

What Operating system can Optergy be installed on?

Optergy Proton and Enterprise servers are equipped with meter and device data acquisition software, no additional computers or operating systems are required. Optergy Enterprise (OE) software may be purchased separately and installed on a customer owned server or virtual machine / raw hardware. No operating system is required.

We only support Windows based systems on our enterprise network. Can Optergy be installed on Windows?

Yes, Optergy can be installed on a Windows operating system. The Windows OS will require VMWare so the Optergy embedded real-time operating system can be manually installed in a virtual environment.

What are the hardware and resource requirements for Optergy?

The system is completely scalable from very small, single building systems to large enterprise systems. The storage, hardware platform and resources required depend entirely upon the scale and scope of the application/installation.

[Please refer to our hardware recommendation document.](#)

Can we install Optergy ourselves?

If Optergy is installed on clients existing hardware then the installation should ideally be carried out by in house IT staff to ensure that all IT policies are complied with. If it installed on a separate hardware platform it can be installed by in-house staff or by your nearest Optergy support office. Either way, installation is fast and easy.

Will Optergy access data on the network?

Optergy will only access the data it has been configured to access. Optergy has its own database where all of the information it gathers from devices is securely stored. The system will only collect information from items such as:

- Utility meters including electricity/gas/water/thermal
- Building Management field controllers
- Weather information from a local weather station or online weather stations
- Pulse counting modules for people counters, traffic counters or energy pulse meter loggers
- Modbus devices connected to the system such as meters and PLCs
- BACnet devices connected to the system typically used to control HVAC systems

Will providing internet access to Optergy open us to hacking?

There are several ways to make Optergy available online. The recommended method of remote access is via a Virtual Private Network (VPN). Should a VPN not be possible or feasible, Optergy can be firewalled to run on its own private network with an independent internet connection, to limit potential risk. To further reduce the chance of being hacked, access can be set up on non-standard ports to prevent opportunistic scanning from bots.

How do I backup data from Optergy?

Optergy has a few methods of backup to ensure all of the data it collects is stored safely. By default, automatic backups are carried out on a weekly basis and are stored locally. Optergy can be configured to automatically send backups to remote servers using either FTP or SFTP. There is also the option to create manual backups and this can be performed locally or remotely.

What redundancy options are available?

The hardware specified for Optergy caters for redundancy and data loss prevention; it is recommended that systems run either software or hardware based RAID. Optergy also monitors power status from the UPS it is connected to. In the event of power loss, the system will safely shut down and when power is reinstated, it will turn on automatically and resume normal operation.

There are additional measures that can be utilised for further redundancy that include:

- Running multiple iterations of Optergy in Parallel all collecting data from the same building subsystems.
- Operating System level redundancy with two servers replaced at OS level.

What are some typical ways Optergy is deployed?

The system may be deployed however you wish or as required to comply with IT policies. However, a few very typical examples are as follows:

Typical Installation 1:	Where it is used as a single building system it is commonly installed on separate hardware with a very small dedicated IP network connecting various building technologies together. Many of these building systems may also use proprietary and non IP based network types. If there is remote access via the internet the system typically has its own, dedicated internet access used only by Facility Managers and building operations staff using only HTML.
Typical Installation 2:	Where it is used in very large facilities, multi-building operations or across campuses and enterprises on the enterprises own network, it is commonly installed on a secure subnet along with other building technologies subsystems with which it communicates. In these situations, it is equally common to install it on the client's hardware (by the customer IT staff) in a VM environment or on dedicated hardware. Most commonly in this situation, off-site access is by VPN although not all IT departments require this.
Typical Installation 3:	Where the enterprise has a large number of small or medium sized buildings and desires a central cloud-based solution (public or private cloud) Optergy can be hosted in a data centre, in-house or by a service provider and the system interconnected by a variety of 3G, Broadband and DSL or ADSL connections.

For more information, go to <https://portal.optergy.com/it-iot-documents>