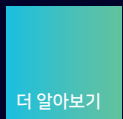




Digitalizing building operation and maintenance

Digital Services

Leveraging on the power of data to enhance resilience & business continuity



SIEMENS

Siemens Smart Infrastructure combines the real and digital worlds across energy systems, buildings and industries, enhancing the way people live and work and significantly improving efficiency and sustainability



Contents

Common Remote Service Platform (cRSP)	4
cRSP IT security	6
CloudFIMs	13
Connect X200	15
Connect X300	25
Appendix	33

Common Remote Service Platform (cRSP)

Support for your systems – whenever you need it



Maximum security –
complete control

Save time with remote services

We provide an extensive range of services via a remote connection. This secure connection gives us access to your systems and enables us to capture and/or adjust the most important parameters. This enables us to take a proactive approach, nipping potential problems in the bud so that availability is maintained.

Service throughout the life cycle

Enabling us to connect remotely to your fire protection, safety, security and building automation systems promises to bring you benefits with operation and maintenance as well as in the event of a fault.

Practical for new and existing systems

The remote connection ensures a prompt response to your requirements for both newly installed systems and existing plant.

Equipped for the digital world

The ability to capture data continuously via a remote connection paves the way for other services such as performance optimization and data monitoring.

Your systems at a glance – always

You need to be confident in the reliability of your systems in order to run your operations consistently, efficiently and cost-effectively. We help you build this reliability by providing precise information and regular performance reports.

On-call around the clock

Our alarm receiving and service centers are there for you 24 hours a day. You also have access to the expert support of trained specialists via the remote connection during the agreed service hours. Our specialists can take appropriate steps immediately where necessary.

Faster initial diagnosis and fault clearance

When your systems encounter difficulties, we can diagnose the problem remotely. Only if we cannot fix the problem via remote, we equip our field service engineer accordingly to ensure we have you up and running again as quickly as possible. This intelligent mix of remote-based and on-site services reduces waiting times and minimizes night deployments.

Your benefits at a glance

- Operator support from Siemens system specialists
- Rapid initial diagnosis enabling targeted fault clearance
- High security standard with end-to-end encryption
- Remote dial-in for own staff and on-call service
- Proactive service protects your investment

더 알아보기



Customer-controlled access

We have established a secure external operation option so that you can gain access from outside of the Siemens network as well. This means that you always have full control over remote access to your systems. You can explicitly block access to particular targets if necessary or grant access only when there is a specific need.

Very high platform availability

Three fully redundant data centers in Germany, Singapore and the USA ensure optimal availability for our remote services.

Regular security audit

The Siemens Computer Emergency Response Team (CERT) is a reliable independent in-house partner that develops preventive security measures and conducts regular audits of our IT infrastructure to check information security.

Information security approved by ISO/IEC27001

Our enterprise-wide common Remote Service Platform (cRSP) offers you a reliable global IT infrastructure with a very high level of data security. We were one of the very first organizations anywhere in the world to establish an information security management system (ISMS) at an international level.

More efficient support for operations

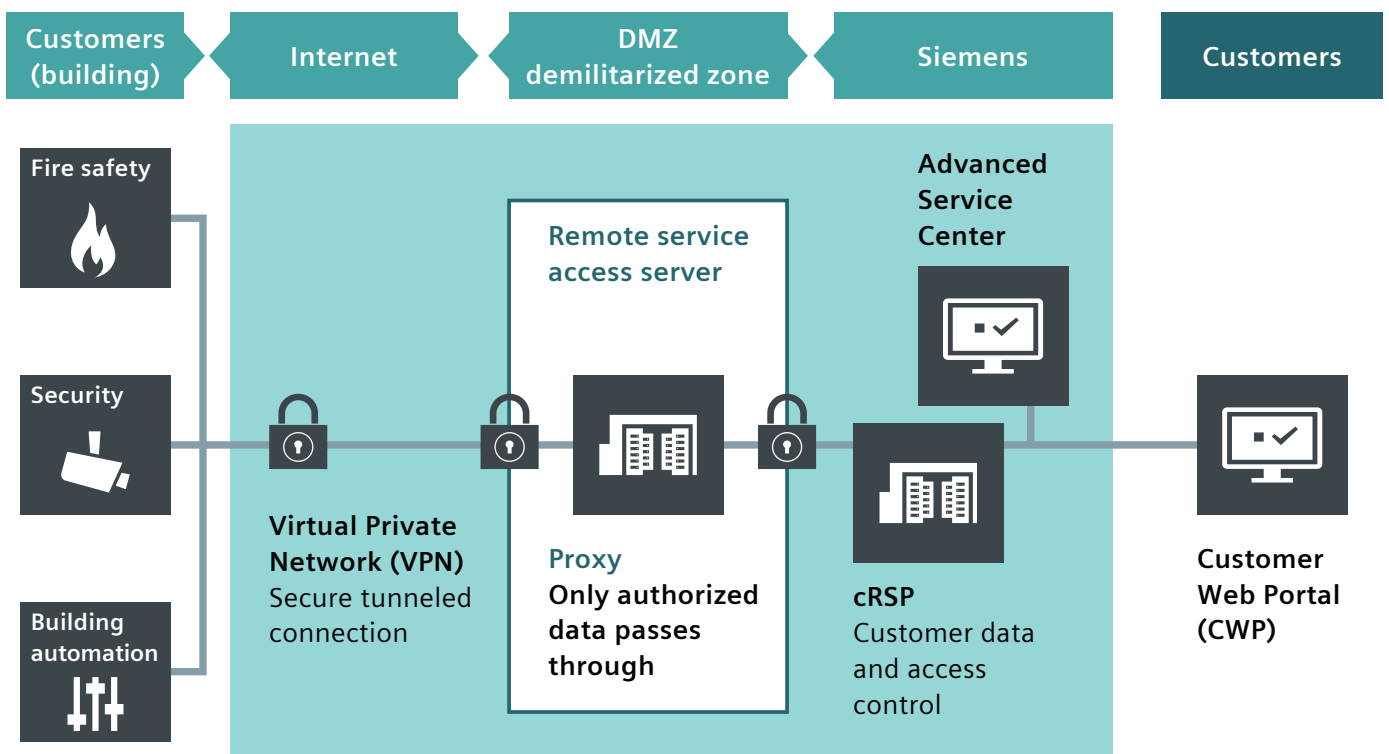
We provide active support with any questions you may have regarding the operation and use of your systems. The remote connection allows us to discover the best answer for you faster and more easily. We are always very happy to help whenever you should find you have questions on the subject of remote access.

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. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under <http://www.siemens.com/cert/en/cert-security-advisories.htm>.



cRSP IT security concept

Data and information on building infrastructure must be available reliably, quickly, globally and securely. Siemens common Remote Services meet all these requirements to the greatest extent.



Document objective

The Siemens common Remote Service Platform (cRSP) is the IT platform used throughout the group for implementing remote access to IP-based equipment. This security concept describes the measures that we at Siemens Smart Infrastructure take to protect customer data and IT systems when using our remote services. In its current version, this concept is applied to all our security, fire safety and building automation systems for which remote services are available over the entire life cycle.

Document layout

This document is divided into two main sections: general operating concept and technical security concept.

The first section, the general operating concept for remote services, discusses the fundamental aspects of information security within our company. The topic of remote services for building technology is introduced next, along with a look at the application-specific use cases for remote connections. This part also deals with the strategic security measures in the areas

of data management and personnel selection, which are organizationally implemented for remote services.

It gives customers a general understanding of data security in remote connections.

The second section, the technical security concept, provides technical measures and advice on remote access, including access types and logging, secure IT infrastructure, protecting data transmissions and protecting against attacks.

The technical components, processes and procedures, such as authentication and authorization, are described in detail here. This part is therefore especially helpful for IT specialists who are interested in the type of connection or encryption methods.

Finally, you will find an overview of the various connectivity options in the appendix.

General operating concept

Our emergency call and service centers are available to you 24/7. Trained specialists are also standing by to provide you with remote assistance.

Data security as a basic requirement

Confidentiality and long-term partnerships are highly valued at Siemens. That is why we give the security of your data the highest priority. Before Siemens implements and enhanced service package with remote support, an in-depth analysis of the situation will be conducted, taking into account national and international regulations, technical infrastructures and industry specifics.



Remote services for building technology

As modern systems and solutions become more and more interconnected, we at Siemens take on the resulting challenge: we offer an extra service portfolio in addition to our existing on-site system service. It is based on remote support, thus providing an even higher level of flexibility and system availability.

The remote connection does not only make it possible to determine the causes of system issues faster and more efficiently, but also enables these issues to be solved quickly and intelligently from a remote location. Even in cases where remote repairs cannot be carried out, the information obtained in advance through remote diagnosis will help the service technician to provide our customers the best possible and highly efficient support on site. This means that our technician exactly knows what is to be expected on site and will have appropriate equipment at hand.

But that is not all. With our proactive services, provided according to the specific use case, Siemens takes preventive action to avoid errors instead of responding only after they have occurred, thus minimizing your system down times.

In addition to this, critical data (e. g. login data) will not be stored in the cRSP.

Within the scope of our proactive services data will be sent on a regular basis via the existing secured connection from the systems to Siemens. This connection will be established after a successful authorization (see "Authentication and authorization" below).

Use cases for remote services

Below is a list of use cases, which may vary according to access type and duration.

Remote commissioning: support for commissioning systems, customizing the configuration/supply

- Operational assistance: Customer support in operating the system
- Remote diagnosis: Advance diagnosis of faults from a remote location, collection of diagnostic information for technician deployment
- Remote repair: Restoring operation, clearing faults, customizing the configuration/supply
- Maintenance support: Preparation and support for maintenance and repairs, downloading updates and patches
- Performance monitoring: Electronic monitoring of the system for faults, threshold values and states

The remote advantage

Remote service provides additional support to optimally service your fire safety, security and building automation systems in the face of growing complexity.

