Desigo™ CC V4.1
Cybersecurity Guidelines
Basic Documentation
# Table of Contents

About This Document .................................................................................................................. 5
Applicable Documents .................................................................................................................. 6
Technical Terms and Abbreviations ............................................................................................. 6
Acknowledgements ....................................................................................................................... 12
Document Revision History .......................................................................................................... 13

1 Cybersecurity Basics ................................................................................................................ 14
   1.1 Introduction .......................................................................................................................... 14
   1.2 Threat and Risk Terminology .............................................................................................. 14
   1.3 System Security ................................................................................................................... 15
   1.4 SSL Certificates .................................................................................................................. 16

2 Network Security Controls ..................................................................................................... 26
   2.1 Protected System Configuration Concept .......................................................................... 26
       2.1.1 Zone Boundary Protection ......................................................................................... 27
       2.1.2 System Components ................................................................................................. 29
       2.1.3 Firewall Rules ........................................................................................................... 30
       2.1.4 Least Functionality Implementation ......................................................................... 39
   2.2 Intended Operational Environments .................................................................................. 40
       2.2.1 All-In-One (One-Seat) System .................................................................................. 40
       2.2.2 Client/Server in the Customer Network ..................................................................... 44
       2.2.3 Server and Remote Web Server (IIS) ....................................................................... 48
       2.2.4 Client/Server with Internet Access .......................................................................... 51
       2.2.5 Large, Distributed Client/Server with Internet Access ........................................... 56
       2.2.6 Distributed System Configurations .......................................................................... 58
       2.2.7 Virtualization ............................................................................................................. 59

3 Cybersecurity Concepts – How to Secure the System ............................................................. 61
   3.1 User Management ............................................................................................................... 62
   3.2 IT Security .......................................................................................................................... 63
   3.3 Communication Security .................................................................................................... 63
   3.4 License Security .................................................................................................................. 64
   3.5 Stored Data Security .......................................................................................................... 64
   3.6 Main Server Folder Shares for Client and FEP Installations .......................................... 64
   3.7 Server Services .................................................................................................................... 66
   3.8 LMS – License Management System ............................................................................... 69
   3.9 Physical and Environmental Security ............................................................................... 69
   3.10 Incident Handling ............................................................................................................. 70
   3.11 Windows Hardening .......................................................................................................... 70
   3.12 Web Browser Security ..................................................................................................... 71
   3.13 Hardening Guidelines ...................................................................................................... 74
       3.13.1 D1: Unsecured Desktop ............................................................................................. 74
3.13.2 D2: Stand-alone Desktop Application ................................................. 75
3.13.3 D3: Client/Server Application in Office Environment ..................... 76
3.13.4 D4: Client/Server Application in a Secured Location/Control Room .. 78
3.13.5 D5: Client/Server Application in a Professional IT Environment ....... 80

4 Checklist ........................................................................................................ 82
About This Document

Purpose
These guidelines are designed to provide the system owner with information security guidelines and controls for Desigo CC system. It describes all the permitted applications for the intended operational environment as well as security-related information for the system owner for maintaining security in the life cycle of the system.

Scope
This document applies to Desigo CC V4.1.

Retention and Availability

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Damage Due to Misuse</strong></td>
</tr>
<tr>
<td>This document must be available in a usable format throughout the entire life cycle of the product. Keep the document for reference and ensure that it can be accessed by target groups.</td>
</tr>
</tbody>
</table>

For additional information on building technology security and our offerings, contact your Siemens sales or project department. We strongly recommend signing up for our security advisories, which provide information on the latest security threats, patches and other mitigation measures.


Target Audience

**Network Administrator** works in the customer or system integrator IT department and is responsible for network design and configuration, including network security controls, such as network segmentation and network access control.

**System administrator** works in the customer or system integrator IT department and is responsible and is responsible for deployment of IT assets and SW components, including their security hardening.

**Field Engineers** provide the basic installation of devices and systems for a specific customer at the customer site. They have the training appropriate to their function and to the products, devices, and systems to be installed. They are also familiar with the applied operating system(s) and the related network environment. Field engineers are responsible for infrastructure troubleshooting (for example, hardware, communication, network, and so on).

Source Language and Reference Document

- The source/original language of this document is English (en).
- The reference version of this document is the international version in English. The international version is localized to German (de).
Applicable Documents

<table>
<thead>
<tr>
<th>Title</th>
<th>Document ID/Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security for industrial process measurement and control – Network and system security</td>
<td>IEC 62443-3</td>
</tr>
</tbody>
</table>

Technical Terms and Abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>The Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.</td>
</tr>
<tr>
<td>BACnet</td>
<td>BACnet is a communications protocol for Building Automation and Control (BAC) networks. BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment. The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the particular building service they perform.</td>
</tr>
<tr>
<td>BIOS</td>
<td>BIOS is non-volatile firmware used to perform hardware initialization during the booting process (power-on startup), and to provide runtime services for operating systems and programs.</td>
</tr>
<tr>
<td>CAPI Certificates</td>
<td>The Microsoft windows platform specific Cryptographic Application Programming Interface (also known variously as CryptoAPI, Microsoft Cryptography API, MS-CAPI or simply CAPI) is an application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. It is a set of dynamically linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data. The Crypto API was first introduced in Windows NT 4.0 and enhanced in subsequent versions. CryptoAPI supports both public-key and symmetric key cryptography, though persistent symmetric keys are not supported. It includes functionality for encrypting and decrypting data and for authentication using digital certificates. It also includes a cryptographically secure pseudorandom number generator function CryptGenRandom. CryptoAPI works with a number of CSPs (Cryptographic Service Providers) installed on the machine. CSPs are the modules that do the actual work of encoding and decoding data by performing the cryptographic functions. Vendors of HSMs may supply a CSP which works with their hardware.</td>
</tr>
<tr>
<td>DiffieHellmann</td>
<td>Diffie–Hellman key exchange (DH) is a method of securely exchanging cryptographic keys over a public channel. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.</td>
</tr>
</tbody>
</table>
### DMZ
DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network and, if its design is effective, allows the organization extra time to detect and address breaches before they would further penetrate into the internal networks.

### ESPA 4.4.4
ESPA 4.4.4 is a protocol controlling wireless pagers. It uses ISO 1745, point-to-point on RS232 as data link layer. The AlphaCom can use this in two ways:
- **Output:** Sends a *start paging* message to a wireless pager transmitter either due to manual action by a user, or by automatic action such as an activation of an input (alarm).
- **Input:** The AlphaCom can be set up to look like a pager transmitter. The AlphaCom inspects the display text and generates events to the Event Handler which do a range of actions. *(Fire Alarm protocol).* The ESPA 4.4.4 message is finally forwarded to one of the AlphaCom's pager protocol outputs.

### FEP
Front End Processor is a computer that extends and distributes connectivity to field networks. The purpose is to off-load from the host computer the work of managing the peripheral devices, transmitting and receiving messages, packet assembly and disassembly, error detection, and error correction.

### Firewall
Firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

### HDB
History Database. Desigo CC History Database server manages historical data collected from subsystems and user activities. The server uses Microsoft SQL to store, manage and maintain the historic data of the system.

### IEC
The International Electrotechnical Commission is an international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as *electrotechnology*.

### IIS
Internet Information Services is an extensible web server created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP.

### IPv4
Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, and was the first version deployed for production in the ARPANET in 1983.
IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model; in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

### IPv6
Internet Protocol version 6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.
<table>
<thead>
<tr>
<th>Technical Terms and Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA-99/IEC 62443 Security Level</td>
</tr>
<tr>
<td>ANSI/ISA 62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (for example, asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, implementing, or managing IACS. These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.</td>
</tr>
<tr>
<td>ISO</td>
</tr>
<tr>
<td>The International Organization for Standardization is an international standard-setting body composed of representatives from various national standards organizations.</td>
</tr>
<tr>
<td>MNS</td>
</tr>
<tr>
<td>Mass Notification System is a platform that sends one-way messages to inform employees and the public of an emergency. Such systems can improve the safety and security of an organization by providing alerts and real-time instruction during a crisis.</td>
</tr>
<tr>
<td>NTLM</td>
</tr>
<tr>
<td>In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN), an older Microsoft product. The NTLM protocol suite is implemented in a Security Support Provider, which combines the LAN Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in a single package. Whether these protocols are used or can be used on a system is governed by Group Policy settings, for which different versions of Windows have different default settings. NTLM passwords are considered weak because they can be brute-forced very easily with modern hardware.</td>
</tr>
<tr>
<td>NTP</td>
</tr>
<tr>
<td>OPC</td>
</tr>
<tr>
<td>The OPC Foundation (OPC formally known as Object Linking and Embedding for Process Control) is an industry consortium that creates and maintains standards for open connectivity of industrial automation devices and systems, such as industrial control systems and process control generally. The OPC standards specify the communication of industrial process data, alarms and events, historical data and batch process data between sensors, instruments, controllers, software systems, and notification devices.</td>
</tr>
<tr>
<td>OPC DA</td>
</tr>
<tr>
<td>OPC Data Access. This group of standards provides specifications for communicating real-time data from data acquisition devices such as PLCs to display and interface devices like Human-Machine Interfaces (HMI). The specifications focus on the continuous communication of data.</td>
</tr>
<tr>
<td>OPC UA</td>
</tr>
<tr>
<td>OPC Unified Architecture. An entirely new set of standards that incorporates all of the functionality of the above standards (and more), but does so using cross platform web services and other modern technology.</td>
</tr>
</tbody>
</table>
Personal Store

The *Local Machine Personal* store contains certificates used either by applications as client/server certificates and belong to this computer only; whereas the *Current User Personal* store contains certificates not bound to any particular machine (for example, you may have a certificate you use to digitally sign documents on several different machines).

The certificate and its private key must be imported into the Windows certificate store (in the Local machine\Personal store; its root certificate must be imported in the Local machine\Trusted Root Certification Authorities (TRCA) store). The private key must be marked as exportable.


PLC

Programmable logic controller or programmable controller is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis.

PMON

Process MONitor is an Oracle background process created when you start a database instance. The PMON process will free up resources if a user process fails (for example, release database locks).

PMON normally wakes up every 3 seconds to perform its housekeeping activities. PMON must always be running for an instance. If not, the instance will terminate.

Public key certificate

In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key.[1] The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.[2] In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization. However, in Transport Layer Security (TLS) a certificate's subject is typically a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name Secure Sockets Layer (SSL), is notable for being a part of HTTPS, a protocol for securely browsing the web.

In a typical public-key infrastructure (PKI) scheme, the certificate issuer is a certificate authority (CA), usually a company that charges customers to issue certificates for them. By contrast, in a web of trust scheme, individuals sign each other's keys directly, in a format that performs a similar function to a public key certificate.

The most common format for public key certificates is defined by X.509. Because X.509 is very general, the format is further constrained by profiles defined for certain use cases, such as Public Key Infrastructure (X.509) as defined in RFC 5280.

https://en.wikipedia.org/wiki/Public_key_certificate

RDP

Remote Desktop Protocol is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

RENO

Remote Notification are notification messages that Desigo CC can deliver, for example, using email, SMS or pagers—to one or more groups of contacts (recipients). They can be of two types: Alarm-based remote notifications: Messages preconfigured to be sent out by the system (or manually by the operator) when certain alarms occur in the building control site. New remote notifications: Messages composed and sent on the initiative of the operator. These operator-issued notifications are not tied to any triggering event.
<table>
<thead>
<tr>
<th>Technical Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA (Rivest–Shamir–Adleman)</td>
<td>One of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public, and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the <em>factoring problem</em>.</td>
</tr>
<tr>
<td>Samba</td>
<td>A Linux application to provide shared access to files for Windows platform computers.</td>
</tr>
<tr>
<td>SHA-2</td>
<td>SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). They are built using a one-way compression function built from a (classified) specialized block cipher. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed <em>hash</em> (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity.</td>
</tr>
<tr>
<td>SI</td>
<td>Smart Infrastructure – Siemens Division.</td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block is an application layer network protocol, mainly used for providing shared access to files.</td>
</tr>
<tr>
<td>SMC</td>
<td>The System Management Console is a standalone tool that initializes a new project, restores a project, and configures system-wide settings such as history database, system users and web server parameters. System Management Console provides the user interface to configure and administer the system and host field system drivers. The server hosts the project to monitor and control the facility including runtime data. Projects are managed by the System Management Console.</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets layer is a cryptographic protocol that provides communication security over a computer network. <a href="https://www.tutorialsteacher.com/https/how-ssl-works">https://www.tutorialsteacher.com/https/how-ssl-works</a></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network. Several versions of the protocols find wide-spread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.</td>
</tr>
<tr>
<td>UAC</td>
<td>User Account Control is a technology and security infrastructure that aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. In this way, only applications trusted by the user may receive administrative privileges, and malware should be kept from compromising the operating system.</td>
</tr>
<tr>
<td>VAP</td>
<td>Value added partner - Solution Partner.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Access Network. Any broadcast domain that is partitioned and isolated in a computer network.</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>Virtual Private Network. It extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.</td>
</tr>
<tr>
<td><strong>XBAP</strong></td>
<td>XAML Browser Applications (XBAP, pronounced <em>ex-bap</em>) are Windows Presentation Foundation (.xbap) applications that are hosted and run inside a web browser such as Firefox or Internet Explorer.</td>
</tr>
<tr>
<td><strong>XAML</strong></td>
<td>Extensible Application Markup Language is a declarative XML-based language developed by Microsoft that is used for initializing structured values and objects.</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>Extensible Markup Language is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.</td>
</tr>
</tbody>
</table>
Acknowledgements

Responsibility of the System Owner
The information technology (IT) used on site is the responsibility of the system owner.

Standards, Regulations and Legislation
Follow the policies of your company as well as any national regulations or international standards, such as ISO/IEC 27002 and IEC62443.
The Federal Office for Information Security (BSI) provides information on basic Cybersecurity for Germany in both German and English, for example.

Product Security Guidelines
The security guidelines in this document provide the system owner with additional specifications – alongside basic IT protection – for operating a corresponding system. These additional specifications are valid at the time of publication.

Cybersecurity Disclaimer
Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens’ portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens’ guidance on appropriate security measures should be taken into account.

For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html.

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.
## Document Revision History

### Document Identification
The document ID is structured as follows:
ID_Language(COUNTRY)_ModificationIndex_ProductVersionIndex
Example: A6Vnnnnnnnnn_en_a_02

<table>
<thead>
<tr>
<th>Modification Index</th>
<th>Edition Date</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>2019-11-30</td>
<td>Third edition, corresponding with Desigo CC V4.1</td>
</tr>
<tr>
<td>b</td>
<td>2019-06-30</td>
<td>Second edition, corresponding with Desigo CC V4.0</td>
</tr>
<tr>
<td>a</td>
<td>2019-03-30</td>
<td>First edition, corresponding with Desigo CC V3.0</td>
</tr>
</tbody>
</table>
1 Cybersecurity Basics

1.1 Introduction

Cybersecurity includes all mechanisms for defending IT systems (such as computers, devices like primary controllers or web servers of a building automation system) against loss of system and information confidentiality, integrity and availability through unauthorized access, disruption, modification, destruction or retrieval of Unrestricted information as well as the usage of information gained without authorization through fraud and other criminal acts. Cybersecurity can be implemented according to the requirements set out by different industry and national standards that usually define various protection levels depending on the usage of the system and the acceptable risk level.

So far, the large majority of Cybersecurity breaches have been attacks on traditional computer systems, such as internet, intranet or home networks. Damages caused include denial of service, theft of critical private and business information, the defrauding of bank accounts and credit cards and, most recently, so-called ransomware.

In contrast, there have been fewer attacks on industrial controllers, such as building automation controllers because they mostly run on proprietary operating systems, the hardware has limited functionality and they are rarely connected to other networks. Recently, industrial controllers have started to adopt mainstream computer standards in order make them cheaper and more powerful; they are also very often connected to other customer networks and the internet which, in turn, makes them more vulnerable to attackers. Moreover, interconnections can be used to launch an attack from the corporate network to the automation one and vice versa.

Therefore, it becomes important to provide an adequate level of security together with modern building technology solutions.

