

Cerberus® DMS

P55802-Y114-A100



Cerberus DMS is the integrated, scalable, and open danger management platform for managing high-performance buildings. With its intuitive, easy-to-use user interface Cerberus DMS supports the following danger management tasks:

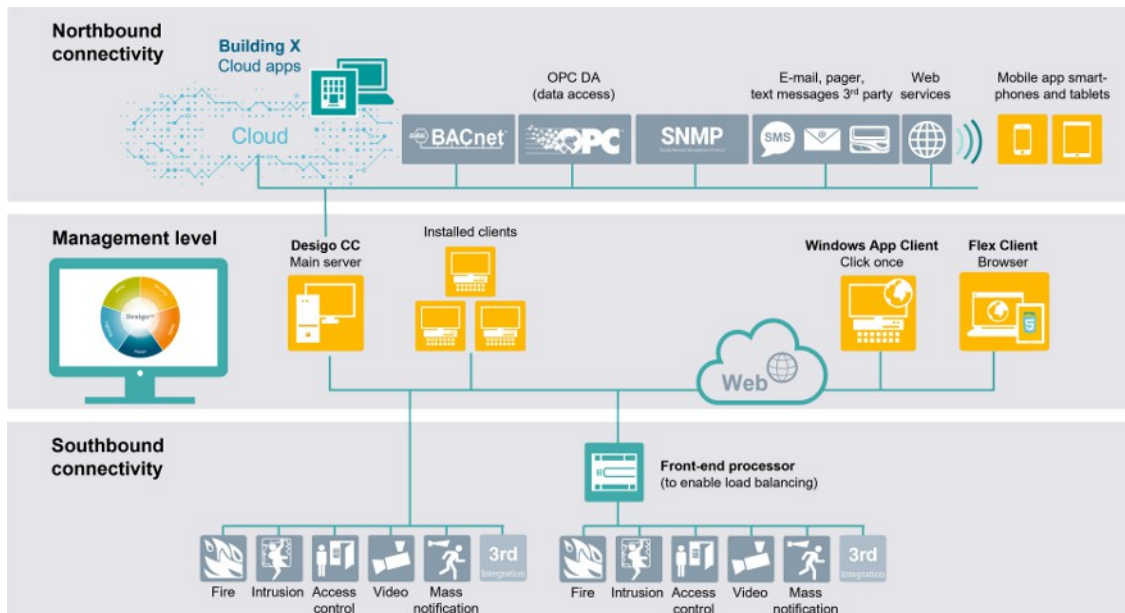
- Operate and monitor the danger management system graphically
- Guide operators in the handling of critical situations
- Detect, visualize, and acknowledge/reset faults and alarms
- Operate and execute typical security tasks such as video surveillance, intrusion detection, and access control monitoring
- 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 notifications via email, SMS, and pagers
- Participate in the Internet of Things through open APIs and custom adapters

General Description

Cerberus DMS offers full integration of fire safety, intrusion detection, 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. The installed client and the Windows Desktop App Client provide the same user interface. The browser-based Flex Client is based on HTML5 technology and combines proven operating concepts with a new user experience. Additionally, web interfaces provide increased flexibility for operation and future extensions such as mobile applications for tablets and smartphones.

System Architecture

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 client
- Connectivity to Building X open platform. This means that selected Cerberus DMS data can be shared with cloud-based Building X applications like Operations Manager or 360° Viewer.
- Open-data libraries designed for extensions and integrations
- Southbound connectivity through BACnet, BACnet/SC, OPC DA and UA, Modbus, HTTP(S), SNMP, HTML5, and SDK to develop subsystem extensions
- Powerful features such as advanced event management, Mobile App, notifications, status and command propagation, 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 with wizards, CAD import, and automatic positioning of graphic symbols
- Support for Siemens and third-party fire-safety and security devices
- Northbound connectivity through BACnet Server, OPC DA Server, and RESTful Web Services interfaces (for example, Power BI Connector)

- Support of authentication via most common OIDC providers (Google, Microsoft, Amazon...)
- 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:

- IT security compliant with the ISA-99/IEC 62443 Security Level 2 (SL2)
- BACnet Protocol Revision 1.20, certified by BACnet Testing Laboratory as BACnet Cross-Domain Advanced Workstation Software (B-XAWS, B-AWS, B-ALWS, B-AACWS, B-RTR, B-BBMD)
- AMEV recommendation BACnet 2017 compliant with Management Operation Unit (MOU-B) profile
- OPC DA V2.05a and V3.0 Server, certified by the OPC Foundation certification program

UL/ULC listed to:

- UL-864 10th edition Standard for Control Units and Accessories for command and control when installed on a UL-864 approved computer
- UL 2017 2nd Edition, General-Purpose Signaling Devices and Systems
- UL-2572 2nd Edition Standard for Mass Notification
- UL 2610 2nd Edition Standard for commercial premises security alarm units and systems (this standard replaced UL 1076)
- UL-294 7th Edition Standard for Safety–Access Control System Units
- CAN/ULC-S527 3rd Edition: Control Units for Fire Alarm Systems
- CAN/ULC-S559 2nd Edition, Equipment for Fire Signal Receiving Centre and Systems
- CAN/ULC S576 1st Edition, Standard for Mass Notification System Equipment and Accessories

Designo CC V6 is not UL/ULC listed. If UL or ULC approval is required, please use V7 or V8. UL/ULC listing for V9 is still pending.

Technical Data

Operating System Compatibility

The Server and Installed Clients run on the following Microsoft operating systems and editions:

- Microsoft® Windows 10 64-bit (Enterprise and IoT Enterprise LTSC editions)
- Microsoft® Windows 11 (Pro Enterprise and IoT Enterprise)
- Microsoft® Windows Server 2019
- Microsoft® Windows Server 2022
- Microsoft® Windows Server 2025

Flex Clients and Windows App Clients run on the following Microsoft operating systems and editions:

- Microsoft® Windows 10 64-bit (Enterprise and IoT Enterprise LTSC editions)
- Microsoft® Windows 11 (Pro and Enterprise)

Server Hardware Requirements (minimum recommendation)

Physical Machines

- Hard disk: 1 x SSD 256 GB (client); 1 x SSD 512 GB to 2 TB (server)
- RAM: 8 GB (client); 16 GB (small or medium-sized server); 32 GB (large-sized server); 64 GB (distributed system)
- Processor:
Server-grade CPU like Intel Xeon or AMD EPYC (or equivalent),
CPU Mark $\geq 13,000$, Single Thread Rating $\geq 2,300$,
 ≥ 2 cores (client), ≥ 4 cores (server)

Embedded Hardware (limited to 10,000 system objects)

- Hard disk: 256 GB SSD
- RAM: 16 GB
- Processor: Celeron 6600HLE @ 2.10 GHz cores (or equivalent)

Virtual Machines

- Hard disk: 1 x SSD 256 GB (client); 1 x SSD 512 GB to 2 TB (server)
- RAM: 8 GB (client); 16 GB (small or medium-sized server); 32 GB (large-sized server); 64 GB (distributed system)
- Processor:
>= 4 vCPUs assigned to the VM

Microsoft SQL Server Compatibility

Microsoft SQL Server 2022 Express is free and included with the installation media. Additional supported SQL version and editions are:

- Microsoft® SQL Server 2019 (Express, Standard, and Enterprise)
- Microsoft® SQL Server 2022 (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™ Compact DMS

For more information, refer to your local sales organization.

Cybersecurity 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 <https://www.siemens.com/cert/> => 'Siemens Security Advisories'.