The advantages of cRSP include

- Remote monitoring to proactively detect and correct interruptions in order to minimize system downtimes
- Faster and more efficient determination of the causes of system problems
- Fast, intelligent correction of problems through remote intervention
- Service engineers arrive on site already well informed and optimally equipped
- Fast user support for application issues
- Ability to escalate support

Data management

Siemens treats your data as confidential and grants access only on a need-to-know basis. The implementation of this principle is supported by rule-based access mechanisms, which are mapped within an infrastructure and tool landscape designed specifically for this purpose. The data management measures implemented depend on your data protection requirements, the type of data and the provisions of applicable regulations.

Personnel selection

Our service technicians and experts are aware of the need for confidentiality in handling your data and know the serious consequences of failure to comply with the relevant regulations. As a result, only employees who have been trained in data protection and IT security are allowed to work in our Remote Service Center. Siemens has strict selection criteria, and our service technicians must participate in ongoing training and processes. Your data is thus always in safe hands

Platform availability

The availability of our remote services is secured by three data centers in Germany, Singapore and the United States. The capacity of each center was designed so that the cRSP platform remains unaffected in the event of a malfunction. The integration of additional plans for disaster recovery (DR) and business continuity management (BCM) ensures the highest possible availability of our remote services.

Siemens CERT auditing

The Siemens Computer Emergency Response Team (CERT) is an internal, independent and trustworthy partner which develops preventive security measures and assesses the information security of the IT infrastructure.

Certification

Siemens was one of the world's first organizations to implement an internationally valid information security management system (ISMS) according to ISO/IEC 27001 for remote services. Our cRSP platform is audited regularly for effective protection and continuous improvements.

You determine how access takes place

As a basic requirement, you must contractually authorize every service activity. Access is designed to only be granted for the contractually agreed use cases.

To enable access to your systems from outside the Siemens network, the Customer Web Portal (CWP) with enhanced security requirements (2 factors authentication) has been established. In addition to just setting up a connection, you also have the option of explicitly barring access to individual destinations and enabling them again only when needed. Combined with the retrieval of log files on successful access attempts, this gives you always control over remote access to your system.

Access scenario example

- The customer has the possibility to lock all connections or just specific systems. The service technician requiring access to a locked system needs to contact the customer. The customer can then log in to CWP and unlock the required connection. After that, the technician can connect and implement the necessary service tasks remotely. When the service is finished, the customer can lock the connection again.
- Full access: an expressly authorized service engineer has the customer's permission to connect to the system at any time. Each system access is automatically logged for customer review. Customers commonly choose to grant full access when proactive preventive maintenance and highest possible system availability are their key considerations.
- In real time or at agreed intervals. This makes it possible to collect statistical data for system optimization, proactive fault management and services. Siemens works closely together with the customer to ensure that only the agreed type of data is transmitted.

Authentication and authorization of Siemens service personnel

The central backend of the cRSP platform is in a separate segment within the Siemens intranet.

Siemens therefore issues PKI certificates for employees. Every time a service technician logs into the cRSP portal, her / his access rights are verified based on PKI, a strong authentication method using a smart card. The access models you define are then mirrored within our cRSP platform and converted to authorized IT system access levels. These access levels are then matched to the service technicians verified identify.

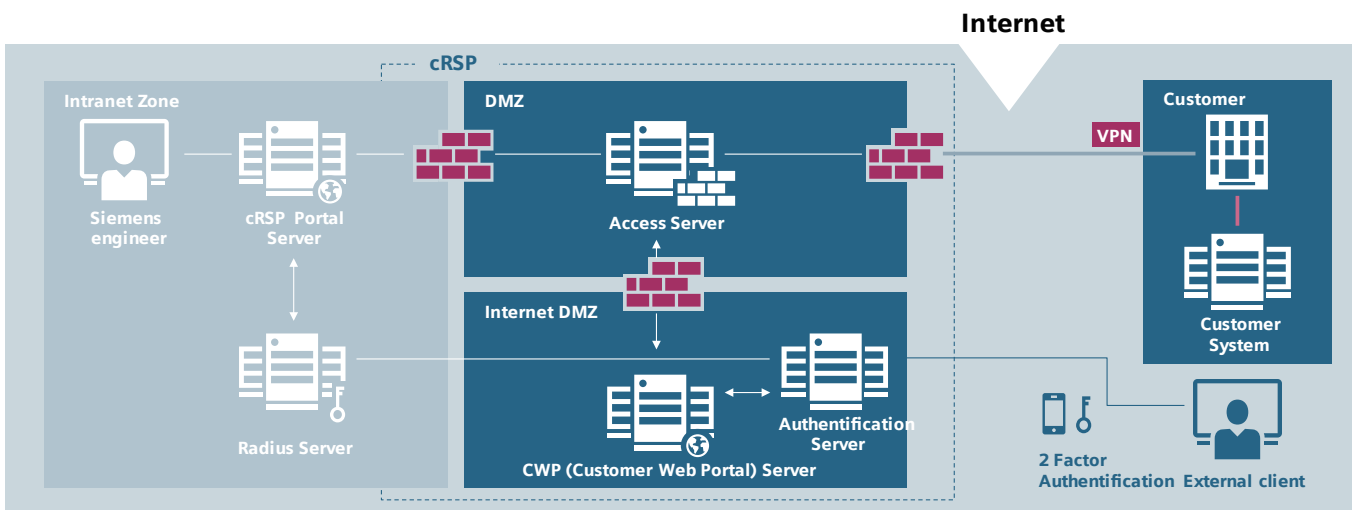
Using this procedure means that service technicians can access only those areas of your system for which they have been expressly authorized ahead of time.

Authenticating and authorizing your personnel

To enable you to access your systems outside the Siemens network, the Customer Web Portal (CWP) with enhanced security requirements (two factors authentication) has been established.

The CWP itself is within the Siemens DMZ (Demilitarized Zone; see Network structure for more information). Established users and their authorizations, like Siemens intranet users, are stored on a server in another network segment. Authentication takes place in the CWP with the user ID, a password and a mobile PIN. If you need to access the web portal, enter your user name and password as well as your mobile PIN or email.

If you have any questions or need assistance, please contact your usual local country organization.



Technical security concept

Network structure

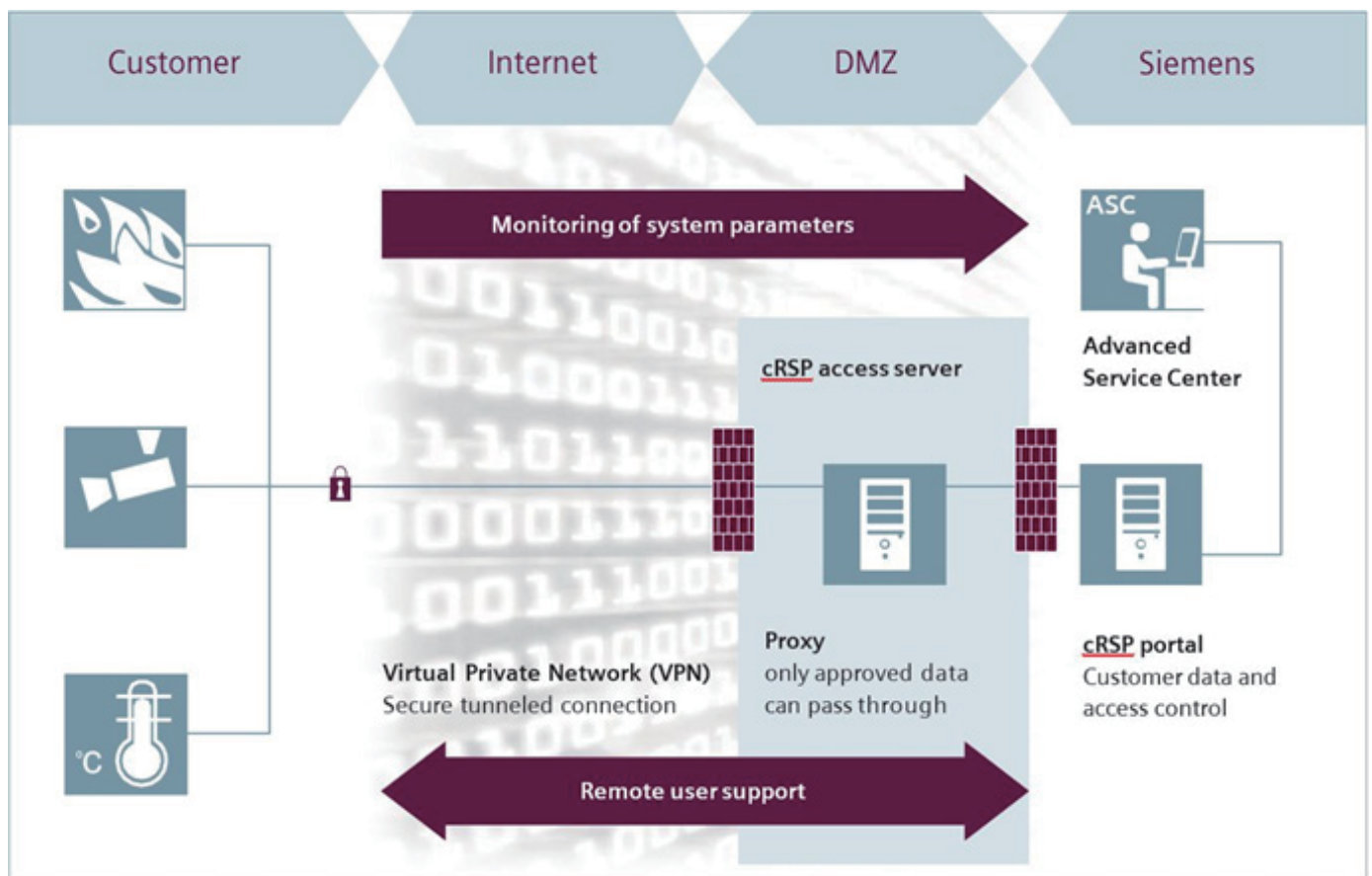
To protect your network as well as the Siemens intranet against threats, Siemens has secured the cRSP infrastructure in a DMZ. Service technicians do not set up end-to-end connections to your systems or vice versa. Instead, the connections end in the DMZ, which is secured on both sides by firewalls. The reverse proxy server establishes the connection to your system and mirrors the incoming communication to the Siemens intranet. This prevents a connection from being set up between the Siemens intranet and your network using unauthorized protocols, since the mirroring (procedure) only works with predefined protocols.

