



## On Premise - Hosting Recommendations & Responsibilities

### Introduction

Our team strongly recommends going with our SaaS offering in the majority of cases, as clients who use our cloud offering don't need to worry about the resources or the responsibilities associated with hosting the Claromentis web application. However, we fully support On Premise deployments as well. This article provides a guide on the hosting recommendations and responsibilities for On Premise deployments.

Server requirements are dependent on a number of factors, the most important of which are:

- Number of concurrent users (users logging in and actively using applications at exactly the same time)
- The expected size of documents that will be uploaded to the intranet

The Claromentis framework effectively contains 3 main components, which are:

- The Claromentis application and supporting services
- The Database (MySQL or MSSQL)
- The Data (the actual data files, e.g. documents uploaded)

### General Recommendations

- Commonly, small to average sized systems are hosted on a combined web/database server, while larger systems are load balanced using a load balancer, two or more web servers and a separate database server. This allows for horizontal scaling as the company grows as well as failover protection in the event of server failure. For additional redundancy we also support multiple database servers in master/slave or master/master configurations.
- In general terms, the web services benefit when CPU resources are increased. It is also better to have more CPU's (physical or core), than it is to have a single CPU with great speed. Servers hosting the data will of course require disk space to accommodate the total number and size of files to be stored.
- It is recommended that Claromentis be installed on a newly installed operating system, which does not host other websites or services, since installations and maintenance may affect or interrupt the services we install on your behalf. Our team only require the operating system installed and patched, our team will take care of the install of everything else listed below (apart from MSSQL, see the MSSQL note in the Compatibility Matrix).
- We recommend using virtual machines, as this will make it easier to schedule backups and refresh development/testing environments (by cloning the VM's).

### Compatibility Matrix

In short, the Claromentis software can operate using either MySQL or MSSQL. Claromentis also utilises some additional third party services, which we've listed below.

Please refer to the matrix below for specific compatibility requirements.

Component	Version	Notes
Windows	2016,	

Servers	2019, 2022	
MySQL Server	5.7	<ul style="list-style-type: none"> <li>We recommend MySQL for Windows servers.</li> <li>Any MySQL version &lt;5.7 do not support utf8_mb4 and are therefore not supported.</li> </ul>
Microsoft SQL Server (MSSQL)	2016, 2017, 2019, 2022	<ul style="list-style-type: none"> <li>MSSQL is only supported if referenced from a Windows Web Server</li> <li>If you would like to use MSSQL, you'll need to provide access to an existing MSSQL cluster or set up a standalone SQL server. We can then connect to this database using the SQL native drivers. If you'd like Claromentis to install the database on your behalf, this is only possible for 'MySQL' installations. We support SQL Standard or Enterprise variants but not SQL express, due to the performance limitations.</li> </ul> <p><b>Important configuration for MSSQL</b></p> <ul style="list-style-type: none"> <li><b>UTF-8</b> will need to be set as the default character set for any database created for the Claromentis Intranet.</li> </ul> <p>The above is important to avoid encoding issues with the Claromentis platform.</p>
IIS	8, 8.5, 10	
Microsoft Visual C++ Redistributable	2015	This is a requirement for PHP
.NET Framework	3.5 +	This will be required for the MSSQL server, if you're planning on setup a standalone MSSQL server for us to connect to
PHP	7.4	
Java JRE	8+	
LibreOffice	7.5+	
ImageMagick	7+	
wkhtmltopdf	wkhtmltox-0.12.5-1	
ElasticSearch		

#### Minimum Server Resources / Requirements

Number of Users	Number of CPU's	Memory (RAM/GB)	Network Speed
1-100	2	8	100Mbit
100-500	4	8	100Mbit
500+	We recommend setting up a load balanced environment for any system with more than 500 users		

#### Load Balanced Environment

Claromentis provides the option of hosting an intranet in a load balanced environment. This is particularly beneficial for clients who have a vast number of users, or for those who want enhanced performance or failover.

Please speak to either your account manager or project manager and ask for a recommended topology. We'll need the following information from you

to put together this topology:

- Total number of users that will have access to the system
- Expected number of concurrent users (users logging in and actively using applications at exactly the same time). If you're not sure about this, we can estimate this for you based on your total number of users
- The expected size of documents that will be uploaded to the intranet (in GB) during the first 12 months

Once we have this, we'll send over a recommended topology based on your specifications.

### **Server Disk Space**

It is the responsibility of the client to provision a suitable amount of disk space for the Claromentis framework. Typically, the Claromentis footprint alone should have an allowance of 30GB. Additional space should be allocated for the data held on the intranet and within the database server.