1.2 Threat and Risk Terminology

The following is a brief glossary of common terminology used in Cybersecurity.

An asset is a material or immaterial entity that must be protected. It is important to list the relevant assets and understand their values (for the business and potential attackers) in order to define the correct level of protection.

A vulnerability is a weakness or lack of protection of a system that can be exploited. Examples are hardcoded passwords, network services that do not properly verify their inputs, self-made cryptography algorithms, and so on.

The exposure defines how easily an attacker can get access to the system in order to perform malicious actions. Typically, the exposure is high if the system is connected to the internet and can thus be reached from remote.

A threat is any potential damage that can result from the exploitation of vulnerability by a threat agent, for example, a hacker can spot and use a hardcoded password to gain access to a system.

The impact is the amount of damage that is suffered by assets in case there is a Cybersecurity incident. In some cases, it is possible to estimate the extent of the damage, even in monetary terms, such as the costs of replacing devices. However, more often, the damage involves a loss of reputation and other intangible assets that are difficult to calculate.

A risk is the probability that the threat agent would find and exploit the vulnerability weighted with the relative impact on the business, for example, a hacker can find the default admin password in some documentation: if the password was not properly
changed during the engineering phase, the system is at high risk, because the hacker can use it to install malicious software with administrator privileges.

A control or countermeasure is put in place to mitigate the risk and can include HW or SW procedures, for example, a system with default passwords can be isolated from the rest of the system to reduce the likelihood of being accessed by an attacker.

![Figure 1: Threat and Risk Terminology](image)

### 1.3 System Security

As explained in the introduction, every modern building automation system must ensure an adequate level of Cybersecurity protection. It is, however, impossible to reach a complete level of security, so that there is always a residual risk. The cost of a countermeasure must not exceed the potential damage it can provide. In any case, the system owner must understand the residual risk and decide if it is acceptable for the business.

It is important to adopt a systematic view of the security requirements, so that the effectiveness of the controls is evaluated as a whole, rather than addressing every component separately. In particular, compensatory counter measures can be employed to mitigate the vulnerabilities of given subsystems so that the overall desired security level is achieved.

It is also important that the different players involved contribute to the system (manufacturers, system integrators and operators) according to their specific roles. The responsibility of the manufacturers is to deliver security-capable products, up to the level specified in their product documentation. The integrators are responsible to design and deploy the solution according to the security specifications of the operator and to respect the intended operational environments of used products. Finally, the system operators are responsible for ensuring that the security is kept up to date within the lifetime of the solution.

Maintaining the security of the solution requires establishing a continuous security program framework that periodically assesses the desired target security level, the risks of the system, the status and effectiveness of deployed controls and implements corrective measures.
The guidelines detailed in this document support a continuing process to achieve Cybersecurity at system level.

1.4 SSL Certificates

SSL stands for Secure Sockets Layer, a global standard security technology that enables encrypted communication between a web browser and a web server. It is utilized by millions of online businesses and individuals to decrease the risk of sensitive information (for example, credit card numbers, usernames, passwords, emails, and so on) from being stolen or tampered with by hackers and identity thieves. In essence, SSL allows for a private conversation between the two intended parties only.

To create this secure connection, an SSL certificate (also referred to as a digital certificate) is installed on a web server and serves two functions:

- It authenticates the identity of the website (this guarantees visitors that they are not on a bogus site).
- It encrypts the data that is being transmitted.

SSL versus TLS

SSL and TLS generally mean the same thing. TLS 1.0 was created by RFC 2246 in January 1999 as the next version of SSL 3.0. Most people are familiar with the term SSL so that is usually the term that is used when the system is using the newer TLS protocol.

SSL creates an encrypted connection between your web server and your visitors' web browser allowing for private information to be transmitted without the problems of eavesdropping, data tampering, and message forgery.

To enable SSL on a website, you need to get an SSL Certificate that identifies you and you have to install it on your web server. When a web browser is using an SSL certificate it usually displays a padlock icon, but it may also display a green address bar. Once you have installed an SSL Certificate, you can access a site securely by changing the URL from http:// to https://. If SSL is properly deployed, the information transmitted between the web browser and the web server (whether it is contact or credit card information), is encrypted and only seen by the organization that owns the website.

“SSL Certificates are small data files that digitally bind a cryptographic key to an organization’s details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.”

Who may need an SSL certificate

Any individual or organization that uses their website to require, receive, process, collect, store, or display Unrestricted or sensitive information. Some examples of this information are:

- Logins and passwords
- Financial information (for example, credit card numbers, bank accounts)
- Personal data (for example, names, addresses, social security numbers, birth dates)
- Proprietary information
- Legal documents and contracts
- Client lists
- Medical records
How to know if a website is secure
The presence of an SSL certificate helps in determining whether or not a website is
secured. Websites secured with an SSL certificate have a green address bar, a green
padlock symbol near the URL and also have HTTPS as the prefix to their URL. All
these indicators help in determining whether or not a website is enough secure.

Factors to consider before buying an SSL Certificate
There are several factors to consider before choosing a certificate.
- Speed of issuance
- Warranty period
- Type of validation
- Domains and subdomains covered
- Market reputation of the brand

What is the SSL Certificate
The SSL certificate (also known as digital certificate) plays an important role in
securing the communication between two systems.
The SSL certificate is a data file issued by the authorized Certificate Authority (CA). As
stated in the previous chapter, SSL uses asymmetric cryptography to establish an
encrypted link between the two systems using a key pair (public key and private key).
The SSL certificate contains the owner's public key and other details. The web server
sends a public key to the browser through an SSL certificate and the browser verifies
it and authenticates the web server using the SSL certificate.
The X.509 standard defines the format of the digital certificate. SSL uses the X.509
format. In other words, SSL certificates are actually X.509 certificates.
The SSL certificate in X.509 format includes the following information:
- Version: The version number of the certificate data format as per X.509.
- Serial number: Unique identifier of the certificate assigned by the CA
- Public Key: The owner's public key
- Subject: Owner's name, address, country and domain name
- Issuer: Name of the CA who issued the certificate
- Valid-From: The date the certificate is valid from
- Valid-To: The expiration date
- Signature Algorithm: The algorithm used to create the signature
- Thumbprint: The hash of the certificate
- Thumbprint Algorithm: The algorithm used to create a hash of the certificate

Types of SSL Certificates
There are different types of SSL certificates available today based on the validation
level and the number of domains they secure. The encryption levels remain the same
for all types of certificates, but the validation levels and appearance are different.
There are many different types of SSL certificates based on the number of domain
names or subdomains owned, such as:
- Single – secures one fully qualified domain name or subdomain name
-Wildcard – covers one domain name and an unlimited number of its subdomains
- Multi-Domain – secures multiple domain names
And the level of validation needed, such as:
• **Domain Validation** – this level is the least expensive and covers basic encryption and verification of the ownership of the domain name registration. This type of certificate usually takes a few minutes to several hours to receive.

• **Organization Validation** – in addition to basic encryption and verification of ownership of the domain name registration, certain details of the owner (such as name and address) are authenticated. This type of certificate usually takes a few hours to several days to receive.

• **Extended Validation (EV)** – this provides the highest degree of security because of the thorough examination that is conducted before this certificate is issued (and as strictly specified in guidelines set by the SSL certification industry’s governing consortium). In addition to ownership of the domain name registration and entity authentication, the legal, physical and operational existence of the entity is verified. This type of certificate usually takes a few days to several weeks to receive.

**Compare types of SSL Certificates**

• **Domain Validation (DV) SSL**
  – Proves domain ownership
  – Boosts Google® ranking
  – Strong SHA-2 and 2048-bit encryption

• **Organization Validation (OV) SSL**
  – Proves domain ownership
  – Validates organization
  – Boosts Google® ranking
  – Strong SHA-2 and 2048-bit encryption

• **Extended Validation (EV) SSL**
  – Proves domain ownership
  – Validates organization
  – Shows business is legitimate
  – Displays business name on the green address bar
  – Boosts Google® ranking
  – Strong SHA-2 and 2048-bit encryption

**Supported Cryptographic algorithms in Desigo CC**

Desigo CC supports RSA-2048 SHA-256 Certificates. Basically, CAPI certificates are required. The Web Server also supports CNG Certificates.
### Types of SSL Certificates based on Validation Level

Websites use SSL certificates to set up a trust level with their visitors and customers. Different businesses require to set up different levels of trust. For example, websites which collect user's important information need to transfer it securely. Financial institutions need to set up domain authenticity as well as data security. So, CA needs to validate the website owner's information based on the trust they want to set up. The following three types of certificates are based on the level of validation.

**Domain Validated Certificates**

The Domain Validated (DV) certificate requires the lowest level validation because the main purpose of DV certificates is to make the secure communication between the domain's web server and browser. CA only verifies that the owner has a control over the domain.

**Organization Validated Certificates**

The Organization Validated (OV) certificate requires a medium level validation where CA checks the rights of an organization to use the domain and also the organization's information. The OV certificate enhances the trust level of the organization and its domain.

**Extended Validated Certificates**

The Extended Validated (EF) certificate requires a high-level validation where CA conducts rigorous background checks on the organization according to guidelines. This includes verification of the legal, physical and operational existence of the entity.

### Types of SSL Certificates based on the Number of Domains they Secure

The following certificates are based on the number of domains needs to be se-cured.

**Single Domain Certificate**

The single domain certificate secures one fully qualified domain name. For example, a single domain certificate for www.example.com will not secure the communication for mail.example.com.

**Wildcard SSL Certificate**

The wildcard SSL certificate secures an unlimited number of subdomains for a single domain. For example, a wildcard SSL certificate for example.com will also secure mail.example.com, blog.example.com, and so on.

<table>
<thead>
<tr>
<th>Components</th>
<th>Crypto API Certificates</th>
<th>CNG Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinCC OA Communication</td>
<td>RSA 2048 with SHA256 encryption Certificates supported; Certificate revocation not supported.</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Web Server Communication</td>
<td>No known restrictions since this is completely managed by IIS. Anyway, it is recommended to have certificate with minimum RSA 2048 with SHA256 encryption.</td>
<td>No known restrictions since this is completely managed by IIS. Anyway, it is recommended to have certificate with minimum RSA 2048 with SHA256.</td>
</tr>
<tr>
<td>Client Identification</td>
<td>RSA 2048 with SHA256 encryption Certificates supported.</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Application/Code signing</td>
<td>RSA 2048 with SHA256 encryption Certificates supported. Certificate should be exportable and should have code signing feature.</td>
<td>RSA 2048 with SHA256 encryption Certificates supported. Certificate should be exportable and should have code signing feature.</td>
</tr>
</tbody>
</table>
Unified SSL Certificate/Multi-Domain SSL Certificate/SAN Certificate
The unified SSL certificate secures up to 100 domains using the same certificate with the help of the SAN extension. It is especially designed to secure Microsoft Exchange and Office Communication environments.

Once you choose what type of SSL certificate you require, you must obtain it from a trusted CA.

Where you can get SSL certificates
Probably the most important part of an SSL certificate is where it comes from. SSL certificates are issued by Certificate Authorities (CAs), organizations that are trusted to verify the identity and legitimacy of any entity requesting a certificate.

The CA’s role is to accept certificate applications, authenticate applications, issue certificates, and maintain status information on certificates issued.

You may also be able to purchase digital certificates from a domain name registrar or website hosting provider.

Certificate authority (CA)
A certificate authority is an entity which issues digital certificates to organizations or people after validating them. Certification authorities have to keep detailed records of what has been issued and the information used to issue it and are audited regularly to make sure that they are following defined procedures. Every certification authority provides a Certification Practice Statement (CPS) that defines the procedures that will be used to verify applications. There are many commercial CAs that charge for their services (VeriSign). Institutions and governments may have their own CAs, and there are also free Certificate Authorities.

Every certificate authority has different products, prices, SSL certificate features, and levels of customer satisfaction.

Browser compatibility
The certificate that you purchase to secure your website must be digitally signed by another certificate that is already in the trusted store of your user’s web browser. By doing this, the web browser will automatically trust your certificate because it is issued by someone that it already trusts. If it is not signed by a trusted root certificate, or if links in the certificate chain are missing, then the web browser will give a warning message that the website may not be trusted.

So, browser compatibility means that the certificate you buy is signed by a root certificate that is already trusted by most web browsers that your customers may be using. Unless otherwise noted, the certificates from all major certificate providers listed on SSL Shopper are compatible with 99% of all browsers.

How many domain names can be secured
Most SSL server certificates will only secure a single domain name or subdomain. For example, a certificate could secure www.yourdomain.com or mail.yourdomain.com but not both. The certificate will still work on a different domain name, but the web browser will give an error anytime it sees that the address in the address bar does not match the domain name (called a common name) in the certificate. If you need to secure multiple subdomains on a single domain name, you can buy a wildcard certificate. For a wildcard certificate, a common name of *.yourdomain.com would secure www.yourdomain.com, mail.yourdomain.com, secure.yourdomain.com, and so on. There are also special certificates such as Unified Communications (UC) or Multi-Domain SSL certificates that can secure several different domain names in one certificate.
Trust seal
A trust seal is a logo that you can display on your website that verifies that you have been validated by a specific certificate provider and you are using their SSL certificate to secure your site. It can be displayed on secure and non-secure pages and is most appropriate on pages where customers are about to enter their personal information such as a shopping cart page, but they can be displayed on every page to help build trust. Every certificate authority's trust seal is different and some look more professional so you should consider what the seal looks like in order to maximize the customer's trust.

Some things to keep in mind
When choosing the right SSL provider, consider the fact that users’ web browsers normally keep a cached list of trusted CAs on file – so if a digital certificate is signed by an entity that is not on the approved list, the browser will send a warning message to the user that the website may not be trustworthy.

How visitors know a site has an SSL certificate
There are four visual clues:
1. Padlock to the left of the URL
2. https URL prefix instead of http
3. A trust seal
4. A green address bar (when an EV SSL certificate is issued)

How to Get an SSL Certificate
You can get an SSL certificate from any authorized Certificate Authority (CA) to secure the communication between two systems.
There are two ways to get an SSL certificate:
1. Buy a certificate from CA.
2. Get a free certificate from a non-profit open CA.
Buy an SSL Certificate

You can buy an SSL certificate from CA or their reseller. The prices vary depending on the CA and type of the SSL certificate.

The following are the overall steps for buying SSL certificates from a CA:

1. **Choose a Certificate Authority (CA):** You can choose your CA from where you want to buy an SSL certificate. There are many CAs such as Comodo, DigiCert, RapidSSL, GeoTrust, Thawte, Certum, and so on. You may choose the CA based on your budget and the features you need to manage the certificate. There are resellers who provides cheap SSL certificates from these CAs.

2. **Select the certificate you need:** Once you select a CA, you can choose the certificate you require for your website based on the validation method and the number of websites you want to secure.

3. **Purchase the certificate:** Once you choose the certificate you require, make the payment to proceed. For some CA, this step comes after submitting a CSR.

4. **Generate and submit a CSR (Certificate Signing Request) to the CA:** You need to generate a CSR from your web server and submit it to the CA. To learn more about what a CSR is and how to generate it, see the next chapter.

5. **Download the SSL certificate (after successful validation):** After submitting a CSR, the CA will take some time for validating your information. This may vary based on the validation certificate you purchased. For a DV certificate, it should be quick. But it will take a little longer to validate for an OV or an EV certificate. Once the CA successfully validates your information, you will get an email containing the certificate or you can download it from your account on the CA's website.

6. **Install an SSL certificate on your web server:** Once you get your SSL certificate, you need to install it on the web server from where you generated your CSR. The installation process depends on the OS of your server.

Certificate Signing Request

In order to get an SSL certificate for your website, you need to generate and submit a Certificate Signing Request (CSR) to the CA (Certificate Authority).

What is a CSR?

A CSR is an encoded message submitted by an applicant to a CA to get an SSL certificate. In other words, it is a request from an applicant to a CA to get a digital certificate.

A CSR contains a public key and the applicant's information such as FQDN (Fully Qualified Domain Name), organization name and address. The CA validates the applicant's information and issues an SSL certificate with the public key included in the CSR.

Generally, a CSR is generated using the web server where the SSL certificate is going to be installed. However, it can also be generated using SSL tools or a modern browser such as Chrome or Firefox. The most common format for CSRs is the PKCS.