This architecture prevents, for example:

- Unauthorized access from one network to the other
- Access from a third network (by unauthorized systems and users)
- Fraudulent use of secret passwords, access data, etc.
- The transmission of viruses or other harmful programs from one network to the other

Virtual private network via a broadband connection

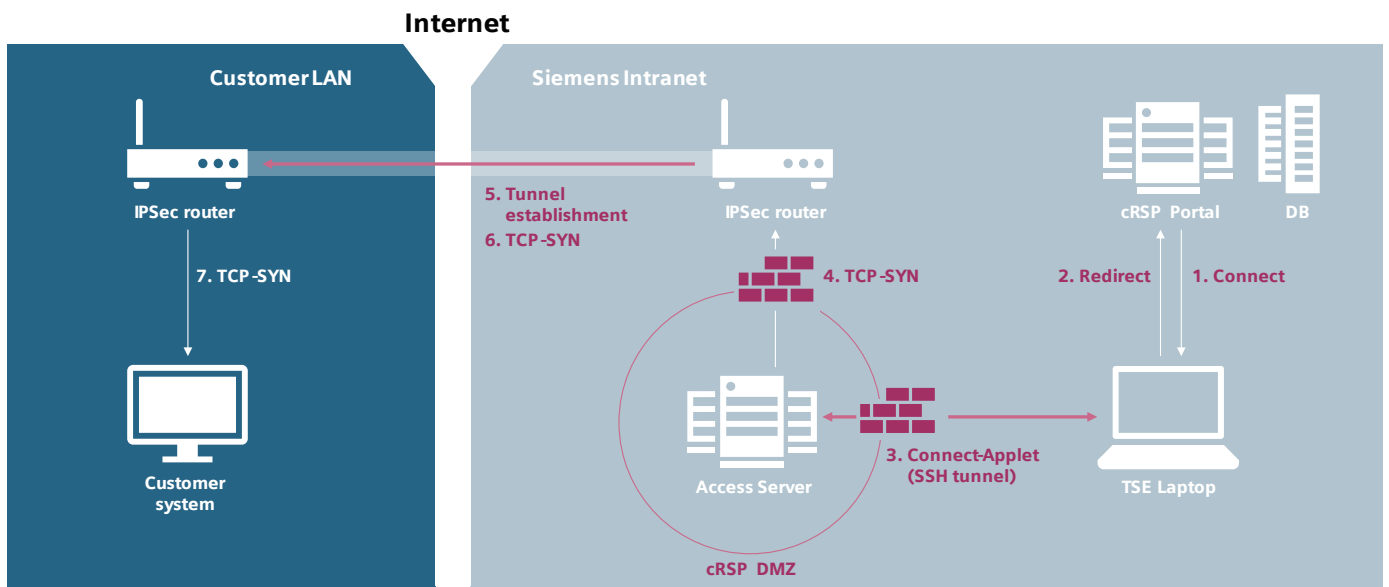
cRSP always uses a secure VPN tunnel over a broadband internet connection. This offers the following advantages: a maximum level of security, high data transfer rates, high availability.



Security measures for IPsec

Siemens uses the established standard IP Security (IPSec) with preshared secrets for encrypted and authenticated data transmission. A minimum recommended configuration is: Preshared secrets consist of an arbitrary string of minimum 12 random characters. The Internet Security Association and Key Management Protocol (ISAKMP) is used to exchange securely encryption key

information. Encrypted secure payload (ESP) ensures data confidentiality through an AES-256 encryption while the SHA2 hash method offers integrity and authenticity of your data. Diffie Hellman key exchange with a key size of 2048 bit (group 14) is used for key exchange security and Perfect Forward Secrecy (PFS).

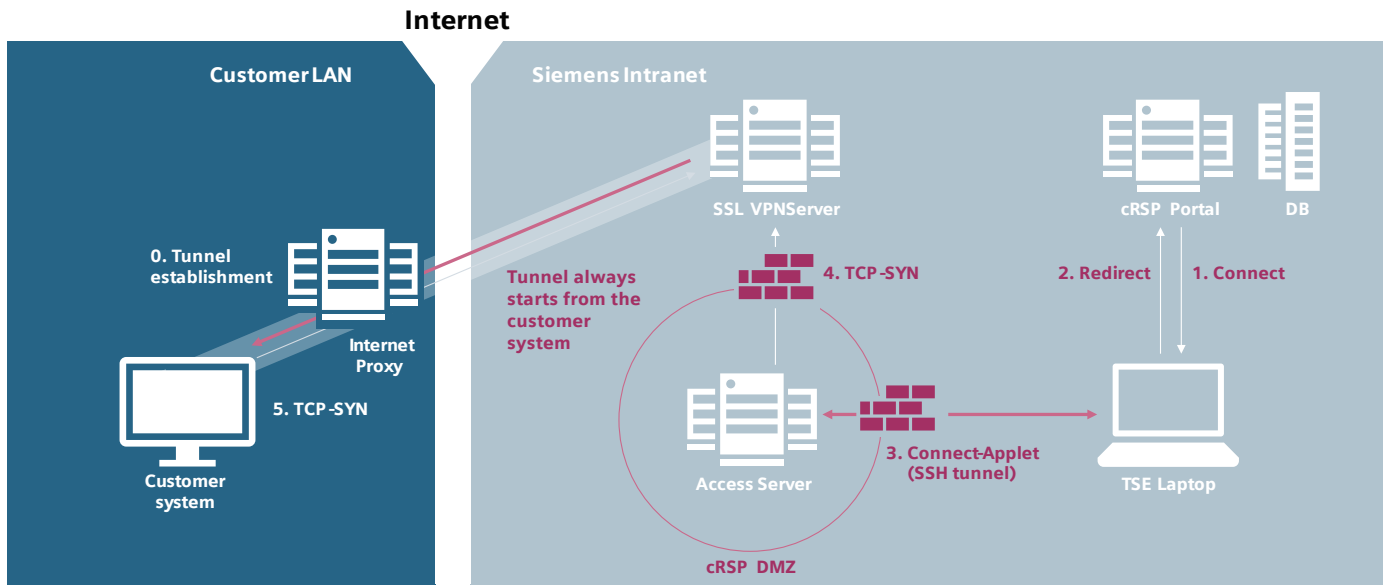


Security measures for SSL-VPN

As an alternative to IPsec VPN Siemens also provides a solution based on SSL VPN (using state-of-the-art TLS 1.3). This solution can be installed on windows or linux (only specific distributions are supported). It is also installed on the DigitalizationBox and on the Remote Solution Gateway.

Before a connection is set up, the device must be registered with a one-time pass-

word (OTP). This OTP is generated using the system's unique data and is valid only for its registration process. The SSL connection to the VPN server can be established only if the server certificate was signed by an internal Siemens Certification Authority (CA). This ensures that only this specific device is able to communicate with the cRSP servers. An additional hardware-based hash ensures that no unauthorized device can set up a connection to the cRSP (system cloning)



Security measures in the customer network

The following section provides a list of the protocols and services used. Should you need any other specific security measures or customized firewall functions for special applications, network segments, etc., they are available depending on your choice of connectivity options.

Protocols

Depending on the product type to be serviced, various protocols are supported by the cRSP secured connection to the customer system

- The HTTP protocol (preferably HTTPS)
- Microsoft Remote Desktop, Telnet, PuTTY, NetOp, WinVNC; Anydesk
- BACnet
- A large range of UDP based connectivity products (e.g. FS20 fire systems)
- Other protocols, if needed
- Ftp/sftp (file transfer protocol, secure file transfer protocol)

Secured cRSP server

Our backend exclusively consists of hardened systems which are designed for stability. Moreover, frequent updates make sure that actively developed distributions remain secure. According to the current state of the art, infections by worms, viruses, Trojan horses and other attacks therefore remain highly unlikely. In addition, our secured cRSP servers as well as the encrypted databases on these servers are in accordance with the most recent security guidelines. The effectiveness of these protection measures is audited (ISO/IEC 27001:2013) on a regular basis ensuring that the cRSP servers are operated with state-of-the-art technology.

CloudFIMs : Putting good data to great use

A smarter approach to energy efficiency and equipment reliability

Could your building be more energy efficient?

Operating buildings in an energy efficient way is becoming increasingly important. Quite often, poorly performing equipment remains undiscovered for long periods of time, resulting in businesses spending too much on energy. Today, tenants expect more from their buildings. User experience, comfort and a heightened awareness of sustainable energy practices are putting more pressure on building owners. Simultaneously, building owners face pressure to lower operating costs. Adopting a more modern approach to building operations can deliver significant savings. In fact, energy efficiency measures can result in energy savings of 30 percent for HVAC.

