The Cerberus DMS management platform provides an integrated approach to managing and controlling facilities from a flexible, easy-to-use interface that allows users to:

- Operate and monitor the danger management system graphically
- Detect, visualize, and acknowledge/reset faults and alarms
- Guide operators in the handling of critical situations
- Operate and execute typical security tasks such as video surveillance, intrusion detection, and access control monitoring
- Create schedules to automate danger management operation and configure exceptions
- Create and configure report definitions to produce a variety of performance reports
- Store and retrieve system activity data, and view data logs
- Create and execute automated reactions between the networked systems
- Send automatic remote notifications via email, SMS, and pagers
- Participate in the Internet of Things through open APIs and custom adapters

Cerberus DMS offers full integration of fire safety, access control, and video systems, while also supporting open standards such as BACnet, OPC, Modbus, and more. Cerberus DMS also provides customizable and market-specific distributions. Options are available for dedicated, browser-based, and Windows desktop app clients using the same user interface. Additionally, web interfaces provide increased flexibility for operation and future extensions such as mobile applications for tablets and smartphones.
Cerberus DMS is a client-server system designed to augment existing building infrastructure and integrate with standard IT hardware, software, and networks. The open, adaptable architecture supports the most common Windows-based IT infrastructures. In addition, Cerberus DMS allows full server functionality in virtual IT environments and advanced networks. A Cerberus DMS installation can be configured as a single server or as multiple servers in a distributed configuration.

**System Capabilities**

- Fully scalable and secure distributed client/server architecture with multi-language support
- Web and remote access from mobile clients
- Open-data libraries designed for extensions and integrations
- Support for BACnet, OPC, Modbus, HTTP(S), SNMP, and HTML5 standards
- Powerful features such as advanced event management, Mobile App, remote notifications, scheduler/reaction processor, long-term storage, user management
- Support for 150,000 objects in a single system or up to 1,500,000 objects in distributed systems
- Consistent user interface concept across all applications, with graphic-oriented operation workflows
- Online engineering, CAD import, and automatic positioning of graphic symbols
- Support for Siemens and third-party fire-safety and security devices
- Northbound connectivity through OPC DA server and REST Web Services interfaces
- Southbound open interfaces and SDK to develop subsystem extensions
- Consolidated Ecosystem program and network to share and expand subsystem extensions, applications, utilities, and tools

**Certifications and Approvals**

Cerberus DMS has been tested against a wide range of domain- and country-specific norms and standards, including:

- BACnet Revision 1.15, certified by BACnet Testing Laboratory as BACnet Advanced Workstation Software (BTL B-AWS)
- IT security compliant with the ISA-99/IEC 62443 Security Level: SL1
- OPC DA V2.05a and V3.0 Server, certified by the OPC Foundation certification program
- UL listed to UL-864 10th edition Standard for Control Units and Accessories for command and control when installed on a UL-864 approved computer
- ULC listed to ULC-S527-11 3rd edition for command and control when installed on a ULC-S527 approved computer
- UL listed to UL-2572 for Mass Notification (for monitoring only when installed on a UL-2572 approved computer)
- ULC listed to ULC-S576 for Mass Notification (for monitoring only when installed on a UL-2572 approved computer)
- UL listed to UL-294 7th edition Standard for Safety–Access Control System Units
Technical Data

All systems should be dimensioned according to project size, and you should maintain OS compatibility until Microsoft retires the product.

Operating System Compatibility
The Server and Installed Clients run on the following Microsoft operating systems and editions:
- Microsoft® Windows 7 64-bit (Professional and Enterprise)
- Microsoft® Windows 10 64-bit (Professional and Enterprise)
- Microsoft® Windows Server 2012 R2 64-bit
- Microsoft® Windows Server 2016 64-bit
- Microsoft® Windows Server 2019 64-bit

Web Clients and Windows App Clients run on following Microsoft operating systems and editions:
- Microsoft® Windows 7 64-bit (Professional and Enterprise)
- Microsoft® Windows 10 64-bit (Professional and Enterprise)

Hardware Requirements (minimum recommendation)

Physical Machines
- Hard disk: 1 x 256GB SSD (client); 1 x 1024GB SSD (server)
- RAM: 8GB (client); 16GB (small or medium-sized server); 32GB (large server)
- Processor: Core i5 or equivalent ≥3.0 GHz, 2 cores (client); Core i7 or equivalent ≥3.2 GHz, 4 cores per running system (server)
- UL/ULC-listed hardware: required for UL/ULC applications

Virtual Machines
- Hard disk: 1 x 256GB SSD (client); 1 x 1024GB SSD (server)
- RAM: 8GB (client); 16GB (small or medium-sized server); 32GB (large server)
- Processor: 2 vCPUs assigned to the VM ≥3.0 GHz (client); 4 vCPUs assigned to the VM ≥3.2 GHz (server)

Microsoft SQL Server Compatibility
Microsoft SQL Server 2014 R2 Express is free and included with the DVD image. Additional supported SQL version and editions are:
- Microsoft® SQL Server 2012 (Express, Standard and Enterprise)
- Microsoft® SQL Server 2014 (Express, Standard and Enterprise)
- Microsoft® SQL Server 2016 (Express, Standard and Enterprise)
- Microsoft® SQL Server 2017 (Express, Standard and Enterprise)

Ordering Information
For ordering information related to Cerberus DMS, please visit our online tool HIT.

Resources
For the latest information about Building Products and Siemens Smart Infrastructure, visit our Building Products site.
For other datasheets, see the following:
- Desigo CC
- Desigo CC Compact DMS
- Desigo CC Compact BA
- Desigo CC Compact Validated Monitoring
- Desigo CC Compact for Electrical applications
- Desigo CC Connect
For more information, refer to your local sales organization.
Cyber Security Disclaimer

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends compliance with security advisories on the latest security threats, patches, and other related measures—published, among others, under