A CSR is a Base64 ASCII encoding message starting with "-----BEGIN NEW CERTIFICATE REQUEST-----" and ending with "-----END NEW CERTIFICATE REQUEST-----".
The following is a sample CSR:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIERzCCAY8CAQAwZ2ELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5ZMREwDwYDVQQH
DAhuZXcgeW9yazEPMA0GA1UECgwGbXkgb3JnMQswCQYDVQQQLDAiJVEaMBgGA1U
EAwRd3d3Lm15d2Vic210ZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBAgIC
AoIBAQCfkbkuJwMiowgvRAVlXS/H2FQH0I6/p2NyOn7onb8uEV3cmMF4iCzBN6
KJD9qVtmZSBpH9IqrYiEohTxkgJ2c/dyX06eDV87nE53etPO2CM8VqJ0q/7PD0+
7Kvy6jhQVU7Rb1mQrFcrU0GVOQWqptHwbeKFf3mR1PNzygmXAUXkv0XdstQPm
b5sVx965SGoIqrGRUDp1+UNUCeI198AVPEiDUg1VqY+mUmOcCk0153UtxDUMoc
gS5WlfD83We35a7I6++FAvDkk31g6v6Jxfs/EzZ6D0iityDMAWNRwDvaYcu06O8Ye/
rt9mFF90xMMn7xi0CaLzG7JrJaqMBAAAGggGZMBoGCisGAQQBgcNAgMxDBY
KNI4xLjcm2DMEuMjAlBgrBgEEAYI3FRQxKDAmAgEFDAkZWsLVBDAtkZWsLVBD
XER1dgwLSW5ldElnci5leGUwcgYKkwYBBAGCnx0CAjFkMGICAQEeWgBNAKAYwB
YAG8AcwBvAGYAdAAgAFIAUwBBACAuWBDAGgAYQBuAG4A2QBsACAAQwByAHKAcAB
0AG8AZwByAGEAcABoAGkAYwAgAFAAcBgvAHYAaQBkAGUAcMBADCBzwYJKoZIhvc
NAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEFBQcDATB
4BgkqhkiG9w0BCQ8EazBmA4GCCqGSIb3DQMCgIgDAOBqghkkiG9w0DBAICAIw
BAEFMAcGBs0AwIHMaoGCCqGSIb3DQHMB0GA1UdDgQWBBBS4t+amOyNS+ECWFIXw
eBUR+XrTv+TCTFtvFRIq35T960o79JqJ2paD+PS9HNg:lenS05l0dserA/pn/1rG9T+n
la6jTj6BEwOLaTfnq8KtkyYiROOC9LqhQCN84PQuO3L9c1LrsV//1C4hGkFUbG
-----END NEW CERTIFICATE REQUEST-----
```

**SSL Certificate Formats**

An SSL Certificate is essentially an X.509 certificate. X.509 is a standard that defines the structure of the certificate. It defines the data fields that should be included in the SSL certificate.

There are different formats of X.509 certificates such as PEM, DER, PKCS#7 and PKCS#12. PEM and PKCS#7 formats use Base64 ASCII encoding while DER and PKCS#12 use binary encoding. The certificate files have different extensions based on the format and encoding they use.
SSL Certificate Format

PEM Format
Most CAs (Certificate Authority) provide certificates in PEM format in Base64 ASCII encoded files. The certificate file types can be .pem, .crt, .cer, or .key. The .pem file can include the server certificate, the intermediate certificate and the private key in a single file. The server certificate and intermediate certificate can also be in a separate .crt or .cer file. The private key can be in a .key file.

PEM files use ASCII encoding, so you can open them in any text editor such as Notepad, Word, and so on.

Each certificate in the PEM file is contained between the statements:

```
---- BEGIN CERTIFICATE----
```---

The private key is contained between the statements:

```
---- BEGIN RSA PRIVATE KEY------
```---

The CSR is contained between the statements:

```
----BEGIN CERTIFICATE REQUEST------
```---

PKCS#7 Format
The PKCS#7 format is a Cryptographic Message Syntax Standard. The PKCS#7 certificate uses Base64 ASCII encoding with file extension .p7b or .p7c. Only certificates can be stored in this format, not private keys.

The P7B certificates are contained between the statements:

```
"-----BEGIN PKCS7-----" and "-----END PKCS7-----"
```

DER Format
The DER certificates are in binary form, contained in .der or .cer files. These certificates are mainly used in Java-based web servers.

PKCS#12 Format
The PKCS#12 certificates are in binary form, contained in .pfx or .p12 files. The PKCS#12 can store the server certificate, the intermediate certificate and the private key in a single .pfx file with password protection. These certificates are mainly used on the Windows platform.

CAs provide certificates in any of the above formats.

Install an SSL Certificate
Here follows the steps for installing an SSL certificate on your web server.

Installation of an SSL certificate depends on many things such as where you generated the CSR, the type of certificate files you obtained from the CA, the types of certificate files your web server supports and so on.

The following are the steps involved in the process:

1. Gather the necessary files.
2. Identify the certificate file type and format your web server requires.
3. Convert the certificate file type to web server compatible files.
4. Install the certificates on your web server.
5. Bind the installed SSL certificate to your website.
6. Test the certificate.
1 — Gather the necessary files
In order to install an SSL certificate on your web server and bind it to your domain, you must have the following files:

1. SSL Certificate for your domain
2. Intermediate certificates or CA bundle (optional)
3. Private key

You must obtain a certificate file for your domain and intermediate certificate files from the CA where you submitted the CSR. The CA may not have issued an intermediate certificate or may have issued more than one intermediate certificate. Most likely you will have intermediate one or more certificates.

You may have the private key stored in a .key file type. However, it depends on where you generated the CSR and where you want to install it. If you generated the CSR from the same web server where you want to install an SSL certificate, then you will not have a private key file because it is secretly stored by the web server. If you generated the CSR using a browser or an SSL tool, then you should have a saved private key in a separate .key file. If the web server where you generate the CSR is different from the web server where you are going to install the certificate, then you need to export the private key from where you generated the CSR because the private key is generated at the same time when the CSR is generated.

So, gather all the required files before proceeding.

2 — Identify the certificate file type and the format your web server requires
Once you have the necessary certificate files, you need to check the certificate file type and the format your web server supports. Different web servers and hosting platforms support different formats and types of certificate files. For example, Apache and other similar web servers support certificates in PEM format, whereas Microsoft Windows support certificates in PKCS#7 format.

Some web servers and hosting platforms require separate certificate, intermediate certificate and private key files, whereas others require a single file for all. For example, Microsoft Azure cloud platform requires all files in a single PKCS#12/PFX format.

So, identify the appropriate format and file type that your web server supports.

3 — Convert the certificate file type to web server compatible files
If the certificate files and format you obtained from the CA are not supported on your web server or hosting provider, then you have to convert the certificates to your web server supported format using OpenSSL.

Convert your SSL certificate files as per your web server supported format using OpenSSL. Some web servers require a single file for your domain certificate, intermediate certificate and private key while other web servers require a separate file for each. For example, Azure App Service requires PKCS#12 format in a .pfx file with certificate, intermediate certificate and private key. So, you need to consider that too.

To learn about OpenSSL conversion commands, see the next chapter.

4 — Install the certificates on your web server
So, once you have certificate files in the required format and type, you can install your SSL certificate on your web server. In the Desigo CC online help, see Configuring Security in Typical Deployments.

5 — Bind the installed SSL certificate to your website
Once you have installed your SSL certificate, you have to bind it to your website. Again, this depends on the web server or hosting provider.

6 — Test the https website
In this last step, you should test your SSL certificate with the SSL tools and check whether or not it is working properly.
2 Network Security Controls

The following sections detail the concept of a protected system configuration as well as specific use cases. The network security-related controls aim at mitigating the risk of exploitation of possible Desigo CC vulnerabilities.

To enhance security, follow the policies of your company as well as any national legislations or international standards, such as ISO/IEC 27002 and IEC62443.

2.1 Protected System Configuration Concept

The Desigo CC system is a critical business application and must be protected from attacks and unauthorized access.

Desigo CC (server) should be operated in a separated network zone further called backbone. Desigo CC (web server) should also be operated in a separated zone called DMZ (demilitarized zone).

The components in the DMZ and backbone zones should not be connected to other networks (for example, intranet or internet), with the exception of the required connections detailed in this document. Required connections are those to the clients in the Office network and DMZ. The communication between DMZ and backbone and other zones should be limited to the necessary minimum by means of a firewall.

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insecure Networks</td>
</tr>
<tr>
<td>Connections between computers in backbone level and insecure networks like the internet or any other networks can compromise the security of the system.</td>
</tr>
</tbody>
</table>
2.1.1 Zone Boundary Protection

- The Desigo CC backbone level and DMZ level are security zones that are physically protected (for example, locked in rack in server room) and use separated networks that only permit Restricted access to its components.
- A separate VLAN alone does not meet the requirements for zone boundary protection. A firewall is required too.
- Allowed components in the Desigo CC backbone level protection zone are: Desigo CC server, Desigo CC computer with Secure Global Desktop and Samba server, related clients and printers. In case one of the allowed components is remote, a physically protected and secured communication is also required.
- Allowed components in the Desigo CC DMZ level protection zone are: Desigo CC as well as an optional computer with OPC Clients or Secure Global Desktop.
- The zone boundary protection must be implemented via firewall to limit the inbound and outbound communication among network zones.
Figure 2: Zone Boundary Protection
2.1.2 System Components

As illustrated below, the Desigo CC software can be installed on a single server or broken up in the following main functional blocks:

- Management System Server: Monitors and commands the field networks, executes automatic actions and interacts with users through clients.
- Database Server: Manages the Historical data collected by Desigo CC.
- MNS
- Video
- Web Server: provides connectivity for web clients.
- FEP (Front End Processor): Extends and distributes connectivity to field networks.
- Installed Clients: Provide user access to Desigo CC user functionalities, connecting directly to the Management System Server.
- Windows App and Web Clients: Provide user access to Desigo CC functionalities through the web server.

Figure 3: Protected System Configuration Concept
2.1.3 Firewall Rules

The firewall rules table shows a list of required ports and services needed to allow the communication between different network zones of a protected system configuration. In general, all the protective controls for data connections/network traffic at zone boundaries must be configured as follows:

- Deny by default.
- Allow only ports/services that are required to operate Desigo CC.

The following list exemplifies the allowed ports/services for a typical system configuration. Depending on system configuration on site, divergent set of rules may result.

Ideally, an advanced Firewall should:

- Identify and control applications on any port
- Identify and control anomalous behavior
- Decrypt outbound SSL/TLS and control SSH
- Provide application function control
- Systematically manage unknown traffic
- Scan for viruses and malware in all applications, on all ports
- Enable the same application visibility and control for all users and devices
- Make network security simpler, not more complex, with the addition of application control

1) See the description of the certificate usage in the sections that follow.

Firewall Settings

When using Desigo CC with a firewall, the execution of processes that open ports for the communication are Unrestricted by the firewall.

You must add the following ports as exceptions to the firewall if you are installing Desigo CC on a server. Configuring your firewall settings allows the access between the server and all its client stations and also between the server and field panels.

The table below lists the TCP and UDP ports you should add to the server firewall and any network firewalls between the server and clients and the server and field panels.

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not open a port for a program you do not recognize. The following table lists all the ports required for safe operation of the system. Ports that are not required for system operation must be closed for security risks.</td>
</tr>
</tbody>
</table>
## Server Communication

Port usage across machine boundaries for client-server and server-server communication

### Core Services on Main Server

<table>
<thead>
<tr>
<th>Providing Component</th>
<th>Default Port</th>
<th>Protocol</th>
<th>Port Config.</th>
<th>Port exposure to other machines in the network</th>
<th>Connects to this port</th>
<th>Refer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Manager</td>
<td>TCP: 4897</td>
<td>SMC</td>
<td>WinCC OA Communication</td>
<td>Exposed if project is set to &quot;Nonsecure&quot; in SMC</td>
<td>Installed Client (Non secure)&lt;sup&gt;(2)&lt;/sup&gt; FEP (Nonsecure)&lt;sup&gt;(3)&lt;/sup&gt;</td>
<td>2.2.2 [➙ 44] 2.2.4 [➙ 51] 2.2.5 [➙ 56] 2.2.6 [➙ 58] 2.2.7 [➙ 59]</td>
</tr>
<tr>
<td>WCCILdata.exe&lt;sup&gt;(1)&lt;/sup&gt;</td>
<td>UDP: 4897</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Manager</td>
<td>TCP: 4998</td>
<td>SMC</td>
<td>WinCC OA Communication</td>
<td>Exposed if project is set to &quot;Nonsecure&quot; in SMC</td>
<td>Installed Client (Non secure)&lt;sup&gt;(2)&lt;/sup&gt; FEP (Nonsecure)&lt;sup&gt;(3)&lt;/sup&gt;</td>
<td>2.2.2 [➙ 44] 2.2.4 [➙ 51] 2.2.5 [➙ 56] 2.2.6 [➙ 58] 2.2.7 [➙ 59]</td>
</tr>
<tr>
<td>WCCILevent.exe&lt;sup&gt;(1)&lt;/sup&gt;</td>
<td>UDP: 4998</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution Manager</td>
<td>TCP: 4777</td>
<td>SMC</td>
<td>WinCC OA Communication</td>
<td>Distributed systems only Exposed if project is set to &quot;Nonsecure&quot; in SMC</td>
<td>Remote System (Non secure)&lt;sup&gt;(1)&lt;/sup&gt;</td>
<td>n/a</td>
</tr>
<tr>
<td>WCCILdist.exe&lt;sup&gt;(1)&lt;/sup&gt;</td>
<td>UDP: 4777</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDB Reader</td>
<td>TCP: 7774</td>
<td>SMC</td>
<td>WinCC OA Communication</td>
<td>Exposed if project is set to &quot;Nonsecure&quot; in SMC</td>
<td>Installed Client (Non secure)&lt;sup&gt;(2)&lt;/sup&gt;</td>
<td>2.2.2 [➙ 44]</td>
</tr>
<tr>
<td>WCCOAHDBReader.exe&lt;sup&gt;(2)&lt;/sup&gt;</td>
<td>UDP: 7774</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCom Manager</td>
<td>TCP: 8000</td>
<td>SMC</td>
<td>HTTP(S) – WCF Web Service</td>
<td>Exposed if 'Web Server Communication' is enabled</td>
<td>Separate Web Server&lt;sup&gt;(3)&lt;/sup&gt;</td>
<td>2.2.3 [➙ 47] 2.2.4 [➙ 51] 2.2.5 [➙ 56] 2.2.6 [➙ 58] 2.2.7 [➙ 59]</td>
</tr>
<tr>
<td>WCCOACCComMgr.exe&lt;sup&gt;(2)&lt;/sup&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Providing Component</td>
<td>Default Port</td>
<td>Port Config.</td>
<td>Protocol</td>
<td>Port exposure to other machines in the network</td>
<td>Connects to this port</td>
<td>Intended Operat. Environm.</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>---------------------------</td>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>SSL Proxy Manager WCCILproxy.exe³</td>
<td>TCP: 5678</td>
<td>SMC</td>
<td>WinCC OA Communication</td>
<td>Exposed if project is set to &quot;Secure&quot; in SMC</td>
<td>Installed Client (Secure)⁷ FEP (Secure)⁷ Remote System (Non secure)¹¹</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>UDP: 5678</td>
<td></td>
<td>(SSL encrypted)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query Cache Manager WCCOQueryCache.exe²</td>
<td>TCP: 4779</td>
<td>SMC</td>
<td>WinCC OA Communication</td>
<td>Exposed if Query Cache Manager is activated for a project and project is set to &quot;Nonsecure&quot; (in SMC)</td>
<td>Installed Client (Non secure)⁷ FEP (Nonsecure)⁷</td>
<td>n/a</td>
</tr>
<tr>
<td>SMC ProjectData Service Siemens.Gms.Smc.WCFWindowsServiceHost.exe²</td>
<td>TCP: 8888</td>
<td>SMC</td>
<td>HTTP – WCF Service</td>
<td>always exposed</td>
<td>Installed Client (Secure)⁵ FEP (Secure)⁵ FEP (Nonsecure)⁵</td>
<td>2.2.2 [➙ 44] 2.2.4 [➙ 51] 2.2.5 [➙ 56]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Monitoring Service GMS_WCCILpmon_[ProjectName].exe¹</td>
<td>TCP: 4999</td>
<td>SMC</td>
<td>http / pmon protocol</td>
<td>never exposed</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Only used for communica</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>tion of component on the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>local machine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>TCP: 80</td>
<td>SMC</td>
<td>HTTP</td>
<td>always exposed</td>
<td>Remote Client Web Client</td>
<td>2.2.1 [➙ 40] 2.2.3 [➙ 47] 2.2.5 [➙ 56] 2.2.6 [➙ 58] 2.2.7 [➙ 59]</td>
</tr>
<tr>
<td>Component, Executable</td>
<td>Default Port</td>
<td>Port Config.</td>
<td>Protocol</td>
<td>Port exposure to other machines in the network</td>
<td>Connects to this port</td>
<td>Refer to</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>----------</td>
<td>------------------------------------------------</td>
<td>-----------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| Microsoft IIS                                | TCP: 443     | SMC          | HTTPS    | always exposed                                  | Remote Client Web Client | 2.2.1 [➙ 40]  
2.2.3 [➙ 47]  
2.2.5 [➙ 56]  
2.2.6 [➙ 58]  
2.2.7 [➙ 59] |
| MS SQL Server Browser                        | UDP: 1434    | SQL Server   |          | depends on SQL Server configuration Default: exposed |                       | 2.2.6 [➙ 58] |
| MS SQL Server DB instance (HDB)               | TCP: variable | SQL Server   |          | depends on SQL Server configuration Default: exposed |                       | 2.2.6 [➙ 58] |
| File and Printer Sharing (NetBIOS Session Service connections) | TCP: 139   | n/a          | TCP      | Installed Client (Secure)  
Installed Client (Non secure)  
FEP (Secure)  
FEP (Nonsecure)  
Separate Web Server  
Remote System (Secure)  
Remote System (Non secure) |                       | 2.2.2 [➙ 44]  
2.2.3 [➙ 47]  
2.2.4 [➙ 51]  
2.2.5 [➙ 56]  
2.2.6 [➙ 58]  
2.2.7 [➙ 59] |
## Network Security Controls
### Protected System Configuration Concept

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component, Executable</strong></td>
<td><strong>Default Port Config.</strong></td>
<td><strong>Port exposure to other machines in the network</strong></td>
</tr>
<tr>
<td>File and Printer Sharing (Server Message Block transmission and reception via Named Pipes)</td>
<td>TCP: 445</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- The port must be configured in the firewall of the main server for inbound communication if the host is protected by a firewall.
## Deployment Variants: Remote IIS and Remote SQL Server

<table>
<thead>
<tr>
<th>Providing Component</th>
<th>Remote Consumer</th>
<th>Default Port</th>
<th>Port Config.</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft IIS on separate Web Server</strong></td>
<td>Remote Client Web Client</td>
<td>TCP: 80</td>
<td>SMC or IIS</td>
<td>HTTP</td>
</tr>
<tr>
<td><strong>Microsoft IIS on separate Web Server</strong></td>
<td>Remote Client Web Client</td>
<td>TCP: 443</td>
<td>SMC or IIS</td>
<td>HTTPS</td>
</tr>
<tr>
<td><strong>MS SQL Server Browser</strong> sqlbrowser.exe</td>
<td>Main Server(1)</td>
<td>UDP: 1434</td>
<td>SQL Server</td>
<td></td>
</tr>
<tr>
<td><strong>MS SQL Server DB instance (HDB)</strong> sqlserver.exe</td>
<td>Main Server(1)</td>
<td>TCP: variable(3)</td>
<td>SQL Server</td>
<td></td>
</tr>
</tbody>
</table>

### Core Services on FEP

<table>
<thead>
<tr>
<th>Providing component</th>
<th>Default Port</th>
<th>Port Config.</th>
<th>Protocol</th>
<th>Port Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PMON service</strong></td>
<td>TCP: 4999</td>
<td>SMC</td>
<td>http / pmon</td>
<td>Remote Client Web Client</td>
</tr>
</tbody>
</table>

**NOTE:** Only used for communication between components on the local machine.
## Optional Services on the Main Server

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Service Interface WCCOAWsi.exe</td>
<td>TCP: 8080</td>
<td>SMC</td>
<td>HTTP(S) – REST Web Service</td>
<td>always exposed</td>
<td>Separate Web Server</td>
</tr>
<tr>
<td>OPC DA</td>
<td>TCP: 135</td>
<td></td>
<td>RPC End Point Mapping</td>
<td></td>
<td>3rd Party OPC Client Outside Main Server</td>
</tr>
<tr>
<td>OPC UA: Local Discovery Server Siemens.Gms.OPCServer.exe</td>
<td>TCP: 4840</td>
<td></td>
<td>OPC/TCP</td>
<td></td>
<td>3rd Party OPC Client Outside Main Server</td>
</tr>
<tr>
<td>OPC UA: Local Discovery Server Siemens.Gms.OPCServer.exe</td>
<td>TCP: 4883</td>
<td></td>
<td>HTTPS</td>
<td></td>
<td>3rd Party OPC Client Outside Main Server</td>
</tr>
<tr>
<td>OPC UA: Local Discovery Server Siemens.Gms.OPCServer.exe</td>
<td>TCP: 52601</td>
<td></td>
<td>HTTP</td>
<td></td>
<td>3rd Party OPC Client Outside Main Server</td>
</tr>
<tr>
<td>OPC UA: UA Wrapper Siemens.Gms.OPCServer.exe</td>
<td>TCP: 48400</td>
<td></td>
<td>OPC/TCP</td>
<td></td>
<td>3rd Party OPC Client Outside Main Server</td>
</tr>
<tr>
<td>OPC UA: UA Wrapper Siemens.Gms.OPCServer.exe</td>
<td>TCP: 48401</td>
<td></td>
<td>HTTP</td>
<td></td>
<td>3rd Party OPC Client Outside Main Server</td>
</tr>
<tr>
<td>Desigo CC and Surveillance/Milestone recording servers WCCOAWsi.exe</td>