CloudFIMs from Siemens offers a smarter approach

To overcome these problems, building owners and operators are seeking new data driven approaches that more proactively identify issues and address them based on their potential impact. CloudFIMs, use performance data and trends from the building automation system to identify Facility Improvement Measures (FIMs) which can be implemented remotely for immediate savings. By identifying and correcting schedule and programming issues, buildings maintain an energy efficient and continuously optimized environment.

Highlights

Leverage cloud-based analytics from Siemens to proactively identify Facility Improvement Measures (FIMs) and implement them remotely to maintain an efficient and continuously optimized environment.

Key benefits

- Reduce OPEX spending by proactively identifying energy and operational efficiency improvement measures
- Improve equipment reliability and reduce risks associated with costly downtime.
- Reduce total cost of building ownership
- Prioritize possible improvement measures based on business impact
- Take actions remotely and ensure issue resolution is quantified

Equipment options available

- Air Handling Units (AHUs)
- Boiler plant
- Chiller plant (KPI monitoring)

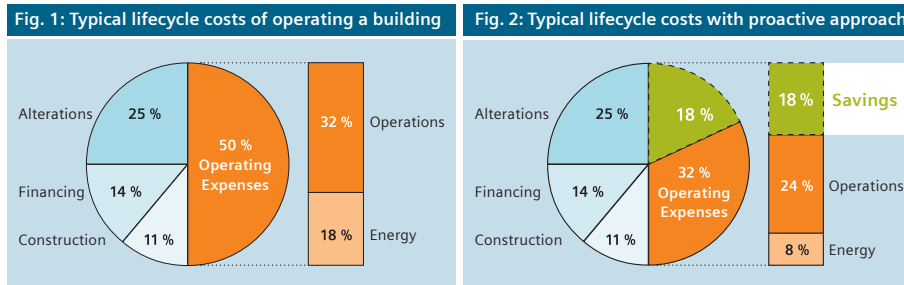


더 알아보기



Controlling the cost of ownership and enabling savings

Over the 40-year lifecycle of a building, the cost to operate the building and for the energy it consumes accounts for 50 percent of the building's total cost (Figure 1). Research shows that building owners and operators who take a more proactive and comprehensive approach to building maintenance, which includes CloudFIMs from Siemens, can reduce a building's overall cost of ownership by roughly 18 percent (Figure 2).



Sources: Association of Energy Engineers, Lawrence Berkeley Labs

Using the latest in building analytics from Siemens Navigator, CloudFIMs focus on the most common facility issues and enables remotely implemented actions that proactively and decisively achieve your desired results. Navigator also delivers the CloudFIMs dashboards which give customers visibility into building performance by deploying a robust set of analytics to track and report operational issues, and track savings that result from remote corrections.

How CloudFIMs deliver energy savings impact

CloudFIMs have been carefully crafted to show quick, high-impact energy savings results, and includes repairs that can be identified and diagnosed remotely. CloudFIMs can detect and proactively improve a wide range of facility improvement measures (FIMs):

CloudFIM	Description
AHU – Heat recovery shows a low efficiency or isn't working	Heat recovery can reduce up to 70 percent of the heating or cooling energy for an air handling unit depending on the indoor and outdoor conditions
AHU – Simultaneous heating and cooling prevention	Prevents reheating and recooling air simultaneously, which can save up to 20 percent of a facility's energy
AHU – Overventilation prevention	Prevents heating or cooling outside air for no reason and protect customers from draft. This can save up to 15 percent of an AHU's energy costs including electricity, heating and cooling energy
Boiler – Low efficiency prevention	Reducing the boiler temperature or the return temperature can increase the energy efficiency of the heat generation by up to 10 percent
Boiler – Identification of a bad hydraulic behaviour	A good hydraulic balance in the heating loop increases boiler efficiency by up to eight percent and improves comfort
Chiller – Increasing the chilled water setpoint	Increasing the setpoint temperature of a chiller can enable more free cooling (reduce the operation time of a chiller) and increase the chiller performance of three percent/°C.
Chiller – Reducing the cooling water setpoint	Reducing the cooling water setpoint increases the performance of a chiller to one percent/reduced °C
Chiller – Low efficiency prevention	Monitoring and maintaining the inlet and outlet temperatures in the right range, increase the efficiency and the life cycle of a chiller.

Navigator

The cloud-based energy and asset management platform

Analyze data

- Leverage advanced fault detection and diagnostic capabilities
- Identify inconsistencies and possible root causes
- Gain transparency into equipment and building performance

Create actionable insight

- Identify possible actions to improve performance
- Prioritize actions based on cost-effectiveness and impact
- Quantify the expected benefits and any potential risks

Secure, flexible remote connection

- Flexible – Siemens can connect wirelessly, via VPN client, virtual network, or separate network connection.
- Secure – ISO 27001 Certification applies to VPN client and virtual networks to specify the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.



Connect X200

CXG3.X200

Connect X200 for the cloud integration of Siemens Smart infrastructure as well as third-party systems

-
- 2-port Ethernet switch for LAN (incl. Daisy Chaining)
 - 1-port Ethernet for WAN
 - 2 EIA-485 interfaces
 - USB interface for 4G dongles
 - Operating voltage AC 24 V or DC 24 V
 - Mounting on standard rails or on the wall
 - Plug-in screw terminal blocks
 - Multi-site management (depending on firmware)
 - Remote operation & monitoring (depending on firmware)
 - Alarm treatment (depending on firmware)
 - Remote tool access, update and configuration via Siemens Cloud Services (depending on firmware)

Functions

Connect X200 provides two integration levels for connecting devices to the cloud: System integration (between the Connect X200 and the devices) and cloud integration (between the Connect X200 and the cloud).

A broad range of devices can be integrated on the system level (i.e. Desigo, FS20, third-party systems). Connect X200 supports various protocols (BACnet, Modbus,) and different media (Ethernet, serial EIA-485 bus).

The device supports Ethernet and 4G on the cloud level via the MQTT protocol.

The specific set of supported functions may vary according to the region (for example UL markets) and according to the connected system. Detailed information about the latest supported functions can be found in the release notes of the installed software.

Functions

Connect X200 is a physical device that is the connecting point between the cloud and controlled/monitored devices, such as controllers, sensors, and actuators in the building.

The device integrates common BACnet/IP or Modbus/TCP devices and systems as well as Siemens fire system protocols.

It securely transmits data to the cloud over cable networks or over mobile networks (e.g. 4G: With a router). 4G USB Dongle support is available in addition (see "Accessories").

Type summary

Type	Order number	Description
CXG3.X200	S55842-Z131-A100	Connect X200

Equipment combinations



Accessories

The accessories listed below are tested but not sold by Siemens Smart Infrastructure.

Manufacturer	Type	Description
Siemens	6EP3332-6SB00-0AY0	Power supply DC 24 V / 2.5 A
Verizon	USB730L / MC730	4G USB Dongle
Huawei	E3372 / E3372h - 153	4G USB Dongle
Huawei	E3372 / E3372h - 320	4G USB Dongle
Alcatel	IK40V-2AALDE1	4G USB Dongle



Please confirm compatibility of the chosen 4G Dongle according to the infrastructure of your regional Internet Service Provider before choosing and ordering a specific device (i.e. compatibility of regional 4G frequency bands). Consult 4G Dongle-Setup (A6V12059208) for further instructions and information.


Technical and mechanical design

The compact build can be mounted on standard rails or walls.

1	Plastic housing
2	LEDs for communication and status
3	Service button
4 a)	2-port Ethernet switch with 2 LEDs per port
4 b)	1-port Ethernet interface with 2 LEDs for WAN (Internet access)
5	Plug-in terminal blocks with screw terminals Power supply
6	USB interface for 4G dongles
7	Plug-in terminal blocks with screw terminals COM1 / COM2
8	DIP switches for bus termination and polarization (COM1 / COM2)
9	Slider for mounting on standard mounting rails
10	Eyelets for cable ties
11	Holes for wall mounting
12	Date / Series and Serial number

LED indicators

Activity	LED / Interface	Color	Activity	Function
	Ethernet 1...3	Green	Continuously ON Continuously OFF Flashing	Link active No connection Network traffic
		Yellow	Continuously ON Continuously OFF	Link 100 Mbps Link 10 Mbps
<ul style="list-style-type: none"> ■ RUN ■ COM1 TX ■ COM1 RX ■ APPS ■ COM2 TX ■ COM2 RX ■ SVC 	RUN	Green	Continuously ON Continuously OFF Flashing	Device operational Device not operational Start-up or program halted
		Red	Continuously OFF Continuously ON Rapid flashing	OK HW or SW fault - power off and on the X200 Firmware missing/application corrupt
		Blue	Continuously ON Continuously OFF Flashing	Connection to the cloud OK No connection to the cloud Onboarding to cloud not finished or device certificates not updated
	APPS	Green	Continuously OFF Continuously ON Flashing	No app(s) installed on the device Installed app(s) are properly working Installed app(s) are (re)starting
	SVC	Red	Continuously OFF Continuously ON	IP address not assigned to LAN port IP address assigned to LAN port
	COM1 / 2 TX	Yellow	Flashing	Communication
	COM1 / 2 RX	Yellow	Continuously OFF	No communication to subsystem

Activity	LED / Interface	Color	Activity	Function
 SVC	Service button		Long press, up to 30s (power off device first)	Press and hold button, restart and wait until RUN LED is steady green and then release button. A factory reset will be performed. All configuration data/installed apps are deleted.
			Short press	IP address 169.254.169.254 will be assigned to LAN port for the duration of 15 min.