Here are some common starting points:

- 20GB free space for the database
- 100GB free space for the Claromentis framework and data

### **Hosting Responsibilities**

Clients who host their intranet within their own infrastructure are responsible for various aspects of the maintenance of their hosting environment.

### **Internal Infrastructure**

If you use your own infrastructure to host your Claromentis intranet, you are responsible for maintaining the infrastructure. The Claromentis team are responsible for troubleshooting within the Claromentis product and services but are unable to troubleshoot any external infrastructure.

It's important that you keep your infrastructure fully maintained and up-to-date, including the following areas:

- DNS (Fully qualified domain name / URL that is being used to access your Claromentis intranet)
- SSL certificates
- SMTP relays
- Proxies and reverse proxies
- SSO Identity Providers
- Active Directory server setup
- Physical/virtual server setup

Our customer support and technical teams will always investigate faults with any part of your Claromentis intranet. If we find that the fault is caused by any infrastructure, product or service outside of the Claromentis intranet system, we will raise it as work to be done by your team, product or service provider. At this point, we may still be able to assist you with the investigation. If the fault is confirmed to be outside of our responsibility, then we will need to charge for any investigative work at our current daily rate.

### **SSL Certificates**

Self-signed certificates can't be used if you connect & use third party API such as Push Notifications. In this instance, and externally signed SSL certificate from a recognised certificate authority will need to be used. If not third party API is being used, a self-signed SSL certificate may still be provisioned.

### **MSSQL Clusters**

It is a requirement that as the client you back up the Claromentis MSSQL instance when contained within a cluster. This would also be at the point of any maintenance or upgrade that Claromentis carry out. We will ask for an additional, manual MSSQL backup to be taken before we perform this work.

As this is a cluster, which will contain other external databases that are outside of the Claromentis database, our TechOps & Development team may also ask for troubleshooting queries to be performed by yourselves. We will be unable to perform these as the Claromentis database is housed on a shared cluster that we are unable to manage.

### **Backup Procedure**

Clients are responsible for the setup and maintenance of a backup schedule for disaster recovery.

It is essential that the following components are backed up, to avoid data loss in the event of a disaster.

- The database
- The 'application' folder - this contains the Claromentis framework and supporting binaries as well as any custom work
- The 'data' and 'local data' folders

The backup procedure will depend on the server configuration.

- We recommend using Virtual Machines wherever possible and creating a snapshot schedule for each Virtual Machine. This backup should run at least daily and retain data for at least the past 30 days (or according to your own backup schedules)
- In addition to this, we'd recommend the scheduling of backups for the MySQL or MSSQL database into a single file (.sql for MySQL or .bak for MSSQL) and copying this, along with the 'application', 'data' and 'local data' folders to an offsite location, as a secondary backup to use in the event of the Virtual Machine snapshots failing.

## **Staging / UAT Environment**

We strongly recommend that all on-premise systems have a separate staging/UAT server. This can then be used to perform all upgrades and customisations which can then go through change control/UAT (User Acceptance Testing) prior to our team scheduling in any work on the live environment.

By hosting a staging environment in addition to a live environment, clients can benefit from the following:

- Upgrades and customisations can be implemented onto the staging server for client approval and feedback before they are added to the live system.
- Downtime and disruption of the live system is kept to a minimum, with all work carried out on the staging system first, and only moved to the live system once permitted by the client.
- Training can be performed on the UAT environment

Please note that a separate license will need to be purchased for the staging/UAT environment. Contact your account manager or project manager for further information.

## **Firewall Responsibilities**

Maintenance and configuration of on-premise firewalls is the sole responsibility of the client.

## **Anti-virus**

We recommend implementing a lightweight anti-virus solution on all servers.

## **Monitoring**

We recommend setting up a monitoring solution to check for any anomalies that could signify a potential active threat and to ensure that key resources are within acceptable limits. This includes monitoring of disk space, as the site will require the disk space to be increased, as more content is uploaded to your site.

## **Security Vulnerabilities**

It is the responsibility of the client to apply any patches or updates that fix the operating system or software security vulnerabilities (for any software that isn't installed by Claromentis). If any of the Claromentis framework or supporting services are identified as vulnerable, it is up to the client to notify the Claromentis team by submitting a support ticket and we will take appropriate action.

## **Disaster Recovery**

It is the responsibility of the client to restore their hosting environment in the event that it becomes unavailable. In the event that a disaster occurs, please submit a support ticket and let us know if you need any advice on the best practice for restoring access to the Claromentis instance.