# Siemens common Remote Service Platform (cRSP)

**Support for your systems – whenever you need it**

**siemens.com/bt/services**

**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 and 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

# Maximum security – complete control

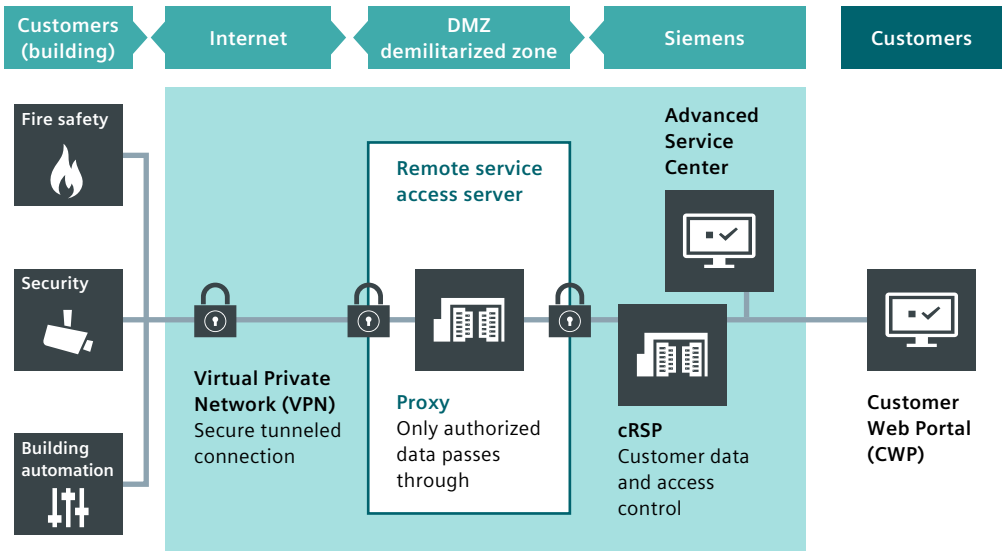
**Customer-controlled access**
We have established a secure external operation option so that you can gain access from outside of the Siemens network as well. This means that you always have full control over remote access to your systems. You can explicitly block access to particular targets if necessary 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.




Article no. BT_0124_EN
(Status 06/2020)

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.