<td>TCP: 7563</td>
<td></td>
<td>WCF – TCP – HTTP web services (NTLM) – Active X</td>
<td>always exposed</td>
<td>Separate Web Server</td>
</tr>
<tr>
<td>XNET fire control panels (FireFinder XLS/MXL, Desigo Fire Safety Modular, and Cerberus Pro Modular)</td>
<td>TCP: 2000</td>
<td></td>
<td>TCP[16]</td>
<td></td>
<td>Separate Web Server</td>
</tr>
</tbody>
</table>
Directories of the host processes:
1) Located in C:/Siemens/Automation/WinCC_OA/3.15/bin/
2) Located in [Installation Directory]/GMSMainProject/bin/

Variable ports:
3) The port of an SQL server named instance is by default variable; Refer to SQL server documentation on how to configure a fixed port for a named instance.

Consumer:
5) SMC
6) Executables on the client installation
   [Installation Directory]/GMSMainProject/bin/Siemens.Gms.ApplicationFramework.exe
   C:/Siemens/Automation/WinCC_OA/3.15/bin/WCCOActrl.exe
7) Executables on the client installation
   [Installation Directory]/GMSMainProject/bin/Siemens.Gms.ApplicationFramework.exe
8) Executables on the FEP installation opening outbound connections
   [Installation Directory]/GMSMainProject/bin/Siemens.Gms.ApplicationFramework.exe
   C:/Siemens/Automation/WinCC_OA/3.15/bin/WCCOActrl.exe
   Additional executables on the FEP depend on the driver type. For example, BACnet: [Installation Directory]/GMSMainProject/bin/WCCOAGmsBACnet.exe
   SNMP: C:/Siemens/Automation/WinCC_OA/3.15/bin/WCCOAsnmp.exe
9) Microsoft IIS
10) [Installation Directory]/GMSMainProject/bin/WCCOAHDBReader.exe
    [Installation Directory]/GMSMainProject/bin/WCCOAHDBWriter.exe
    [Installation Directory]/GMSMainProject/bin/WCCOAReportMan.exe
11) [Installation Directory]/GMSMainProject/bin/WCCOACoHoMngr.exe
12) C:/Siemens/Automation/WinCC_OA/3.15/bin/WCCILdist.exe
13) FlexC; TCP default port 52000; configurable; encrypted.
14) EDP – TCP (for import); default port 52000; encrypted; custom protocol.
15) EDP – UDP (From Version 3.3, only project upgrade), default port 52000; custom protocol.
16) Default port 1977; custom protocol.
### Subsystem Connectivity

Outbound connections (ports used by the host to connect to automation systems)

<table>
<thead>
<tr>
<th>Field</th>
<th>System</th>
<th>Hosts</th>
<th>Component / Process</th>
<th>Port</th>
<th>Port Configuration</th>
<th>Comment</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>APOGEE</td>
<td>P2</td>
<td>Main Server, FEP</td>
<td>APOGEE P2 driver</td>
<td>TCP: 3001</td>
<td>APOGEE Network SnapIn</td>
<td>Required for APOGEE Ethernet Microserver (AEM)</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAapogee Drv.exe</td>
<td>UDP: 3001</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APOGEE</td>
<td>P2</td>
<td>Main Server, FEP</td>
<td>APOGEE P2 driver</td>
<td>TCP: 5033</td>
<td>APOGEE Network SnapIn</td>
<td>Required for APOGEE Ethernet networks</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAapogee Drv.exe</td>
<td>UDP: 5033</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APOGEE</td>
<td>P2</td>
<td>Main Server, FEP</td>
<td>APOGEE P2 driver</td>
<td>TCP: 5441</td>
<td>No</td>
<td>Required for APOGEE Ethernet networks (diagnostic channel)</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAapogee Drv.exe</td>
<td>UDP: 5441</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BACnet</td>
<td></td>
<td>Main Server, FEP</td>
<td>BACnet Driver</td>
<td>UDP: 47808</td>
<td>BACnet SnapIn</td>
<td>Communication with BACnet field systems (APOGEE BACnet, Desigo PX, Desigo TRA, FS20)</td>
<td>BACnet/IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAgmsBACnet.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus</td>
<td></td>
<td>Main Server, FEP</td>
<td>Modbus Driver</td>
<td>TCP: 502</td>
<td>Modbus SnapIn</td>
<td>Communication with Modbus TCP devices</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAmod.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPC</td>
<td></td>
<td>Main Server</td>
<td>OPC Driver</td>
<td>TCP: 135</td>
<td>No</td>
<td></td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAopc.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPC</td>
<td></td>
<td>Main Server</td>
<td>OPC Driver</td>
<td>TCP: variable</td>
<td>Windows Registry</td>
<td></td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAopc.exe</td>
<td></td>
<td>variable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simatic</td>
<td>S7</td>
<td>Main Server, FEP</td>
<td>Simatic S7 Driver</td>
<td>TCP: 102</td>
<td>No</td>
<td>Communication with S7 PLC (also for Siclimat-S7 devices)</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAs7.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
<td>Main Server, FEP</td>
<td>SNMP Driver</td>
<td>UDP: 161</td>
<td>SNMP Network</td>
<td></td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAsmtp.exe</td>
<td></td>
<td>Configuration SnapIn</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPC</td>
<td></td>
<td>Main Server, FEP</td>
<td>SPC Driver</td>
<td>TCP: 50000</td>
<td>SPC Driver SnapIn</td>
<td></td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WCCOAsPC.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XNET</td>
<td></td>
<td>Main Server, FEP</td>
<td>XNET Driver</td>
<td>TCP: 1977</td>
<td>XNET Driver SnapIn</td>
<td></td>
<td>TCP/UDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NCCGMS.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1) Required for APOGEE Ethernet Microserver (AEM)
2) Required for APOGEE Ethernet networks
3) Communication with Modbus TCP devices
4) Communication with S7 PLC (also for Siclimat-S7 devices)
5) No
A Modbus subsystem uses the underlying Modbus Driver from WinCC OA. It uses Modbus protocol over TCP. During import, the field engineer has to specify the IP Address and the port number for communicating with the device. If the port number field is left empty, then the Modbus Importer applies the default value: 502. However, after the import, the user can modify both IP address and port number from the Desigo CC client.

The default port for the first BACnet driver is UDP: 47808. The port can be changed. Every additional driver needs another UDP port.

The default port for the first SNMP network is UDP: 161. The port can be changed. Every additional network needs another UDP port.

4 ports for OPC client/server communication; default variable range: 1024...5000 (settable through registry key HKEY_LOCAL_MACHINE/Software/Microsoft/Rpc/Internet)

Remote Notification
Outbound connections (ports used by the host to connect to remote notification systems)

<table>
<thead>
<tr>
<th>Hosts</th>
<th>Component / Process</th>
<th>Port Configuration</th>
<th>Comment</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Server</td>
<td>ESPA driver WCCOAGmsCoHoMngr.exe</td>
<td>variable</td>
<td>RENO SnapIn (Pager)</td>
<td>Communication with ESPA Pager modem</td>
</tr>
<tr>
<td>Main Server</td>
<td>GSM driver WCCOActrl.exe</td>
<td>variable</td>
<td>RENO SnapIn (SMS)</td>
<td>Communication with GSM modem</td>
</tr>
<tr>
<td>Main Server</td>
<td>Mail WCCOActrl.exe</td>
<td>TCP: 25, 110, 143</td>
<td>RENO SnapIn (Mail)</td>
<td>Communication with mail servers. It can be unsecure or secured with SSL or TLS protocols.</td>
</tr>
<tr>
<td>Main Server</td>
<td>TAP driver Siemens.Gms.RENO.TAPDevMogr.exe</td>
<td>variable</td>
<td>RENO SnapIn (Pager)</td>
<td>Communication with TAP Pager modem</td>
</tr>
</tbody>
</table>

Remote Notification
Outbound connections (ports used by the host to connect to remote notification systems)

<table>
<thead>
<tr>
<th>Hosts</th>
<th>Component / Process</th>
<th>Port Configuration</th>
<th>Comment</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Server</td>
<td>ESPA driver WCCOAGmsCoHoMngr.exe</td>
<td>variable</td>
<td>RENO SnapIn (Pager)</td>
<td>Communication with ESPA Pager modem</td>
</tr>
<tr>
<td>Main Server</td>
<td>GSM driver WCCOActrl.exe</td>
<td>variable</td>
<td>RENO SnapIn (SMS)</td>
<td>Communication with GSM modem</td>
</tr>
<tr>
<td>Main Server</td>
<td>Mail WCCOActrl.exe</td>
<td>TCP: 25, 110, 143</td>
<td>RENO SnapIn (Mail)</td>
<td>Communication with mail servers. It can be unsecure or secured with SSL or TLS protocols.</td>
</tr>
<tr>
<td>Main Server</td>
<td>TAP driver Siemens.Gms.RENO.TAPDevMogr.exe</td>
<td>variable</td>
<td>RENO SnapIn (Pager)</td>
<td>Communication with TAP Pager modem</td>
</tr>
</tbody>
</table>

2.1.4 Least Functionality Implementation
Ensure that no ports apart from those specified in the firewall rules are open. Also, make sure that no services other than those strictly required for full system functionality are running during normal system operation.
2.2 Intended Operational Environments

2.2.1 All-In-One (One-Seat) System

Intended Use Case
This is the configuration choice in all cases where only one client is required, and system size is limited. The Desigo CC server, database service and one installed client are deployed on the same hardware platform, which can be physical or virtual. The field networks are connected directly to the Desigo CC server.

Figure 4: One-Seat System
Stand-alone System without a Local Web Server (IIS)

The following describes a stand-alone configuration, where the Desigo CC server and the Desigo CC installed client are located on a single computer. In this scenario, web clients or Windows App clients are not involved.

**What is a Stand-alone System?**

A single dedicated workstation that runs both the Desigo CC server and the Desigo CC client application, typically communicating with a field system in a networked environment. It includes the following features:

- Own administration
- Microsoft SQL Server installed locally
- IPv4
- No IT firewalls in between Desigo CC components (since there are no remote clients, firewalls do not need to be opened for communication)

**Security**

- Simple setup (certificate configuration not required).
- Effort for security configuration is low.
- A stand-alone system is secure in regard to attacks from the outside. However, installation guidelines for closing outside communication by firewall settings, virus scanner, and backup must be followed to secure the system.
Settings Reference
For reference, see Restoring a Project or Creating a Project from a Template in the Desigo CC online help.

Stand-Alone System with a Local Web Server (IIS)
The following describes a typical deployment scenario for setting up a Desigo CC system with a local web server (IIS) on a single computer.

What is a Local Web Server?
The web client and Windows App client options require installing an optional web server component (IIS). When the web server (IIS) is installed on the same computer as the Desigo CC server, it is called the local web server (IIS).

What is a Stand-alone System with a Local Web Server?
A local web server is a single dedicated workstation with the following features:

- Desigo CC server
- Web server (IIS)
- Own administration
- Microsoft SQL Server installed
- Accessed by means of web client and Windows App client
- Intranet, own network segment
- IPv4
- No IT firewalls (to other network segments or to the Internet)

Security
- Simple setup
- Effort for security configuration is medium
- A stand-alone system with a local web server must be protected against attacks from other machines in the network. Follow the configuration guidelines to limit outside communication by firewall settings, virus scanner, and so forth to secure the system.
Certificate Usage on a Stand-alone System with a Local Web Server
This section describes how to configure the web server using the same certificate for both the website and the web application.

- No certificate is required for the communication between the Desigo CC server and the installed client or FEP since there is no FEP and no remote installed client in this deployment.
- The communication between the Desigo CC server and the local web server (IIS) can be left unsecured (without certificates), since they are both installed on the same machine.
- The communication between the web server and web/Windows App clients shall always be secured. Hence, the website and the web application creation certificates are mandatory. Desigo CC supports the use of either the same or different certificates for the website and the web application. Usage of TLS 1.2 is suggested whenever possible.
- The certificate and its private key must be imported into the Windows certificate store (in the Local machine\Personal store; its root certificate must be imported in the Local machine\Trusted Root Certification Authorities (TRCA) store). The private key must be marked as exportable.

**NOTICE**

Validity of Self-Signed Certificates
Self-signed certificates allow local deployments without the overhead of obtaining commercial certificates. When using self-signed certificates, the owner of the Desigo CC system is responsible for maintaining their validity status, and for manually adding them to and removing them from the list of trusted certificates.
Self-signed certificates must only be used in accordance with local IT regulations (several CIO organizations do not allow them, and network scans will identify them). Importing the commercial certificates follows the same procedures.
You must ensure the compliant installation of the trusted material on the involved machines, for example, on all installed clients. In some organizations, this must be done by the IT department.
2.2.2 Client/Server in the Customer Network

Intended Use Case
This is the configuration choice for the cases where multiple installed clients, connected through a dedicated or shared local area network (LAN) are required. Web connectivity is not required. Communication between the key components can be secured by standard IT security mechanisms like certificates.

Figure 7: Stand-alone System with a Local Web Server

Settings Reference
For reference, see Setting up the Web/Windows App Clients in the Desigo CC online help.
The Desigo CC server, database service and the first installed client are deployed on the same hardware platform, which can be physical or virtual. If Windows App clients are required, the web server can also be installed on the same platform. Field networks are connected directly to the Desigo CC server.

FEP can be used to better balance the communication load or to better adapt to the distribution of the field systems. A typical case for FEP usage would be a system with multiple remote sites and one central control location. Installed and Windows App clients are connected to the server by system LAN. The size of the field system and the number of clients that can be supported by this configuration depend on the server hardware configuration.
Client/Server
Each Desigo CC installation has only one server; but it can have multiple clients, running on different computers. You can work with Desigo CC in configuration where a Desigo CC server communicates with multiple Desigo CC clients installed on separate computers. This allows multiple operators to manage and supervise the same site. The communication between the client and the server must be set up using SMC. First, you must set up the server and then the client station. The communication should be secured using certificates (this might be simplified on dedicated and protected networks, such as within a control room).
By default, the template project is created for a stand-alone configuration (with the indication that no communication is possible). To set up a secured/unsecured client/server system, you must edit the project.

Server Station
A dedicated workstation with the following features:
- Desigo CC server
- Own administration
- Microsoft SQL Server installed/remote customer Microsoft SQL Server
- Own network segment
- IPv4/IPv6
- IT firewalls must allow communication between server and client

Client Station
A dedicated workstation with the following features:
- Desigo CC client/FEP
- Own administration
- IPv4/IPv6
- Internal firewalls

Security
- Secure client/server deployments require medium configuration setup.

Certificate Usage
This scenario explains setting up a secured client/server communication using certificates from the Windows store.
For a client/server deployment, the following restrictions apply with respect to certificates:
- The root certificate validates the certificates used for communication. Therefore, it must be the same for all host certificates and it must be installed on the server and on all clients.
- The root and communication (host) certificates must be different and have different subject names.
- The communication certificates should be specific. Therefore, it is recommended to use different host certificates for client and server.
- The communication certificates are used by the Desigo CC client/FEP. Therefore, the logged on user of the client/FEP operating system requires access to the private key of the host certificate stored in the Windows Certificate store.

The owner of the Desigo CC system is responsible for distributing authorized certificates and keys. This is often done by the IT infrastructure, particularly, if commercial certificates are used instead of the self-signed ones.
Network Security Controls
Intended Operational Environments

Deployment Diagram

1. Root Certificate (.cer) file
2. Client/FEP Host Certificate (.pfx) file

Client/Server Communication Mode = Secured

Client/FEP with Installed Client

Management System Server with Installed Client, Microsoft SQL Server

– Root Certificate (.cer file) in TRCA
– Server Host Certificate (.pfx file) in Personal
– Client/FEP Host Certificate (.pfx + .cer files)

Note that the meaning of TRCA and Personal Store is explained in Technical Terms and Abbreviations [➙ 6].

Settings Reference
For reference, see Setting up the Installed Client in the Desigo CC online help.
2.2.3 Server and Remote Web Server (IIS)

Intended Use Case
This section describes a typical deployment scenario for setting up a Desigo CC system with the web server (IIS) installed on a separate computer.

Figure 11: Server and Remote Web Server
Figure 12: Server and Remote Web Server
Server Station
A single dedicated workstation with the following features:
- Desigo CC server is installed.
- Microsoft SQL Server is installed on the Desigo CC server.
- The server project folder is shared.
- The required certificates (SMC-created or commercial) are imported into the Windows Certificate store:
  - The root certificate is imported into the Trusted Root Certification Authorities store.
  - The host certificate and its private key are imported into the Personal store.
- The host certificate used must have a private key; no private key is needed for a root certificate.

Remote Web Server (IIS) Station
This chapter describes how to configure the web server to use the same certificate for both the website and the web application.
- The web client and Windows App client options require installing an optional web server (IIS) component. When the web server (IIS) is installed on a separate computer it is known as the remote web server (IIS).