Product documentation

Related documents such as the environmental declarations, CE declarations, etc., can be downloaded from the following Internet address:

www.siemens.com/bt/download

Notes



Safety

 CAUTION	
	<p>National safety regulations</p> <p>Failure to comply with national safety regulations may result in personal injury and property damage.</p> <ul style="list-style-type: none"> Observe national provisions and comply with the appropriate safety regulations.


Mounting position and ambient temperature

The devices can be snapped onto standard rails or screwed onto a flat surface. Plug-in screw terminals connect power and interfaces (except for Ethernet).


Ambient temperature -5...50 °C (23...122 °F)	Ambient temperature -5...45 °C (23...113 °F)
<ul style="list-style-type: none"> Wall, horizontal <ul style="list-style-type: none"> From left to right From right to left 	<ul style="list-style-type: none"> Overhead Wall, vertically <ul style="list-style-type: none"> From top to bottom From bottom to top On a horizontal surface

 CAUTION	
	<p>Risk of overheating for failure to comply with ambient temperature</p> <p>Burning and damage to the device</p> <ul style="list-style-type: none"> Ensure sufficient ventilation to comply with the permissible ambient temperature within the panel or installation box. The temperature must be at least 10K (18° F) lower outside the installation box.


Installation

⚠ WARNING	
	<p>Electric shock</p> <p>Incorrect installation of the device may lead to electric shock injuries when touching the device!</p> <ul style="list-style-type: none"> • Install the device in a lockable cabinet or use terminal covers. • Do not install the device in locations where children are likely to be present. • Conductors with a cross-section of 0.5 mm² (AWG24) or greater shall comply with the requirements of IEC 60332-1-2 and IEC 60332-1-3 or IEC TS 60695-11-21.

Commissioning / service

NOTICE	
	<p>When using a 4G dongle</p> <p>Reboot the device after a 4G dongle has been connected. For details see 4G Dongle Setup (A6V12059208).</p>

Disposal

	<p>The device is considered an electronic device for disposal in accordance with European Directive and may not be disposed of as domestic waste.</p> <ul style="list-style-type: none"> • Use only designated channels for disposing the devices. • Comply with all local and currently applicable laws and regulations.
---	---

Technical data

Power supply

Operating voltage 24 V AC (24 V _~ , ⊥, ⚡)	AC 24 V -15 / +20 % (SELV / PELV) or AC 24 V Class 2 (US) 48...63 Hz
Operating voltage 24 V DC	DC 24 V -15 / +20 % (SELV / PELV) or DC 24 V Class 2 (US)
Functional ground (US) Functional earth ⚡	The terminal for the functional ground must be connected on the installation side with the building grounding system (PE).
Screw terminals for wire cross sections up to	Max. 2.5 mm ² (14 AWG)
Internal fusing	2.5 A irreversible / non-replaceable
External supply line fusing (EU)	Non-renewable fuse max. 10 A slow or circuit breaker max. 13 A Tripping characteristic B, C, D per EN 60898 or Power supply with current limitation of max. 10 A

Power consumption (for supply planning)

Power consumption AC	16 VA
Power consumption DC	8 W

Function data

Hardware information	
Processor	NXP i.MX8 DualX
Storage	2 GB RAM 8 GB eMMC

Data backup in the event of power failure
Super cap to support real-time clock (7 days).

Interfaces

Ethernet interfaces	
Plug	3 x RJ45, shielded
Interface type	10Base-T / 100Base-TX, IEEE 802.3 compatible
Bit rate	10/100 Mbps, autosensing
Protocol	BACnet on UDP/IP and HTTPs on TCP/IP
Cabling, cable type	10 Mbps: Min. CAT3, shielded cable is recommended 100 Mbps: Min. CAT5, shielded cable is recommended
Cable length	Max. 100 m (330 ft)

Screw terminals, plug-in	
Cu-wire or Cu-strand with wire end sleeve	1 x 0.6 mm \varnothing to 2.5 mm ² (22 to 14 AWG) or 2 x 0.6 mm \varnothing to 1.0 mm ² (22 to 18 AWG)
Cu-strand without wire end sleeve	1 x 0.6 mm \varnothing to 2.5 mm ² (22 to 14 AWG) or 2 x 0.6 mm \varnothing to 1.5 mm ² (22 to 16 AWG)
Stripping length	6...7.5 mm (0.24...0.29 in)
Screwdriver	Slot screws, screwdriver size 1 with shaft \varnothing = 3 mm
Max. tightening torque	0.6 Nm (0.44 lb ft)

EIA-485 interfaces	
Interface type	EIA-485, electrically isolated
Baud rate	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 (depending on the configuration)
Internal bus termination	120 Ohm, switchable with DIP switch

EIA-485 interfaces	
Internal bus polarization	270 Ohm pull-up/pull-down resistances, switchable with DIP switch
Cabling (in-house cabling only) Cable length	3-wire cable Max. 1000 m (3300 ft)
Protection	Short-circuit proof Protection against faulty wiring with AC 24 V and DC 24 V

USB interface (4G internet connection)	
Plug	Type A
Interface type	USB 2.0
Bit rate	480 Mbit
Max. load	500 mA
Max. cable length	5 m

Conformity

Ambient conditions and protection classification	
Classification as per EN 60730 Automatic action Control function Degree of pollution Overvoltage category	Type 1 Class A 2 III
Design	Suitable for use in protection class I or II systems
Degree of protection of housing to EN 60529 Front parts in DIN cut-out Terminal part	IP30 IP20
Climatic ambient conditions <ul style="list-style-type: none"> Storage / Transport (packaged for transport) as per IEC EN 60721-3-1 / IEC EN 60721-3-2 Operation as per IEC/EN 60721-3-3 	<ul style="list-style-type: none"> Class 1K22 / 2K12 Temperature -25...70 °C (-13...158 °F) Air humidity 5...95 % (non-condensing) Class 3K23 Temperature -5...50 °C (23...122 °F) (for details see chapter Mounting) Air humidity 5...95 % (non-condensing)
Mechanical ambient conditions <ul style="list-style-type: none"> Transport per IEC/EN 60721-3-2 Operation as per IEC/EN 60721-3-3 	<ul style="list-style-type: none"> Class 2M4 Class 3M11

Standards, directives and approvals	
Product standards	EN 60730-1 and EN 62368-1
Product family standard	EN 50491-x
Electromagnetic compatibility (EMC)	For residential, commercial, and industrial environments
EU conformity (CE)	See CE declaration ¹⁾

Standards, directives and approvals	
EAC compliance	Eurasian compliance
RCM conformity	See RCM declaration ¹⁾
UL/cUL approbation (US / Canada)	UL916; http://ul.com/database
CSA certification	C22.2, http://csagroup.org/services-industries/product-listing
Environmental compatibility ¹⁾	The product environmental declaration ¹⁾ contains data on environmentally compatible product design and assessments (RoHS compliance, materials composition, packaging, environmental benefit, disposal).

¹⁾ Documents can be downloaded at <http://siemens.com/bt/download>.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation

FCC Caution: Changes or modifications not expressly approved by Siemens Switzerland Ltd. could void user authority to operate the equipment. United States representative <https://new.siemens.com/us/en/products/buildingtechnologies/home.html>

Industry Canada statement

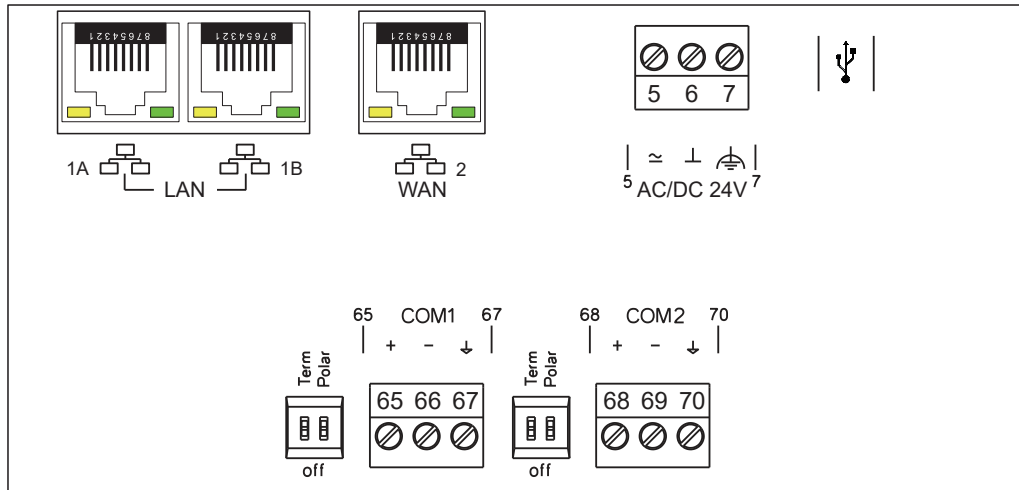
This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Housing

Color top/bottom	RAL 7035 (light grey) / RAL 7016 (anthracite grey)
Dimensions	per DIN 43 880, see dimensions
Weight with/without packaging	350 g / 300 g

