2022	Server OS
Windows Server 2019*	9 January 2024	Server OS
Windows Server 2022	October 13, 2026	Server OS
SQL Server 2016*†	13 July 2021	SQL
SQL Server 2017*	11 October 2022	SQL
SQL Server 2019*	7 January 2025	SQL
SQL Server 2022	11 January 2028	SQL

\* No longer supported. Listed for reference only.

† The mainstream support end date for SQL Server 2016 was 13 July 2021. Even though SP3 does indicate that it is supported by Microsoft past this date. However, Microsoft also states: "When support for a product ends, support of all the service packs for that product also ends. The product's lifecycle supersedes the service pack policy." Therefore, RFMS will view SQL Server 2016 as unsupported from 13 July 2021. Additionally, earlier versions of SQL Server 2016 had reports of compatibility issues with Remote Desktop Services. If your current environment uses SQL Server 2016, please ensure all Windows and SQL updates have been applied.

The required SQL edition (Express, Standard, Web) will depend on several factors, including, but not limited to, database size, number of concurrent connections, and whether your server is cloud-based. While SQL Express technically supports databases up to 10GB, we do not recommend its use for databases larger than 1.5 GB. SQL Express has a memory limitation of 1.4GB and a processor limit of the lesser of 4 cores or 1 socket. These hardware limitations will cause significant RFMS performance degradation if your database is larger than 1.5 GB.

- CONTINUED ON NEXT PAGE -

# SQL Server Compatibility Levels

We strongly recommend testing the SQL Compatibility Level within your environment and consulting with your SQL administrator.

SQL Server Version	Default Compatibility Level	Recommended Compatibility Level
SQL Server 2022	160	150
SQL Server 2019*	150	150
SQL Server 2017*	140	130
SQL Server 2016*	130	130
SQL Server 2014*	120	110
SQL Server 2012*	110	110

\* No longer supported. Listed for reference only.

---

## Printers

### Laser and Inkjet Printers

Recommended printer properties:

- PCL5 or PCL6
- Capable of 19CPI or higher
- Certain reports in RFMS require Legal (or A3 or Ledger) sized paper
- If using an installed printer driver on a Remote Desktop Server, make sure it is RDS compatible

### Remote Printing

Printers can be set up for remote printing in multiple ways, such as:

#### Redirected Printers:

When using Easy Print, it must be enabled on the RDS. This will associate a Universal Print Driver on the Remote Desktop session with your local printer. This may allow your IT technician to keep the RDS free of print drivers. However, there may be certain printer functions or formatting issues that require a print driver to be installed on the RDS as well.

#### Third-Party Add-On Programs:

There are various options for third-party add-ons, which generally have a server software component and a client software component. This will allow the client software component to communicate with the server through the RD session and associate local printers within the remote session. One program that is widely used in this way is TSPrint (not free).