- A remote web server (IIS) hosts websites and web applications. To simplify the website configuration using SMC, it is recommended that you also install the Desigo CC client (or FEP) component on this machine.
- The web application user on this remote web server has access rights on the shared project folder on the server.
- The required certificates (SMC-created or commercial) are imported into the Windows Certificate store:
  - The root certificate of the host certificate provided for CCom port security is imported into the Trusted Root Certification Authorities store.
  - The communication between the web server and the web/Windows App clients is always secured. Hence, the website and the web application creation certificates are mandatory. Desigo CC supports using either the same or different certificates for the website and the web application.
- When a commercial certificate is used for creating a website and web application, then ensure the following:
  - The commercial self-signed certificate must be imported into the Trusted Root Certification Authorities and Personal stores of the Local machine store.
  - The commercial host certificate, along with its private key, must be imported into the Personal store and its root certificate must be imported into the Trusted Root Certification Authorities store of the Local machine store.
- You can also configure a remote web server (IIS) as an installed client/FEP. This will allow you to perform the client/server deployment scenario. For more information, see the client/server deployment scenarios in the following section.

Security
- Secure server/remote web server (IIS) deployments require medium security configuration setup.
- The component in the DMZ are exposed to the internet, therefore it is important to keep them up to date to the latest security patches.
**2.2.4 Client/Server with Internet Access**

**Intended Use Case**
This is the configuration choice for the cases where multiple installed clients, connected through a dedicated or shared LAN are required, but web connectivity is also required to allow remote access through a Desigo CC web client or provide remote connectivity to an external application through the web services.

The Desigo CC server, history database service, web server and the first installed client are deployed on the same hardware platform, which can be physical or virtual.

Field networks are connected directly to the Desigo CC server.

FEP can be used to better balance the communication load or to better adapt to the distribution of the field systems. A typical case for FEP usage would be a system with multiple remote sites and one central control location.

Installed and remote Windows App clients are connected through the system LAN to the server.

The size of the field system and the number of clients that can be supported by this configuration depend on the server hardware configuration.

For systems with Internet access additional support for networks and IT security is available:
- Support of Windows domains and Active Directory
- Support of network policies
- Firewall/DMZ support
For systems with key components in the Internet additional network and IT security measures are required to run Desigo CC properly:

- Only web and Windows App clients are hosted outside the customer network.
- Communication between all key components is required to be secured by standard IT security mechanisms, like virtual private network (VPN) and/or certificates.
- Communication to components in the Internet must be secured by customer or trust center-provided certificates, and must be separated from the customer network by professional hardware firewalls/DMZ.
- Log on to Desigo CC in the Internet only with users of the customer Active Directory
- Field systems must be separated from Internet access.
Figure 15: Intranet-Extranet
Server and a Remote Web Server (IIS) in a DMZ Network

A DMZ (demilitarized zone) refers to an area of a network, usually between two firewalls, where users from the Internet are permitted limited access over a defined set of network ports and to predefined servers or hosts. A DMZ is used as a boundary between the Internet and your company’s internal network. The network DMZ is the only place on a corporate network where Internet users and internal users are allowed at the same time.

In a DMZ setup, the web server (IIS) and the Desigo CC server are hosted on separate machines that are on different networks, separated by firewalls.

In such a scenario, commercial SSL certificates are typically used for the website on IIS. For verifying the signature of the web client/Windows App client, the same certificate or a separate commercial or self-signed certificate, may be used. However, you can use the same certificate if the private key used to secure the web site is exportable.

The following section describes a typical deployment scenario for setting up a Desigo CC system with a remote web server (IIS) in a DMZ scenario.

Server Station

A single dedicated workstation with the following features:

- Desigo CC server is installed.
- Microsoft SQL Server is installed on the Desigo CC server.
- The server project folder is shared.
- The required certificates are imported into the Windows Certificate store:
  - The root certificate is imported into the Trusted Root Certification Authorities store.
  - The host certificate is imported into the Personal store.
- The host certificate used must have a private key; no private key is needed for a root certificate.

Remote Web Server (IIS) Station in a DMZ

This section describes how to configure the web server to use the same certificate for both the web site and the web application.

- A dedicated workstation serving as web server for hosting the website/application. To simplify the website configuration, it is recommended that you install the Desigo CC client or FEP software on this machine.
- The web application user on the remote web server has access rights on the shared project folder on the server.
- The required certificates are imported into the Windows Certificate store:
  - The root certificate of the host certificate provided for CCom port security is imported into the Trusted Root Certification Authorities store.
  - The communication between the web server and the web/Windows App clients is always secured. Therefore, creating the website and the web application certificates is mandatory. Desigo CC supports using either the same or different certificates for the website and the web application.
  - The certificate and its private key must be imported into the Windows certificate store (in the Local Machine\Personal store; its root certificate must be imported into the Local Machine\Trusted Root Certification Authorities (TRCA) store). The private key must be marked to be exportable.
  - If different commercial certificates are used for creating the website and web application, then both must be present in the Trusted Root Certification Authorities store and the Personal store of the Windows Certificate store.
**Security**
- Secure server/remote web server (IIS) deployments require high security configuration setup.
- The components in the DMZ are exposed to internet, therefore it is important to keep them up to date to the latest security patches.

**Deployment Diagram**

*Figure 16: Remote Web Server in a DMZ Scenario*

**Settings Reference**
For reference, see *Setting up a Server and a Remote Web Server (IIS) in a DMZ Network* in the Desigo CC online help.
2.2.5 Large, Distributed Client/Server with Internet Access

Intended Use Case

This is the configuration choice for cases where system size or specific customer indications require the deployment of key Desigo CC components on different hardware platforms, which can be physical or virtual.

Communication between the key components is required to be secured by standard IT security mechanisms like certificates. Communication to components in the Internet must be secured by customer or trust center provided certificates and protected by professional hardware firewalls/DMZ.

Field networks are connected to the Desigo CC server. When appropriate, FEP can be used.

The size of the field system and the number of clients that can be supported by this configuration depend on the server hardware configuration.

For systems with Internet access additional support for networks and IT security is available:

- Support of Windows domains and Active Directory
- Support of network policies
- Firewall/DMZ support

For systems with key components in the Internet additional network and IT security measures are required to run Desigo CC properly:

- Only web and Windows App clients are hosted outside the customer network.
- Communication between all key components is required to be secured by standard IT security mechanisms, like virtual private network (VPN) and/or certificates.
- Communication to components in the Internet must be secured by customer or trust center-provided certificates, and must be separated from the customer network by professional hardware firewalls/DMZ.
- Log on to Desigo CC in the Internet only with users of the customer Active Directory
- Field systems must be separated from Internet access.

Figure 17: Large, Distributed Client/Server with Internet Access
Figure 18: Large, Distributed Client/Server
2.2.6 Distributed System Configurations

Intended Use Case
The distributed system configuration allows interconnecting several projects that run independently, either on one or several physical machines. The interconnection of the projects allows transparent engineering and operation through them seeing them as one and only one system. The distributed system configurations extend even further the support of very large systems, increase robustness eliminating single point of failures and allow geographical or discipline segregation.

Three types of distributed deployments are supported:

- Fully meshed: Each server is logically connected to all others. Clients can see all objects in all servers. Servers can be geographically distributed. Virtual servers are also supported.
- Segmented: A fully meshed configuration where all systems run on the same server. Allows building larger systems on one single server.
- Hierarchical: front servers are logically connected to one head server. Clients connected to the head server can see all objects; clients connected to front servers can only see local objects. For campus or inherently hierarchical applications.

Figure 19: Distributed System Configurations
2.2.7 Virtualization

Intended Use Case
Virtualization has become a widely preferred and suggested environment for IT infrastructure by IT administrators:

- Server (hardware) virtualization is a proven software technology that makes it possible to run multiple operating systems on the same server at the same time, sharing the available hardware resources. It simulates the available hardware and deludes every operating system running on top of it to assume that it is the unique holder of the resource. The details of the physical environment are kept transparent from the operating system.

- Add-on options for hardware redundancy allow running the same virtual machine on multiple physical servers. If a server fails for any reason, another physical server running the same virtual machine can take its place. This minimizes any interruption in service.

- Network virtualization creates logical, virtual networks that are decoupled from the underlying network hardware to ensure the network can better integrate with and support increasingly virtual environments.

- Further virtualization types are desktop-, application- and service virtualization. Virtualization of clients is not recommended. Depending on the virtualization software, performance issues (such as, display of multiple video streams or graphic display) may occur.

Desigo CC supports several server virtualization environments and their redundancy options, including transparent network virtualization. Terminal Server applications, Desktop-, Service-, and Application Virtualization are not supported.

The following key components can be virtualized:
- Desigo CC Server
- Video Management Service
- Microsoft SQL Server
- Microsoft IIS Server
- Desigo CC FEP
3 Cybersecurity Concepts – How to Secure the System

Protection against Casual or Coincidental Violation
Desigo CC complies with the ISA-99/IEC 62443 Security Level: SL1 as long as the recommendations described in this document are implemented in full.

Security Categories
Security in Desigo CC is divided into the following categories:

- Protection
  Protection of Desigo CC against unauthorized and malicious use. This includes provision of secure communication that prevents any manipulation of messages as well as validation of users (authentication) to block unknown users from accessing the system.

- Authorization
  Provision of a fine-grained but easy-to-configure authorization model. It provides access to any system resource and functionality in a way that the access rights of users correspond with their capabilities, such as acting as system administrator or personnel manager and the current operating conditions, such as organization mode and/or the user location.

The features related to Protection can be summarized as follows:

- All communication paths between clients and the server provide encryption and protect against replay attacks as well as data manipulation. The communication between the web server (IIS) and the web clients is always encrypted.
- Communications between the system server and a FEP can be encrypted by Desigo CC.
- Communications between the system server and SQL Server can be encrypted by Desigo CC.
- The runtime data transfer between the system server and IIS can be encrypted by Desigo CC.
- Passwords are handled securely:
  - Encrypted storage and transmission
- Use of public domain algorithms for cryptographic functions, including:
  - AES, DiffieHellmann, RSA, SHA-2, and so on.
  - No self-coded algorithms
- Key strengths are defined as general security baselines, for example:
  - Symmetrical encryption uses 256 bit AES or stronger
  - Asymmetrical encryption uses 2048 bit or stronger

The features related to Authorization can be summarized as follows:

- The Authorization Model allows controlling access, view, and commanding privileges of users and user groups on a very granular level based on resources/groups. These resources/groups can be workstations, features, applications, system objects, system object properties, and logical groups of any kind for these resources.
- Access to the system is treated intuitively – the UI displays only elements such as menus, buttons, list items, tree nodes, and so on where the user has at least read access.
3.1 User Management

User Account Management

**NOTICE**

Desigo CC users can be configured to use local passwords or to use Windows authentication (for example, Active Directory). Use Windows authentication wherever possible to enhance security, control, and management of passwords.

General security guidelines for Desigo CC user account management (Windows OS):

- Use nominative accounts (do not use generic group accounts that are used by multiple persons)
- Rename the default administrator account
- Use strong passwords (for example, 12 characters including upper case, lower case, special characters, and numbers)
- Change passwords on a regular basis, especially passwords for administrator accounts and the password of the service account (root)
- If accounts are created by default or from a template, use different passwords for each installation
- Do not use the same password for the default administrator account and the service account
- Make sure there is a process in place to disable and then remove (above desired logs’ retention time) old/unused user accounts
- Auto-logon features skip the identification of a user and should therefore only be used either in controlled environments, where the effective user can be determined differently, or for users that are only authorized to see non-Unrestricted data

**User Authorization Configuration**

User access rights in Desigo CC are determined by four main factors:

- The system must know the user (authentication)
- The user must be assigned a user group
- The user group has the appropriate application rights
- The user group must have the appropriate scope rights

If all of these conditions are met, the user can log on to Desigo CC and read/write objects and execute tasks, depending on the assigned rights.

For detailed information on how to configure user authorization (users, user groups, application rights, scope rights), see sections *User and User Group Administration* and *Scopes* in the Desigo CC online help.
3.2 IT Security

**NOTICE**

The owner of the Desigo CC system is responsible for establishing and maintaining appropriate IT security, in particular by applying virus scanners, deactivating unneeded services and network ports, and by regular patching and updating the operating system and all installed applications.

3.3 Communication Security

The communication between web clients and the web server (IIS) is always encrypted. The runtime data transfer between a FEP and the system server, between the system server and a web server, and between the system server and installed clients may be encrypted as an option.

The file transfer between the system server and installed clients and between the system server and a web server is unencrypted for performance reasons.

The communication between the system server and the History Database is unencrypted for performance reasons.

Sensitive data (such as, passwords during authentication or user management configuration) is transferred as encrypted content between the Desigo CC clients and the system server (regardless of the communication encryption).

Self-signed certificates are supported to allow local deployments without the overhead of obtaining commercial certificates. When using self-signed certificates, the owner of the Desigo CC system is responsible for maintaining their validity status, and for manually adding them to and removing them from the list of trusted certificates.

Self-signed certificates may only be used in accordance with local IT regulations (some CIO organizations do not allow them, and network scans will identify them). Importing of commercial certificates follows the same procedures.

**Wireless input devices** (especially keyboards) use radio transmission that is often not or inadequately cryptographically protected. Even from greater distances, it is possible to listen in or even plant external data into the system. The use of wireless input devices should be avoided when used in high security environments. If the use of wireless input devices is absolutely necessary, use only devices with proven encryption.

With version 4.0, the Bluetooth (BT) standard includes an encryption mechanism (AES128). In order to be effective, all devices must use BT 4.0. Users should also observe the information provided by the manufacturer.