Connection terminals



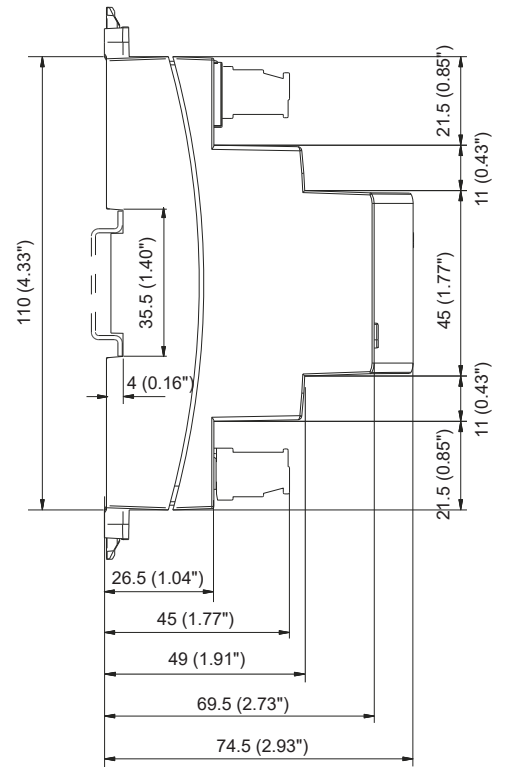
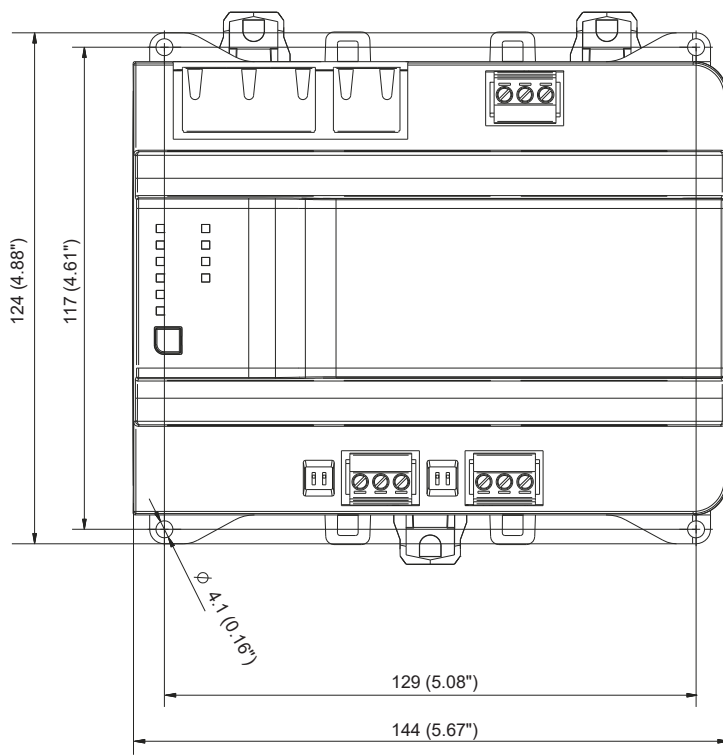
Terminal	Symbol	Description
1A, 1B		2 x RJ45 interface for Ethernet with switch LAN (customer network)
2		1 x RJ45 interface for Ethernet WAN (internet access)
5, 6	≈ , ⊥,	Operating voltage AC 24 V, DC 24 V
7		Functional ground (must be connected on the installation side with the building grounding system (PE)).
USB		USB interface for 4G dongles
Term	on, off	Switch for bus termination
Polar	on, off	Switch for polarization
65, 66, 67	COM1	Interfaces EIA-485
68, 69, 70	COM2	

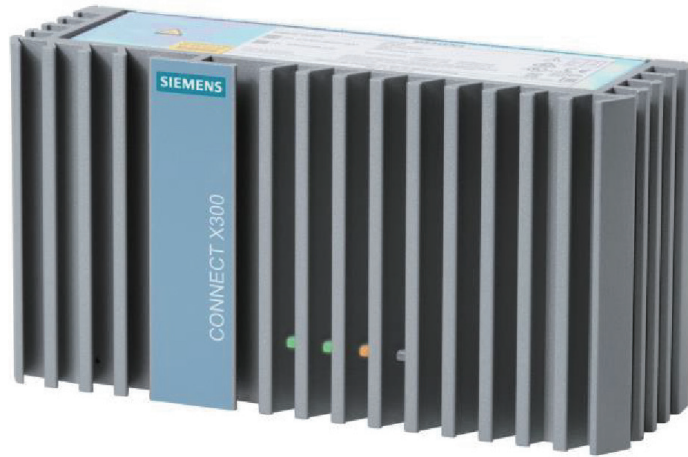
Warranty

The application-specific technical data is guaranteed only in combination with the Siemens products listed in the 'Device combinations' section. If third-party products are used, any guarantee provided by Siemens will be invalidated.

Dimensions

All dimensions in mm and inches





Connect X300

CXG3.X300

Connect X300 for the cloud integration of Siemens Smart Infrastructure as well as third-party systems

- 2 Ethernet ports for WAN and LAN
- Remote firmware and configuration data update over the IP Interface
- LED indication of activities and state
- Operating voltage DC 24 V =
- Plug-in screw terminal block for supply
- Mounting on standard rails or on wall

Depending on firmware, the following functions are supported (examples):

- Multi-site management
- Remote operation & monitoring
- Alarm treatment
- Remote tool access

The specific set of supported functions may vary according to the region (for example UL markets) and according to the connected system.

Features

Connect X300 is a physical device that is the connecting point between the cloud and controlled/monitored devices. This can include controllers, sensors, and actuators in the building etc.

Application

The device integrates BACnet/IP or Modbus/TCP devices and systems as well as FS20 fire panels.

It securely transmits data to the cloud over cabled networks or over mobile networks (e.g. 4G: With a router). 4G USB Dongle support is available in addition (see “Accessories”).

Functions

The Connect X300 provides two integration levels to connect devices to the cloud: System integration (between the Connect X300 and the devices) and cloud integration (between the Connect X300 and the cloud).

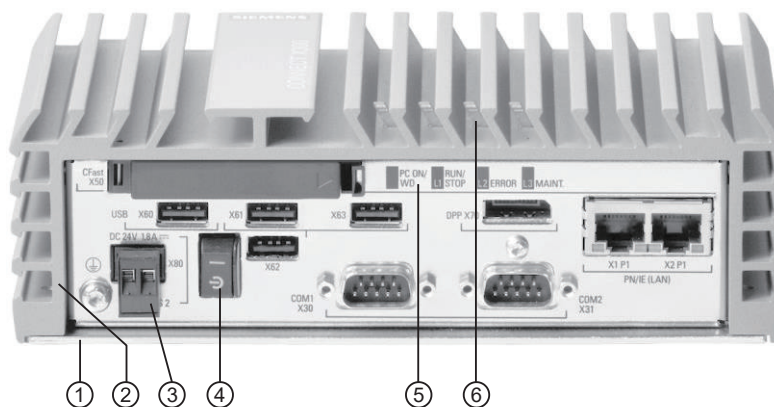
A broad range of devices can be integrated on the system level (Desigo, FS20, third-party systems). It supports various protocols (BACnet, Modbus) and various physical media (Ethernet, serial EIA-485 bus).

The device supports Ethernet and 4G on the cloud level via the MQTT protocol.

Technical design/mechanical design

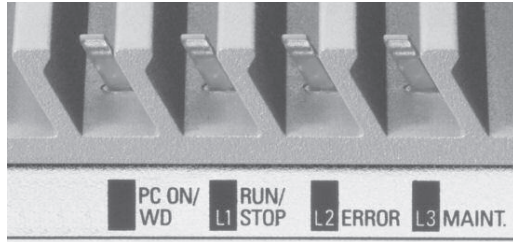
Mechanical design

The device can be mounted on standard rails and walls.



- 1 Base plate
- 2 Cooling fins, aluminum
- 3 Connection: Power supply (**DC 24 V=**)
- 4 Main switch
- 5 Labeling of LED indicators on the front
- 6 LED indicators on the cover (light guides)

LED displays



LED	Activity	Function
PC ON/ WD	Off	Device off
	Orange flashing	BIOS in Power On Self Test (POST)
	Solid Green	Device ready (otherwise re-start the device)
L1 RUN / STOP	Green, flashing	SW applications starting
	Solid Green	All SW application operational
L2 ERROR	Off	Approx. 1 minute off during start-up
	Solid Orange	Internet OK
	Orange flashing	X300 is registered properly and Cloud connection is OK.
	Off	No internet connection
L3	-	Not used

	LED	Color	Activity	Function
	Ethernet 1/2	Green	Steady ON	Link active
			Steady OFF	No connection
			Flashing	Sends 10 or 100 Mbps Ethernet IP packets
		Yellow	Steady ON	Link: 100 Mbps
			Steady OFF	Link: 10 Mbps

Type summary

Device	Type	Description
CXG3.X300	SSN: S55842-Z121-A100	Connect X300

Delivery

Pluggable terminal block for power

Mounting accessories for mounting on standard rails.

Accessories

The accessories listed below are tested but not sold by Siemens Smart Infrastructure.

Manufacturer	Type	Description
Siemens	6EP3332-6SB00-0AY0	Power supply DC 24 V =
Siemens	BR2450A/SCN	Lithium battery with cable and plug 3 V, 0.55 Ah (BIOS backup battery, replace every 5 years)
Verizon	USB730L / MC730	4G USB Dongle
Huawei	E3372 / E3372h - 153	4G USB Dongle
Alcatel	IK40V-2AALDE1	4G USB Dongle

Please confirm compatibility of the chosen 4G Dongle according to the infrastructure of your regional Internet Service Provider before choosing and ordering a specific device (i.e.


compatibility of regional 4G frequency bands). Consult “4G Dongle Commissioning Guide” for further instructions and information.

Product documentation

All relevant documents can be downloaded at the following Internet address:
<http://siemens.com/bt/download> (Enter type CXG3.X300).

Notes

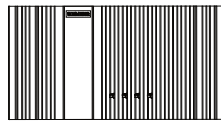
Safety

	<p>⚠ CAUTION</p>
	<p>National safety regulations</p> <p>Failure to comply with national safety regulations may result in personal injury and property damage.</p> <ul style="list-style-type: none"> Observe national provisions and comply with the appropriate safety regulations.
	<p>High temperature on device surface during operation (to 70 °C / 158 °F)</p>

Mounting

The device is suitable for mounting on standard rails.

Mounting position and temperature range

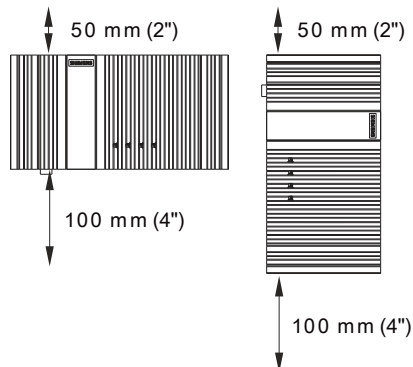


Max. 50 °C (122 °F)

Min. 0 °C (32 °F)

Provide sufficient ventilation in the control cabinet to maintain the ambient temperature (max. 50 °C) and extract residual device heat (up to 32 W).

Required space around the device



Commissioning

Only qualified personnel may commission the device.

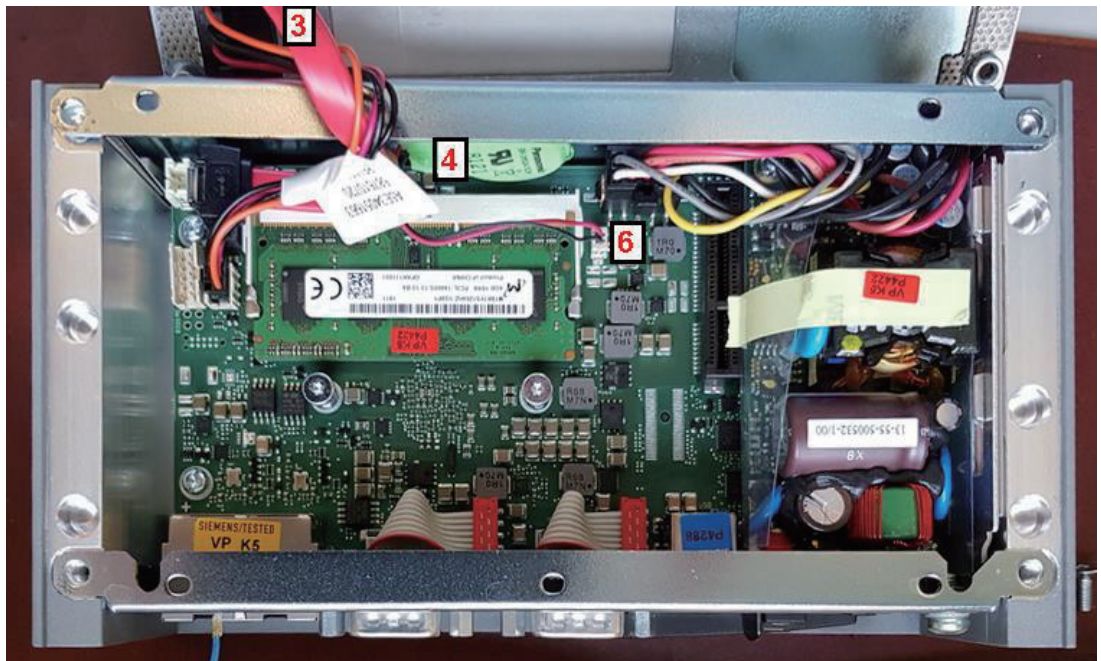
Additional documentation: See <http://siemens.com/bt/download>

**Maintenance:
Replace battery**

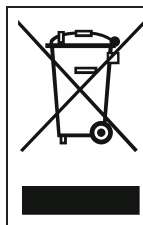
The BIOS backup battery is installed ex works and must be replaced **every 5 years**. See accessories for type number.

Procedure:

1. Assure protection against electrostatic discharge (ESD).
2. Disconnect device from power.
3. Unscrew 6 screws on the base plate (T20) and carefully remove the base plate.
4. Disconnect the ribbon cable on the SSD (not on the motherboard).
5. Remove the battery from the housing wall.
6. Remove the remaining Velcro strips from the housing wall.
7. Unplug the old battery.
8. Carefully install the new battery
(The realtime clock information is lost after 30 seconds without power). In this case, plug in the WAN cable at start up for the device to acquire the time from the Internet).
9. Attach the new battery with the new Velcro strip to the housing wall.
10. Plug in the ribbon cable on the SSD.
11. Reinstall the base plate (maximum torque: 5 Nm / 3.7 lbf ft).



Disposal





The device is considered an electronic device for disposal in terms of the European Directive and may not be disposed of as domestic waste.

- Dispose of the device through channels provided for this purpose.
- Comply with all local, applicable regulations.
- Dispose of empty batteries in designated collection points

Technical data

Power supply

Operating voltage (M, L+)	DC 24 V = $\pm 20\%$ Safety extra-low voltage SELV per IEC/EN / DIN EN / UL 60950-1 or NEC Class 2 or LPS per IEC/EN / DIN EN / UL 60950-1
 DC 24 V = Direct current only!	
Protective earth  Cross section min. 2.5 mm ² / 14AWG	The protective earth connection must be connected on the installation side with the building grounding system (PE).
Power consumption	Max. 1.8 A / 43 W at DC 24 V = Typically 510 mA / 13 W
Internal fusing	None

Function data

Hardware information	
Processor	Intel Celeron N2807, dual core, 1,58 GHz
RAM	4 GB DDR3L
SSD	128 GB, 2.5" SATA

Software information	
OS	Linux

Response to a power outage	
Loss of power buffering	20 ms
BIOS backup battery	

Connections

Power: Pluggable screw terminals,	
Cu-wire or Cu-strand with wire end sleeve	0.75 to 2.5mm ² (28 to 14 AWG)
Cu-strand without wire end sleeve	0.75 to 2.5mm ² (28 to 14 AWG)
Stripping length	6...7.5 mm (0.24...0.29 in)
Screwdriver	Slot screws with a ca. 3 mm blade
Max. tightening torque	0.6 Nm (0.44 lb ft)

Ethernet interfaces	
Plug	2 x RJ45, screened
Interface type	10 / 100 / 1000 Mbps, IEEE 802.3 compatible
Galvanic isolation of system neutral M	Yes

USB interface (Unused)	
Plug	Type A
1 x USB3.0	4 Gbps, 900 mA
3 x USB 2.0	0.48 Gbps, 500 mA
Max. load for all USB consumers	Max. 6 W
Galvanic isolation of system neutral M	No

Serial interface (Unused)	
2x COM	D-sub plug, 9-pin
Protocol	EIA-485
Bit rate	Max 115 Kbps

Screen interface (Unused)	
1x DisplayPort	640 x 480 ... 2560 x 1600 Pixel

Conformity

Ambient conditions and protection classification	
Design	Protection class I per IEC 61140
Degree of protection of housing to EN 60529	IP40
Dust protection	Against foreign particles ≥ 1 mm
Climatic ambient conditions <ul style="list-style-type: none"> Transport (packaged for transportation) to EN 60721-3-2 Operation as per IEC/EN 60721-3-3 	<ul style="list-style-type: none"> Temperature -20...60 °C (-4...140 °F) Air humidity 5...95% (non-condensing) Temperature 0...50 °C (32...122 °F) Air humidity 5...85% at 30 °C (86 °F) (non-condensing)
Mechanical ambient conditions <ul style="list-style-type: none"> Transportation Operation (standard rails) 	<ul style="list-style-type: none"> 5 ... 9 Hz: 3.5 mm, 9 ... 500 Hz: 9.8 m/s² 10 ... 58 Hz: 0.075 mm, 58 ... 200 Hz: 4.9 m/s²
Air pressure.	1080...795 hPa, -1000...2000 m (-3000...6000 ft)

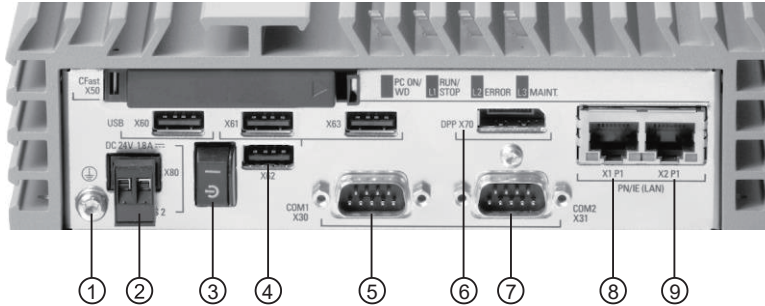
Standards, directives and approvals	
Product standard IT devices - Security	EN 60950-1 through 06/2019 (then EN 61010-2-201)
Electromagnetic compatibility (EMC) Emissions Immunity	For residential, commercial, and industrial environments EN 61000-6-3 EN 61000-6-2
EU conformity (CE)	See CE declaration A5W00052529 ¹⁾
EAC conformity	Eurasia conformity
RCM	Meets EN 61000-6-3
UL, cULus-LISTED (US / Canada)	Underwriters Laboratories (UL) to Standard UL 60950-1 Second Edition, File E115352 (I.T.E) UL 508 (IND.CONT.EQ), File E85972 Canadian National Standard CAN/CSA-C22.2: No. 60950-1-07 CAN/CSA-C22.2: No. 142 Identical to the authorized Listee's model numbers - SIMATIC IPC227E http://ul.com/database
FCC	CFR 47 Part 15 Class A CAN ICES-3 (B)/NMB-3(B)
Environmental compatibility ¹⁾	The product environmental declaration contains data on environmentally compatible product design and assessments (RoHS compliance, materials composition, packaging, environmental benefit, disposal).