3.4 **License Security**

Licensing is important to guarantee the operation of the system within the agreed system limits. Only the system is allowed to change license data.

If a license becomes temporarily unavailable (for example, dongle unplug) the system continues running fully operational for a demo period of 30 minutes. The system continues to check for the license and shuts down at the end of the demo period, if the license checks are unsuccessful.

Exceeding the limits of the license (for example, by integrating more field system data points than stated in the license), puts the system into Courtesy mode. Phases of Courtesy mode accumulate until a total duration of 30 days is exceeded, then the server shuts down. Unless new licenses are purchased and activated, after a manual restart the system returns into Courtesy-mode strike exceeding and shuts down.

Any unauthorized attempt to modify system license data directly in the database (for example, change of the remaining time of a specific license mode) shuts down the system.

3.5 **Stored Data Security**

Data is generally stored unencrypted in Desigo CC. Exceptions are sensitive data such as passwords for accessing Desigo CC (hashed) or passwords required by Desigo CC to access field system devices (encrypted).

**Project Data**

Runtime data (process image) and engineering data is stored in a file-based database in a subdirectory of the project directory. Data is unencrypted and database access can only be prevented by restricting access to the database files. The project directory must be shared when deploying installed clients. It is hence important to restrict access to the DB folder in the project directory to the Windows account running the Desigo CC server.

**Database (HDB)**

Historical data is stored in an access-controlled Microsoft SQL Server database. This database should be outside the project folder to allow for independent handling and backup of project data and historical data. It is recommended to encrypt the connection to the History Database when using a remote Microsoft SQL Server.

**Backups of Project or History Database**

Backups of the system or archives from the History Database are not encrypted and can get restored on any system. Therefore, it is important to store backups in secure locations and encrypt if necessary (different passwords should be used for different sites).

3.6 **Main Server Folder Shares for Client and FEP Installations**

When installing additional installed clients for Desigo CC version 4.x, FEPs or a remote web server, the project directory is no longer shared, with the only exception of the individual folders that need to be accessed remotely. Access to the shares typically is configured using SMC (the engineer only needs to assign the user accounts/groups; SMC takes care of setting the access rights).
The local client and the web server on the Desigo CC server do not need file sharing; only access rights to the folders in the project directory must be configured. Below you can find a description of what can be actually configured.

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avoid Exposed Network Shares</strong></td>
</tr>
<tr>
<td>Since exposed network shares could be used to illicitly discover Unrestricted information from the network, avoid unrestricted use as much as possible. For example, only to the users and the computer that need access. In Desigo CC, shares are only needed for installed clients and the web server (unless they are on the same machine), not for the Windows App and web clients. Since these should be reached via dedicated server or control room network, never expose the shares to the office network or customer intranet (direct or through VPN) and never expose shares to the Internet.</td>
</tr>
</tbody>
</table>

See section *Setting Up the Project* in the Desigo CC online help. Please take note the following terms:

- **Windows client account**
  Refers to the user logged on to Microsoft Windows on the client machine; this Windows user can be different from the user logged on to Desigo CC.

- **Web server account**
  Refers to the account configured in the Desigo CC web server installation.

The following subdirectories of the [project] directory are accessed by the client installation (installed client or FEP) and the web server.

- **Documents**
  Provide read access on all files and subfolders to the web server account and all Windows client accounts.

- **Devices, Graphics, Libraries, and Profiles**
  Provide read/write access on all files and subfolders (including the permission to delete them, but not the root folder itself) to the web server account and all Windows client accounts.
  - **Graphics**
    Access may be Unrestricted to read-only for Windows client accounts that only display but do not configure graphics.
  - **Libraries**
    Access may be Unrestricted to read-only for Windows client accounts that run Desigo CC in Operation mode only.
  - **Profile**
    Provide read access to all Windows client accounts, read/write access to the web server account.

- **Shared**
  Provide read access on all files and subfolders to the web server account and all Windows client accounts.

- **All other folders**
  Provide read/write access to the [System Account] only ([System Account] is configured in SMC).
  **Do not provide access on these folders to any other account.**
3.7 Server Services

The following services are deployed on the Desigo CC server:

**GMS_WCCIlpmom_[Project Name]**
This service can run under a local Windows account without administrator privileges.

**Siemens GMS HDB Service**
This service can run under a local Windows account without administrator privileges.

**Siemens GMS Closed Mode Service**
This service must run under local system or a Windows account with administrator privileges.

**Siemens GMS SMC ProjectData Service**
This service supports setting up distributed systems, and remote installed clients and FEPs. This service is not needed for operating Desigo CC and can be disabled in the Windows Services once the setup of remoted components is completed.
In case of distributed systems it is recommended to disable this service after system configuration and re-enable it only during system reconfiguration.

**SQL Server ([Instance Name]) and SQL Server Browser**
Microsoft SQL Server services for the History/MNS Database (if the database is deployed on the Desigo CC server).
Additional services are installed depending on the extension modules deployed (please refer to the respective integration guides), for example:

**OPC Enum**
Belongs to the Desigo CC OPC server.
- Select **None** as your **Authentication Level**.
- **Launch Permissions** - Select the option **Use Default**.
- **Access Permissions** - Select the option **Use Default**.

Configuration Permissions:
- **Anonymous**
- **Everyone**
- **Guests**
- **Interactive**
- **Network**
- **System**

Ensure that all of the accounts above receive **Full Control** rights.
If you are using IIS (Internet Information Services) as an OPC client make sure to add the following accounts as well:
- **IWAM_<computer-name>**
- **IUSR_<computer-name>**

Use the Interactive Account or System Account.

**UA Local Discovery Server**
Belongs to the Desigo CC OPC server.
Allow the **UA Local Discovery Server to start Automatically**.
Configure your Firewall to permit **TCP port 4840**.

**UA COM Server Wrapper**
Belongs to the Desigo CC OPC server.
The OPC UA wrapper enables a UA client to connect to a COM-based OPC DA2/DA3 server. Internally the wrapper is a small UA server that obtains data from its internal COM DA2/DA3 client. This client can be configured to connect to any compliant OPC server.

Siemens BT Video API Service
This service is part of the Video extension module and can also be deployed on a remote machine as an option.
By default, the BT Video API service runs on the Desigo CC server as an anonymous Windows Network Service. For security reasons, you must make it instead run as a named account, with administrator privileges. In addition, for proper operation of the Video extension, Desigo CC services must also be set to run under this named account.

On the Desigo CC server computer, you must create a VideoAPIService user account in Windows.

NOTE: The account must be an administrator Windows user, and it will also be assigned the role of administrator in the VMS.
Depending on the deployment scenario, this task is performed in the following ways:
- If the VMS server runs on the same computer as the Desigo CC server: create a VideoApiService local account on the shared computer.
- If VMS server runs on a separate computer different from the Desigo CC server:
  - On a Windows domain, create a domain VideoApiService account, which can be used on all the computers of the domain.
  - On a Windows workgroup, create the same VideoApiService account as local user on the Desigo CC server and on the VMS server. Use the same user name and password on both computers. If a password change is done later (for example, due to enforcing password policy), the change must be done consistently on both computers.

In any case, for more information about creating a new Windows user account, refer to the Microsoft documentation and online help.

Add Credentials of the Basic User on the Station
Next, the Windows Credential Manager will be used to add the BasicStreamingUser created above to the Desigo CC station where video streams must be displayed.
Repeat this procedure for all the Desigo CC stations where you want to display streaming video.

1. On the Desigo CC station where you want to show video streams, open the Windows Credential Manager as follows:
   a. Select Start > Control Panel.
   b. Select User Accounts > Credential Manager.
2. Select Windows Credentials.
3. Click Add a generic credential.
4. In the Internet or network address field, enter VMS server host name.
5. In the User name field, enter exactly the following string: [BASIC]\BasicStreamingUser.
6. In the Password field, enter the password you used for creating the VideoAPIStreamingUser, above.
   ✷ The credentials of the BasicStreamingUser are added to the vault of the Desigo CC computer.
7. Restart the Desigo CC application.

**VMS Service (Embedded Surveillance VMS200)**

Installed separately by users, not by the Video extension module. The Video Management System (VMS) server can be installed on the same computer as the Desigo CC server or on a separate computer.

**Install VMS Server on the same computer as the Desigo CC Server**

The VMS uses default website ports 80 (HTTP) and 443 (HTTPS) for its client stations. This setting cannot be changed. When installing VMS on the same computer as the Desigo CC server, you must check in SMC that these ports are not already used by a Desigo CC website (for example, to support web clients or web services), and if necessary, switch the Desigo CC website to use different ports (for example, 8080 and 8443, respectively). In addition, if the default IIS website was removed during the Desigo CC installation, you must re-create it before installing VMS.

1. In the SMC Websites, do not use the ports 80 and 443, which will be used by VMS.

2. If the default IIS default website was removed (for example, to replace it with a Desigo CC website), you must create it again before installing the VMS server.
   - Run the **Internet Information Services (IIS) Manager** (refer to Microsoft documentation).
   - In the **Sites** node, re-create the default website.

3. In the **Add Website** dialog box, enter the following settings:
   - **Site name**: enter Default Web Site.
   - **Application Pool**: click **Select...**, and choose DefaultAppPool.
   - **Physical path**: enter %SystemDrive%\inetpub\wwwroot.
   - **Binding options**: use the default settings.

4. Install the VMS server.

In the setup wizard, after selecting the installation language and the license file (valid licenses are listed in Video VMS Reference), you can:

- Choose the **Single Server** installation variant, which is largely predefined and very easy (you can only select the file location and the product language).
- Choose the **Custom** installation variant (recommended to optimize the SQL database functions). In the subsequent custom installation steps, proceed as follows:
  a. In the SQL section, select the GMS_HDB_Express SQL server instance.
  b. Use the default settings for all other installation options.

You can also install the VMS software before Desigo CC, and you can share the SQL Server installed by the VMS with Desigo CC.

**Install VMS Server on a Computer Different from the Desigo CC Server**

- Install the VMS server following its separate installation instructions. In the VMS software setup, you can select the **Single-Server** (recommended) or the **Custom installation** variant.

**NOTE:** Do not use the **Distributed-Servers** variant. This is referred to architectures with multiple VMS servers.
3.8 LMS – License Management System
The BT LMS (Licensing Management System) provides the common BT Licensing solution to support the global SI (Smart Infrastructure) initiatives. To harden an LMS installation, refer to the following link:

3.9 Physical and Environmental Security
In order to protect the Desigo CC server, the cabling, and the clients, do the following:
- Desigo CC servers and all servers that are connected to Desigo CC should be located in a data center or server room with restrictive access control.
- Desigo CC clients that are directly accessed by users could be locked in furniture in a way that a regular user does not have physical access to the client computer and its interfaces like USB ports or CD drive. Alternatively, client machines could be also located in an access-controlled data center or server room providing restrictive access control like the Desigo CC servers.
- Protect physical access to the cabling in the Backbone Level protection zone.
- Define and implement processes for granting and revoking physical access.
- Additional controls, such as site protection, additional restrictive access control for the building and rooms, security guards or surveillance can contribute to the physical security of the system.
3.10 Incident Handling

If a security-related event occurs, please immediately contact your Siemens point of contact (for example, Field Engineer or Sales Representative) or contact Siemens Computer Emergency Response Team for products (ProductCERT).

Internet: [http://www.siemens.com/cert/advisories](http://www.siemens.com/cert/advisories)

Email: productcert@siemens.com

- To ensure that your issue gets resolved soon, please provide your input to ProductCERT either in English or in German.

3.11 Windows Hardening

First of all, let's define *hardening*. When you harden a system, you are attempting to reduce its surface of vulnerability. Ideally, you want to be able to leave it exposed to the general public on the Internet without any other form of protection. This is not a system you will use for a wide variety of services. A hardened system should serve only one purpose—it is a web server or DNS or Exchange Server and nothing else. You do not typically harden a file and print server, a domain controller, or a workstation. These systems need too many functions to be properly hardened.

System Hardening Steps

To harden a Windows server, you must perform the following steps, at a bare minimum:

- **Disable all unnecessary services.** To do this, you first need to determine which services can be disabled. Sounds simple enough, but it is not. For example, it is not possible to disable the Remote Procedure Call (RPC) service. Also, little documentation exists to identify what services a given purpose will require. Even if we had such a list, it would likely change depending on a vendor's specific implementation (say, of a DNS or mail server). In the end, knowing which services are required and which can be disabled is largely a matter of trial and error.

- **Remove all unnecessary executables and registry entries.** Forgetting to remove unneeded executables and registry entries might allow an attacker to invoke something that had previously been disabled.

- **Apply appropriately restrictive permissions to files, services, end points, and registry entries.** Inappropriate permissions could give an attacker an opening. For example, the ability to launch CMD.EXE as *Local System* is a classic backdoor.

The benefits of OS hardening a Windows server are that you will have fewer patches to apply, you will be less likely to be vulnerable to the average exploit, and you will have fewer records to review in the logs. You can focus your attention on what the server is doing, not on unnecessary services it may have running.

On the other hand, it is very difficult to properly harden/configure a system and keep it running effectively. Documentation is scarce and permissions are required to make it effective. Finally, even a hardened Windows server will probably have far too many resident files and registry entries to effectively monitor and maintain.
3.12 Web Browser Security

When using any web browser to run a Desigo CC client, a special attention is required for the security settings of the web browser. Make sure the saving function for credentials is disabled in the web browser setting.

**Update to TLS 1.2 as default secure protocols in Windows**

Transport Layer Security (TLS) is a protocol that provides privacy and data integrity between two communicating applications and is the most widely deployed security protocol used today. TLS is used for web browsers and other applications that require data to be securely exchanged over a network and ensures that a connection to a remote endpoint is the intended endpoint through encryption and endpoint identity verification. Client-server applications use the TLS protocol to communicate across a network in a way designed to prevent eavesdropping and tampering. There are known vulnerabilities associated with SSL 3.0/TLS 1.0 which allow adversaries to monitor/intercept traffic and decrypt secure transmissions. Updating to TLS 1.2 provides an enhanced level of encryption to protect our network.

See how to [Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows](https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls).

**Enable Strong cryptography for components targeted for framework .NET 4.5**

For enabling the cryptography these entries must be specified:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319
SchUseStrongCrypto (type = DWORD, Value = 1 hexadecimal)
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319
SchUseStrongCrypto (type = DWORD, Value = 1 hexadecimal)
```