¹⁾ Documents can be downloaded at <http://siemens.com/bt/download>.

Housing

Dimensions	See "Dimensions"
Weight without / with packaging	1590 g / 1940 g

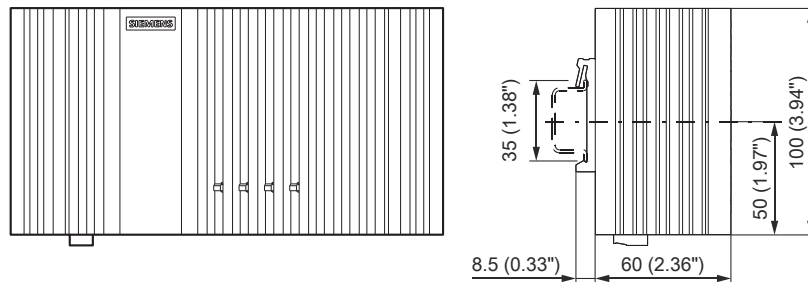
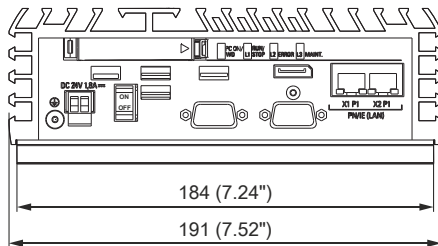
Connections and indicators



- 1 Protective earth The protective earth connection must be connected on the installation side with the building grounding system (PE). Diameter min. 2.5 mm2 /14 AWG
- 2 Pluggable terminal block for operating voltage **DC 24 V =**
- 3 On/off switch. OFF, when pressing symbol "C-"
- 4 USB 2.0, 3.0 interfaces (unused)
- 5 Serial interface, 9-pin for RS 232, EIA-422, EIA-485 (unused)
- 6 DisplayPort interface (unused)
- 7 Serial interface, 9-pin for RS 232, EIA-422, EIA-485 (unused)
- 8 X1P1 = LAN (customer network) Ethernet 10/100/1000 Mbps (with 2 LEDs per port for indicators)
- 9 X2P1 = WAN (Internet access) Ethernet 10/100/1000 Mbps (with 2 LEDs per port for indicators)

Dimensions

Dimensions in mm and inches

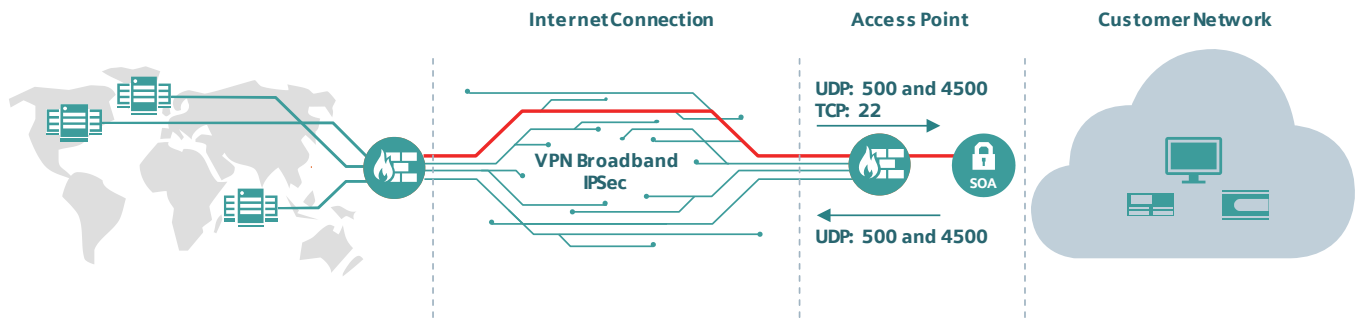


cRSP IT Security Concept - Appendix

IPsec

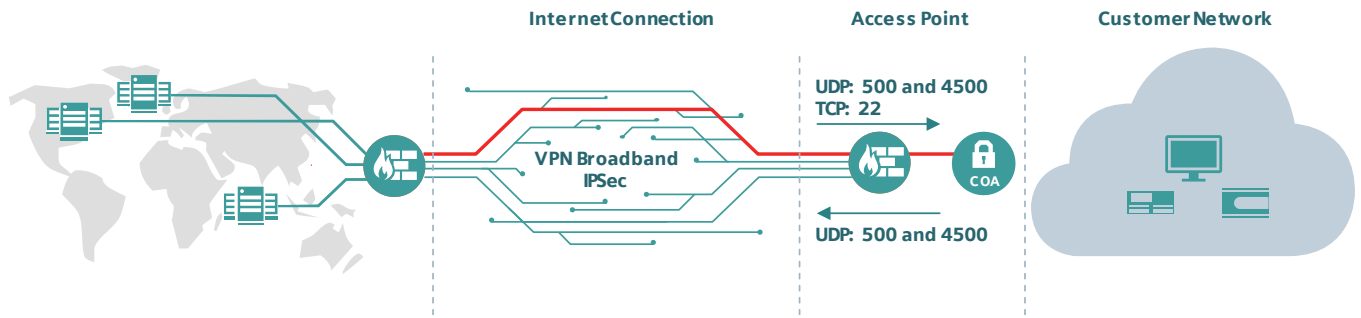
Siemens Owned Access

Connection between cRSP infrastructure and customer network is performed through a router provided by Siemens.



Customer Owned Access

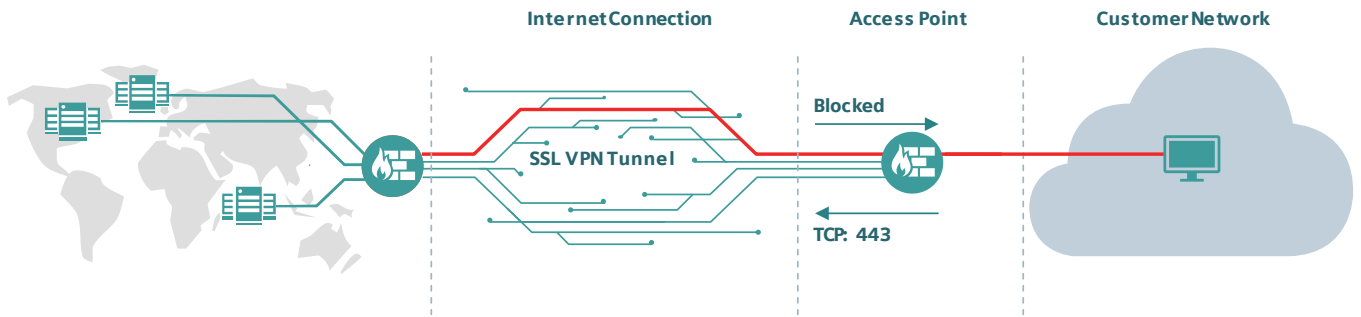
Connection between cRSP infrastructure and customer network is performed through a customer router or it ends at the customer's firewall.



SSL VPN

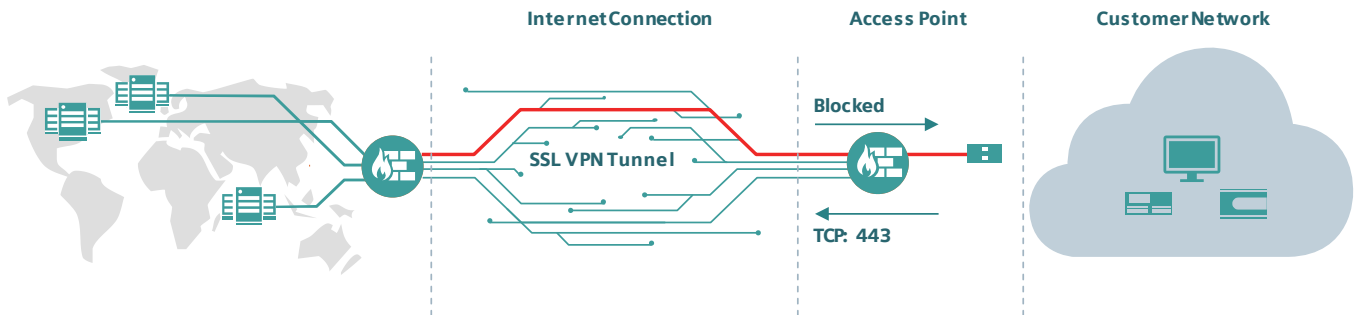
Internet Based Connection

Each equipment is connected to cRSP through internet and utilizes a secure SSL VPN tunnel. Access to internet is provided by the customer.



DigitalizationBox/Remote Solution Gateway

Connection between cRSP infrastructure and customer network is performed through a router provided by Siemens.. Access to internet is provided by the customer or over a mobile connection.



본 브로셔에서 제공되는 정보에 대한 제 3자의 임의의 사용은 소유주의 권리를 침해할 수 있으며 모든 제품 명칭은 Siemens AG 또는 공급업체의 제품명 또는 상표일 수 있습니다.

지멘스(주)
스마트 인프라
03155 서울특별시 종로구 종로3길 17 디타워 10층
Tel: 02) 3450-7302
Fax: 02) 3459-7359
www.siemens.co.kr/si

Smart Infrastructure intelligently connects energy systems, buildings and industries, enhancing the way we live and work to significantly improve efficiency and sustainability.

We work together with customers and partners to create an ecosystem that both intuitively responds to the needs of people and helps customers achieve their business goals.

It helps our customers to thrive, communities to progress and supports sustainable development to protect our planet for the next generation.

Creating environments that care.
siemens.com/smart-infrastructure