**Optional: Disable TLS 1.0 and TLS 1.1**

Desigo CC runs on TLS 1.2. As soon as TLS 1.2 is enabled, and no other software uses TLS 1.0 and TLS 1.1 then TLS 1.0 and TLS 1.1 can be disabled on the server.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
Enabled (type = DWORD, Value = 0 hexadecimal)
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
Enabled (type = DWORD, Value = 0 hexadecimal)
```

**Update PresentationHost.exe to TLS 1.2**

By default, the XBAP client runs using TLS 1.0 even if TLS 1.2 is enabled on all machines at the customer’s site. The browser connects using TLS 1.2, but Microsoft PresentationHost.exe (which executes our XBAP client) reconnects using TLS 1.0. So not only the OS, but also the PresentationHost.exe must use TLS 1.2. There is no official support site from Microsoft dedicated only to this issue; only generic information such as:

In the end what must be done is to enable TLS 1.2 on the machines running the XBAP browser client in the registry (on Windows 10 only the last two entries are needed):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
DisabledByDefault (type = DWORD, Value = 0 hexadecimal)
Enabled (type = DWORD, Value = 1 hexadecimal)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetFramework\v4.0.30319
SchUseStrongCrypto (type = DWORD, Value = 1 hexadecimal)

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NetFramework\v4.0.30319
SchUseStrongCrypto (type = DWORD, Value = 1 hexadecimal)

The ClickOnce client is not impacted. It runs automatically using TLS 1.2 when the protocol is available on the client.

- **Windows SMBv1 Remote Code Execution Vulnerabilities**
  Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.
  To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.
  The EternalBlue exploit targets a vulnerability (addressed in Microsoft Security Bulletin MS17-010) in the SMBv1 protocol, through port 445. During an attack, black hats scan the internet for exposed SMB ports, and if found, launch the exploit code. If the target is vulnerable, the attacker will then run a payload of the attacker's choice on the target. This was the mechanism behind the effective distribution of WannaCrytor.D ransomware across networks.

- **Mitigating Factors: Disable SMBv1 in Windows and Windows Server**
  See the following references:
  https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-in-windows-server-2012/

- **Patching**
  All components (such as virtualization software, operating systems or anti-malware software) should always be running with the latest security patches. It is not within the control of Siemens to provide patches for components that are operated with Desigo CC but do not originate from Siemens, such as client operating systems.

- **Use a proper discovery service**
  The only way to know if a breach or vulnerability exists is to employ broad discovery capabilities. A proper discovery service entails a combination of active and passive discovery features and the ability to identify physical, virtual, and on and off premise systems that access your network. Developing this current inventory of production systems, including everything from IP addresses, OS types and versions and physical
locations, helps keep your patch management efforts up to date. It is therefore important to inventory your network on a regular basis.

- **Perform application patching**
  Many limitations of OS platform support and discovery services lie in accounting for only applications from a specific OS and ignoring third-party software. Much of Windows software vulnerabilities come from non-Microsoft applications running on Windows, which means you not only need comprehensive OS coverage, but also comprehensive application coverage.

- **Apply coverage on and off premise**
  Patching your OS and applications will be meaningless, however, if not done for every computer in every location. Users can work remotely without ever touching the network, but the network must secure these users as if they were on premise. Patch management systems and other security controls should provide the same level of coverage and control off premise as they do on premise.

- **Patch frequently**
  As more end user systems can leave the network, patching frequency becomes more important. You may be following the patching patterns of prominent tech influencers, but they could be wrong for you. Microsoft may keep to a predictable security patch release cycle, but most other vendors have unpredictable release schedules.

<table>
<thead>
<tr>
<th><img src="" alt="NOTICE" /></th>
</tr>
</thead>
</table>
| **End of Life IT Components**

IT components must be replaced as soon they pass their End of Life. EOL IT does not meet today’s needs for cybersecurity.

<table>
<thead>
<tr>
<th><img src="" alt="NOTICE" /></th>
</tr>
</thead>
</table>
| **Use a Test System**

Siemens cannot guarantee that updating of third-party components can be used without consequences on the operation of the overall system. Depending on the criticality of the system, we recommend establishing a release process.
3.13 Hardening Guidelines

This section defines the minimal hardening measures that must be applied for each of the reference deployments in order to comply with Desigo CC requirements and therefore meet Security Level 1 (SL1).

3.13.1 D1: Unsecured Desktop

IT Security Level 1 for Desigo CC cannot be achieved at this level of hardening. Therefore, do not use it without an express written waiver of responsibility by the customer.

<table>
<thead>
<tr>
<th>Measures or Description</th>
<th>Location of the physical server</th>
<th>Physical/virtual server exclusivity</th>
<th>Physical server protective measures</th>
<th>Server protective measures (Software)</th>
<th>Server OS version and set up</th>
<th>Client OS version and set up</th>
<th>Client protective measures (Software)</th>
<th>Connection for clients inside the customer network</th>
<th>Connection for clients outside the customer network (Remote access)</th>
<th>Printers connectivity</th>
<th>IT skills of users</th>
<th>IT skills of system administrators</th>
<th>IT skills of network administrators</th>
<th>IT skills of the installer (BT or VAP)</th>
<th>Field devices connectivity</th>
<th>Connection to other services (for example, OPC servers and clients)</th>
<th>Client Windows login</th>
<th>Desigo CC users</th>
<th>Desigo CC client options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of the physical server</td>
<td>On desktop where access by uncontrolled persons is possible.</td>
<td>Non-exclusive: a computer also used for normal office tasks, including private surfing on the Internet.</td>
<td>None</td>
<td>Standard antivirus and standard desktop firewall configuration (auto allowance ON), maintained.</td>
<td>Off-the-shelf Windows installation</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Through remote desktop</td>
<td>Yes</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Directly on the customer network</td>
<td>Directly on the customer network</td>
<td>Administrative autologon</td>
<td>Desigo CC authentication</td>
<td>Any client options</td>
</tr>
</tbody>
</table>
3.13.2 D2: Stand-alone Desktop Application

Applicability

<table>
<thead>
<tr>
<th>Location of the physical server</th>
<th>On the desktop of one of the users in a controlled office environment (not in a publicly accessible area).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical/virtual server exclusivity</td>
<td>Non-exclusive: a computer also used for regular office tasks.</td>
</tr>
</tbody>
</table>

**Topic** | **Required Hardening** |
---|---|
Physical server protective measures | Unplug and theft protection. |
Server protective measures (Software) | Disable interfaces with memory access (FireWire, USB 3.1). Encrypt the hard disk. Continuously maintained and strong antivirus protection. Continuously maintained desktop firewalls. Firewalls rules not on auto allowance, UPS needed. |
Server OS version and set up | Secure Windows OS installation. Set up and maintain Windows OS security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications. |
Client OS version and set up | n/a |
Client protective measures (Software) | n/a |
Connection for clients inside the customer network | n/a |
Connection for clients outside the customer network (Remote access) | n/a |
Remote access | Through remote desktop |
Printers connectivity | Yes |
IT skills of users | Low |
IT skills of system administrators | Medium |
IT skills of network administrators | Medium |
IT skills of the installer (BT or VAP) | Medium |
Field devices connectivity | Directly, through VLAN or customer networks: customer is responsible for securing it. The assumption is that the customer's IT secures field device connectivity. |
Connection to other services (for example, OPC servers and clients) | Directly, through VLAN or customer networks: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity.

Client Windows login | No autologon or professional KIOSK mode.

Desigo CC users | Use Windows authentication only.

Desigo CC client options | Any client options

### 3.13.3 D3: Client/Server Application in Office Environment

#### Applicability

<table>
<thead>
<tr>
<th>Topic</th>
<th>Required Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of the physical server</td>
<td>On the desktop of one of the users in a controlled office environment (not in a publicly accessible area).</td>
</tr>
<tr>
<td>Physical/virtual server exclusivity</td>
<td>Non-exclusive: a computer also used for regular office tasks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Required Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical server protective measures</td>
<td>Unplug and theft protection.</td>
</tr>
<tr>
<td>Server protective measures (Software)</td>
<td>Disable interfaces with memory access (FireWire, USB 3.1). Encrypt the hard disk. Continuously maintained and strong antivirus protection. Continuously maintained desktop firewalls. Firewalls rules not on auto allowance, UPS needed.</td>
</tr>
<tr>
<td>Server OS version and set up</td>
<td>Secure Windows OS installation. Set up and maintain Windows OS security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications.</td>
</tr>
<tr>
<td>Client OS version and set up</td>
<td>Secure Windows OS installation. Set up and maintain Windows security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications. Managed certificates and credential.</td>
</tr>
</tbody>
</table>
| Client protective measures (Software)                                                                 | Disable interfaces with memory access (FireWire, USB 3.1).  
|                                                                                                    | Continuously maintained and strong antivirus protection.  
|                                                                                                    | Continuously maintained desktop firewalls.  
|                                                                                                    | Firewalls rules not on auto allowance.  
|                                                                                                    | Secure certificate store.  
|                                                                                                    | Set up all applications running on the client. Do not store passwords locally. |
| Connection for clients inside the customer network                                                 | Secured communication configured.  
|                                                                                                    | Segmented Network.  
|                                                                                                    | Network firewalls configured and continuously maintained. |
| Connection for clients outside the customer network (Remote access)                                | Secured communication configured.  
|                                                                                                    | Segmented Network.  
|                                                                                                    | Network firewalls configured and continuously maintained.  
|                                                                                                    | DMZ configured. |
| Remote access                                                                                        | Via remote desktop and VPN.  
|                                                                                                    | Clients on Internet Unrestricted to "need to know". |
| Printers connectivity                                                                                 | Yes |
| IT skills of users                                                                                    | Low |
| IT skills of system administrators                                                                   | Medium |
| IT skills of network administrators                                                                  | High |
| IT skills of the installer (BT or VAP)                                                                | Medium |
| Field devices connectivity                                                                            | Directly, through VLAN or customer networks: customer is responsible for securing it. The assumption is that the customer's IT secures field device connectivity. |
| Connection to other services (for example, OPC servers and clients)                                    | Directly, through VLAN or customer networks: customer is responsible for securing it. The assumption is that the customer's IT secures field device connectivity. |
| Client Windows login                                                                                  | No autologon or professional KIOSK mode. |
| Desigo CC users                                                                                       | Use Windows authentication only. |
| Desigo CC client options                                                                              | Use Windows App and web client only. |
### 3.13.4 D4: Client/Server Application in a Secured Location/Control Room

#### Applicability

<table>
<thead>
<tr>
<th>Topic</th>
<th>Required Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suitable and supported for IT security</td>
<td>If Desigo CC security prescriptions are applied.</td>
</tr>
<tr>
<td>Location of the physical server</td>
<td>Supervised control room desk and enclosure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Required Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical/virtual server exclusivity</td>
<td>Non-exclusive: a computer also used for regular office tasks.</td>
</tr>
<tr>
<td>Physical server protective measures</td>
<td>Server machine locked in cabinet. Unplug and theft protection.</td>
</tr>
<tr>
<td>Server protective measures (Software)</td>
<td>Disable interfaces with memory access (FireWire, USB 3.1). Encrypt the hard disk. Continuously maintained and strong antivirus protection. Continuously maintained desktop firewalls. Firewalls rules not on auto allowance, UPS needed. FEP in enclosed environment (locked cabinet).</td>
</tr>
<tr>
<td>Server OS version and set up</td>
<td>Secure Windows OS installation. Set up and maintain Windows security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications. Secured network configuration (for example, managed access rights to network folders).</td>
</tr>
<tr>
<td>Client OS version and set up</td>
<td>Secure Windows OS installation. Set up and maintain Windows security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications. Managed certificates and credentials.</td>
</tr>
<tr>
<td>Client protective measures (Software)</td>
<td>Disable interfaces with memory access (FireWire, USB 3.1). Continuously maintained and strong antivirus protection. Continuously maintained desktop firewalls. Firewalls rules not on auto allowance. Secure certificate store. Set up all applications running on the client. Do not store passwords locally.</td>
</tr>
<tr>
<td>Connection for clients inside the customer network</td>
<td>Secured communication configured. Segmented network. Network firewalls configured and continuously maintained.</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection for clients outside the customer network (Remote access)</td>
<td>Secured communication configured. Segmented network. Network firewalls configured and continuously maintained. DMZ configured.</td>
</tr>
<tr>
<td>Remote access</td>
<td>Through remote desktop and VPN Clients in Internet Unrestricted to need to know.</td>
</tr>
<tr>
<td>Printers connectivity</td>
<td>Yes</td>
</tr>
<tr>
<td>IT skills of users</td>
<td>Low</td>
</tr>
<tr>
<td>IT skills of system administrators</td>
<td>Medium</td>
</tr>
<tr>
<td>IT skills of network administrators</td>
<td>High</td>
</tr>
<tr>
<td>IT skills of the installer (BT or VAP)</td>
<td>Medium</td>
</tr>
<tr>
<td>Field devices connectivity</td>
<td>Directly, through VLAN or customer networks: customer is responsible for securing it. The assumption is that the customer's IT secures field device connectivity.</td>
</tr>
<tr>
<td>Connection to other services (for example, OPC servers and clients)</td>
<td>Directly, through VLAN or customer networks: customer is responsible for securing it. The assumption is that the customer's IT secures field device connectivity.</td>
</tr>
<tr>
<td>Client Windows login</td>
<td>No autologon or professional KIOSK mode.</td>
</tr>
<tr>
<td>Desigo CC users</td>
<td>Use Windows authentication only.</td>
</tr>
<tr>
<td>Desigo CC client options</td>
<td>Any client options</td>
</tr>
</tbody>
</table>
### 3.13.5 D5: Client/Server Application in a Professional IT Environment

#### Applicability

<table>
<thead>
<tr>
<th>Location of the physical server</th>
<th>Unrestricted server room</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical/virtual server exclusivity</td>
<td>Exclusive: Server only hosts Desigo CC applications.</td>
</tr>
</tbody>
</table>

#### Topic | Required Hardening

<table>
<thead>
<tr>
<th>Physical server protective measures</th>
<th>Server machine locked in cabinet.  Unplug and theft protection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server protective measures (Software)</td>
<td>Disable interfaces with memory access (FireWire, USB 3.1). Encrypt the hard disk. Continuously maintained and strong antivirus protection. Continuously maintained desktop firewalls. Firewalls rules not on auto allowance, UPS needed. FEP in enclosed environment (locked cabinet).</td>
</tr>
<tr>
<td>Server OS version and set up</td>
<td>Patched secure Windows installation. Set up and maintain Windows security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications. Secured network configuration (for example, managed access rights to network folders). Advanced malware protection. Automated backup.</td>
</tr>
<tr>
<td>Client OS version and set up</td>
<td>Secure Windows OS installation. Set up and maintain Windows security. Keep Windows OS continuously updated by security patches. Enforce strong password policy. Restrict access to users and to Desigo CC applications. Managed certificates and credentials.</td>
</tr>
</tbody>
</table>
### Client protective measures (Software)
- Disable interfaces with memory access (FireWire, USB 3.1).
- Continuously maintained and strong antivirus protection.
- Continuously maintained desktop firewalls.
- Firewalls rules not on auto allowance.
- Secure certificate store.
- Set up all applications running on the client. Do not store passwords locally.

### Connection for clients inside the customer network
- Secured communication configured.
- Segmented network.
- Network firewalls configured and continuously maintained.

### Connection for clients outside the customer network (Remote access)
- Secured communication configured.
- Segmented network.
- Network firewalls configured and continuously maintained.

### Remote access
- Through remote desktop and VPN
- Clients in Internet Unrestricted to need to know.

### Printers connectivity
- Yes

### IT skills of users
- Low

### IT skills of system administrators
- High

### IT skills of network administrators
- High

### IT skills of the installer (BT or VAP)
- High

### Field devices connectivity
- Directly, through VLAN and secure routing: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity.

### Connection to other services (for example, OPC servers and clients)
- Directly, through VLAN and secure routing: customer is responsible for securing it. The assumption is that the customer’s IT secures field device connectivity.

### Client Windows login
- Professionally secured KIOSK mode.

### Desigo CC users
- Use IDM/Kerberos authentication.

### Desigo CC client options
- Use Windows App and Web Client only.
4 Checklist

The following checklist should be used to perform security controls for the Desigo CC system components. The checklist must be completed for each instance of any component.

Desigo CC Server Hardening Checklist

• User Configuration
Make sure that the password for the local Administrator account is reset to something secure. Furthermore, disable the local administrator whenever possible.
Consider using a non-administrator account to handle your business whenever possible, requesting elevation using Windows equivalent of Linux `sudo` command (that allows you to run programs with the security privileges of another user by default, as the superuser), Run As and entering the password for the administrator account when prompted.
Verify that the local guest account is disabled where applicable. None of the built-in accounts are secure, guest perhaps least of all, so just close that door.
Use a password policy to make sure accounts on the server cannot be compromised. If your server is a member of AD, the password policy will be set at the domain level in the Default Domain Policy. Stand-alone servers can be set in the local policy editor. Either way, a good password policy will at least establish the following:
  ● Complexity and length requirements – how strong the password must be.
  ● Password expiration – how long the password is valid.
  ● Password history – how long until previous passwords can be reused.
  ● Account lockout – how many failed password attempts before the account is suspended

• Windows Features and Roles Configuration
Microsoft uses roles and features to manage OS packages. Roles are basically a collection of features designed for a specific purpose, so generally roles can be chosen if the server fits one and then the features can be customized from there. Two equally important things to do are:
  1. Make sure everything you need is installed. This might be a .NET framework version or IIS, but without the right pieces your applications will not work.
  2. Uninstall anything you do not need. Extraneous packages unnecessarily extend the attack surface of the server and should be removed whenever possible.
This is equally true for default applications installed on the server that will not be used. Servers should be designed with necessity in mind and stripped lean to make the necessary parts function as smoothly and quickly as possible.

• Update Installation
The best way to keep your server secure is to keep it up to date. This does not necessarily mean applying updates as soon as they are released with little to no testing, but simply having a process to ensure updates is applied within a reasonable window. Most exploited vulnerabilities are over a year old, though critical updates should be applied as soon as possible in testing and then in production if there are no problems.

• Firewall Configuration
If you are building a web server, for example, you only want web ports (80 and 443) open to that server from the internet. If anonymous internet clients can talk to the server on other ports, that opens a huge and unnecessary security risk. If the server has other functions such as remote desktop (RDP) for management, they should only
be available over a VPN connection, ensuring that unauthorized people cannot exploit the port at will from the net.

The Windows firewall is a built-in software firewall that allows configuration of port-based traffic from within the OS. On a standalone server, or any server without a hardware firewall in front of it, the Windows firewall will provide some protection against network-based attacks by limiting the attack surface to the allowed ports. That said, a hardware firewall is always a better choice because it offloads the traffic to another device and offers more options on handling that traffic, leaving the server to perform its main duty. Whichever method you use, the key point is to restrict traffic to only necessary pathways.

- **Remote Access Configuration**
  As mentioned above, if you use RDP, be sure it is only accessible via VPN if at all possible. Leaving it open to the internet does not guarantee that you will be hacked, but it does offer potential hackers another inroad into your server.
  Make sure RDP is only accessible by authorized users. By default, all administrators can use RDP once it is enabled on the server. Additional people can join the Remote Desktop Users group for access without becoming administrators.
  In addition to RDP, various other remote access mechanisms such as PowerShell and SSH should be carefully locked down if used and made accessible only within a VPN environment. Telnet should never be used at all, as it passes information in plain text and is insecure in several ways. Same goes for FTP. Use SFTP or SSH (from a VPN) whenever possible and avoid any unencrypted communications altogether.

- **Service Configuration**
  Windows server has a set of default services that start automatically and run in the background. Many of these are required for the OS to function, but some are not and should be disabled if not in use. Following the same logic as the firewall, we want to minimize the attack surface of the server by disabling everything other than primary functionality. Older versions of Microsoft server have more unneeded services than newer, so carefully check any 2008 or 2003 servers.
  Important services should be set to start automatically so that the server can recover without human interaction after failure. For more complex applications, take advantage of the Automatic (Delayed Start) option to give other services a chance to get going before launching intensive application services. You can also set up service dependencies in which a service will wait for another service or set of services to successfully start before starting. Dependencies also allow you to stop and start an entire chain at once, which can be helpful when timing is important.

- **Further Hardening**
  Microsoft provides best practices analyzers based on role and server version that can help you further harden your systems by scanning and making recommendations.
  Although User Account Control (UAC) can be annoying, it serves the important purpose of abstracting executables from the security context of the logged on user. This means that even when you are logged on as an admin, UAC will prevent applications from running as you without your consent. This prevents malware from running in the background and malicious websites from launching installers or other code. Leave UAC on whenever possible.

- **Logging and Monitoring**
  Make sure that your logs and monitoring are configured and capturing the data you want so that in the event of a problem, you can quickly find what you need and remediate the issue. Logging works differently depending on whether your server is part of a domain. Domain logons are processed by domain controllers, and as such, they have the audit logs for that activity, not the local system. Stand-alone servers will have security audits available and can be configured to show passes and/or failures.
Check the maximum size of your logs and scope them to an appropriate size. Log defaults are almost always far too small to monitor complex production applications. As such, disk space should be allocated during server builds for logging, especially for applications like Microsoft Exchange. Logs should be backed up according to your organization’s retention policies and then cleared to make room for more current events.

<table>
<thead>
<tr>
<th>Controls</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement physical and environmental security controls.</td>
<td>☐</td>
</tr>
<tr>
<td>Implement network separation.</td>
<td>☐</td>
</tr>
<tr>
<td>Implement protective firewall rules.</td>
<td>☐</td>
</tr>
<tr>
<td>Implement secure communication to the clients.</td>
<td>☐</td>
</tr>
<tr>
<td>Implement secure communication to remote Desigo CC (if applicable).</td>
<td>☐</td>
</tr>
<tr>
<td>Implement user management controls.</td>
<td>☐</td>
</tr>
<tr>
<td>Implement access control measures.</td>
<td>☐</td>
</tr>
</tbody>
</table>

**Desigo CC**

Even in homogeneous Windows-only environments, managing vulnerabilities and patches across different OS versions can be a daunting affair. The following can serve as a practical starting point for protecting today’s Windows-based infrastructures against cyber attacks.

**Identify Untested/Secured Firmware and 3rd-Party Firmware Modifications**

Modern Windows (7, 8, 10, and Windows Server versions) use what is known as the UEFI firmware standard in place of a computer or device’s standard BIOS. Because the Windows Binary Loader uses UEFI, and UEFI implementation is in the hands of hardware vendors (for example, IBM, Lenovo, Dell)—less scrupulous brands may be inclined to make extra modifications. It is therefore critical that computers or devices manufactured by suspect brands be identified and carefully scrutinized for their potential impact on IT security.

**Fix Unpatched/Incompatible Drivers**

A myriad of hardware devices and services are in use by today’s computers, which invariably creates an ongoing concern around the incompatibility and vulnerability of drivers. And increasingly, drivers are a common source of new security gaps introduced into the environment. Vulnerability detection should therefore include both software packages as well as discreet, stand-alone components such as drivers. Outdated and non-supported drivers should be removed from systems entirely.

**Address Vulnerabilities in Windows-Bundled Software**

Windows 10 ships with several bundled apps like Photos, Groove Music, and Skype, among others. These items are pre-installed with every user account on your Windows 10, but like all software—are subject to their own specific vulnerabilities and flaws. Software vulnerability scanning should include both the Windows operating system and bundled apps that ship with it.

**Enforce Data Encryption**

Data breaches may be inevitable, but stolen data can still be protected—even when in the hands of attackers. Encryption has its pros and cons, but for the most part is a relatively transparent and easy way to prevent data from being exposed; before and after it has been stolen. BitLocker is Microsoft’s solution for file encryption, and ships with newer versions of Windows. The drawback to BitLocker is that every Windows machine using it also brings a supporting BIOS, and has the Trusted Platform Module (TPM) chip enabled.
**Obfuscate Local Administrator Accounts**

More often, malicious programs and hackers will target default local administrator accounts as low hanging fruit for exploitation. A simple renaming of an administrator account adds a simple but effective layer of defense against brute-force attacks. Choosing a less common name makes the account less susceptible to hacking attempts—though in later versions of Windows, local administrator accounts are disabled by default.

**Disable Guest/Anonymous Accounts**

This applies to both Windows and Windows-related services—so guest and anonymous accounts in use by Windows as well as other Windows-related services (For example Microsoft SQL Server, Exchange) should be disabled. Be sure to account for all Windows-related packages, including Microsoft SharePoint deployments and IIS instances.

**Disable Windows Users**

Windows accounts should be disabled. Only Desigo CC accounts should be allowed.

**Put LAN Manager in Check**

The dated LM (LAN Manager) and NTLMv1 authentication protocols have vulnerabilities and should be disabled. LM hash storage should also be disabled, as LM password hashes are easily converted back to plain text.

**Institute Proper Password Management**

In the Windows security realm, 12 characters is the bare minimum for a marginally strong password. As an added precaution, requiring users to select passwords with a 15-character minimum will suffice—with the usual symbol and case assortment requirements.

<table>
<thead>
<tr>
<th>Controls</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement physical and environmental security controls.</td>
<td>□</td>
</tr>
<tr>
<td>Implement network separation.</td>
<td>□</td>
</tr>
<tr>
<td>Implement protective firewall rules.</td>
<td>□</td>
</tr>
<tr>
<td>Implement secure communication to the clients.</td>
<td>□</td>
</tr>
<tr>
<td>Implement user management controls.</td>
<td>□</td>
</tr>
<tr>
<td>Implement access control measures.</td>
<td>□</td>
</tr>
<tr>
<td>Implement operational security controls.</td>
<td>□</td>
</tr>
</tbody>
</table>

**Clients**

All clients that are attached to other networks must implement secure operation, including hardening and malware protection in order to reduce risk to Desigo CC. Hardening is performed using mostly native Windows and Microsoft tools. Malware and hackers attack by exploiting security vulnerabilities. The solution is to reduce the attack surface so that we provide fewer opportunities for exploitation. The main principle is least privilege. To implement the principle of least privilege is to configure your system so that it only does what you normally do, and nothing else. This minimizes the attack surface, and removes services that listen on the network 24/7 to anybody who wants to send it stuff (like an exploit).

Good security means deter, deny, delay, and detect. Hardening covers the first piece. You must also disable the saving function for credentials for all browsers.
Implement physical and environmental security controls (for non-SGD clients).
Implement network separation.
Implement protective firewall rules.
Implement operational security controls
Implement access control measures.
Disable the saving function for credentials in all browsers.
Implement user management controls.

Firewall
Assuming your firewall is deployed and filtering traffic as intended, keeping your firewall’s operating systems patched and up-to-date is probably the most valuable security precaution you can take.

- **Configure Strong & Non-Default Passwords**
  Ensure that all default and blank passwords are changed to suitably strong values. At a minimum we recommend 10 characters in length, containing a mix of lower and uppercase letters, numbers and special characters.
  See that passwords are not re-used between devices and where passwords appear within configuration files, they are listed in encrypted and non-reversible form.

- **Enforce Local Account Lockouts**
  Enforcing account lockouts protects the accounts against password guessing and brute-force attacks. In combination with enforcing password complexity, this reduces the likelihood of an account being compromised using these techniques.

- **Restrict Access to Administrative Ports**
  Restricting access to administrative ports reduces the attack surface exposed by the device. Access to administrative ports should be Unrestricted to trusted interfaces and/or IP addresses. By amending firewall rules it is possible to restrict access to the web console of both the gateway and the management systems.

- **Disable Plain Text Protocols for Administrative Ports**
  Communication sent using plain text protocols could be sniffed by attackers. Check Point allows a secure, encrypted alternative to every plain text protocol, such as SSH instead of Telnet. Disabling plain text protocols is a quick win in terms of improving security.

- **Configure Suitable Remote Management Access**
  The likelihood is that only authorized personnel in your IT department require to log on and remotely manage devices. For this reason, many firewalls allow configuration to restrict management access to specific interfaces, network ranges, and even IP addresses.
  Use protocols that utilize suitable authentication and encryption. Unencrypted management protocols such as Telnet, TFTP, FTP, SNMP prior to version 3, and HTTP should not be used.
  Using HTTPS or SSH for management is highly recommended, preferably configured to use strong ciphers.

**Predefined Security Zones**
These are the predefined security zones and their intended purposes:
- **WirelessZone** – Networks that can be accessed by users and applications with a wireless connection.

- **ExternalZone** – Networks that are not secure, such as the Internet and other external networks.

- **DMZZone** – A DMZ (demilitarized zone) is sometimes referred to as a perimeter network. It contains company servers that can be accessed from external sources. A DMZ lets external users and applications to access specific internal servers, but prevents external users from accessing secure company networks. Add rules to the firewall Rule Base that allow traffic to the company DMZ: for example, a rule that allows HTTP and HTTPS traffic to your web server in the DMZ.

- **InternalZone** – Company networks with sensitive data that must be protected and used only by authenticated users.

<table>
<thead>
<tr>
<th>Controls</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement physical and environmental security controls.</td>
<td></td>
</tr>
<tr>
<td>Implement network separation.</td>
<td></td>
</tr>
<tr>
<td>Implement protective firewall rules.</td>
<td></td>
</tr>
<tr>
<td>Implement access control measures.</td>
<td></td>
</tr>
<tr>
<td>Implement operational security controls.</td>
<td></td>
</tr>
<tr>
<td>Implement user management controls</td>
<td></td>
</tr>
</tbody>
</table>