SIEMENS

# Improve service levels with Siemens remote support

## Better asset availability and less risk of system downtime

### A new way of delivering service

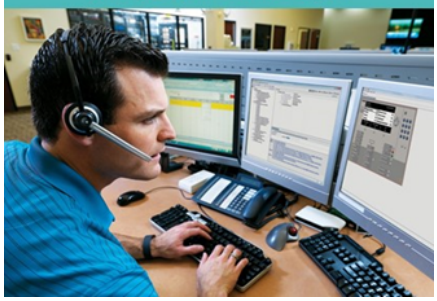
Siemens now provides an extensive range of new digital services via remote connection; these provide seamless support to improve the performance, availability and efficiency of your building automation, security, fire safety and IoT systems.

Our common Remote Service Platform (cRSP) creates a secure, managed connection enabling access to your systems, and facilitating a mix of remote and manned response to enhance delivery of our services.

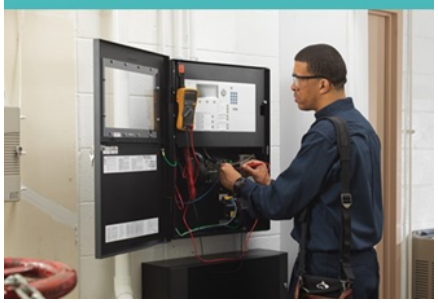
### How can I benefit?

- Reduced risk of downtime with faster, more efficient diagnostics
- Improved fix rates with remote repair and periodical system monitoring
- Manpower efficiencies as engineers arrive on-site fully supported, well-informed and suitably equipped
- Better system information via detailed reports including all testing and event history
- Enhanced intelligence from analysis of faults and trends
- Greater system resilience with cyber system health checks

Support engineer can diagnose faults and perform remote repair



Engineer despatched with right skills and parts needed to fix fault



### What are my options?

We will work with you to ascertain the right access model for your business; typical examples include:

- **Connection on request:** your system can be accessed via individual requests and requires your approval, e.g. a service technician can request access for a single remote session in order to clear a specific fault.
- **Supervised access:** enables you to follow the service technician's activity on your system in real time.
- **Outbound communication:** your system sends information to the Siemens Service Centre via the cRSP platform, in real time or at agreed intervals, enabling collection of statistical data for system optimisation and proactive fault management.
- **Full access:** authorised service engineers have your permission to connect to the system at any time and each access is automatically logged to enable full visibility of activity. You can receive an automatic email at the start and end of each remote session.

# Improve service levels with Siemens remote support

### Will I be cybersafe?
The platform ensures cybersecurity by default, using an encrypted connection, two factor authentication and data protection principles at its core.

### Will qualified people support me?
Our service technicians fully understand the importance of confidentiality when managing customer data and are trained in data protection, IT security and validation processes.

### Will the platform remain available?
The performance of our cRSP platform is guaranteed by three fully redundant data centres to ensure it remains unaffected and provides the highest possible availability of our remote services.

### How will you keep me informed?
Siemens is always able to update you on engineer activity, who has had access to which data, and when and what communications were performed on each system. This audit trail is enabled by the following measures:

- Every single access to a customer system is recorded
- Entry and exit time stamps as well as the engineer's identity are applied
- Report logs are kept on file for at least twelve months, and retention may be extended at your request

### How is system access managed?
- Each direct access to your system is recorded in the cRSP platform and provided with a time stamp
- The log also records the unique user ID of the service technician
- Siemens issues digital IDs for employees via a Public Key Infrastructure (PKI); every time a service technician logs into the cRSP portal, their access rights are verified based on PKI smart card
- The access models you define are then mirrored within our cRSP platform and converted into authorised IT system access levels
- These access levels are then matched to the service technician's verified identity

### Why Siemens for remote access?
Siemens was one of the world's first organisations to implement an internationally valid Information Security Management System (ISMS) according to ISO/IEC 27001 for remote services.

The Siemens Cyber Emergency Response Team (CERT) is an internal, independent and trusted partner which develops preventive security measures and evaluates the information security of the IT infrastructure. Our cRSP platform is audited regularly for effective protection and continuous improvements.

### Who we are and what we do
Siemens Smart Infrastructure RSS is a global business with specialist skills in delivering advanced security, fire safety and energy management solutions. Our capabilities include product manufacture, software integration, system design, turnkey installation and lifecycle support.

We focus on building long term partnerships with our customers to gain insight into their building management, safety, security and sustainability objectives, supporting their requirement for specialist knowledge and enabling a technology and services roadmap that recognises efficiencies and cost savings.

Our service portfolio is designed to help customers meet their challenges, deliver against stringent KPIs and ensure a high level of asset availability. Digital services are enabling us to deliver new corrective and preventive service models, coupled with continuous system performance monitoring and cyber health checks.


Siemens plc, Smart Infrastructure Buildings
Pinehurst 2, Pinehurst Road, Farnborough,
Hampshire, GU14 7BF
**Sales enquiries: 0844 892 1033 option 4**
Tel: 01276 696111
**Email: smart-spaces.gb@siemens.com**

**Let's talk about how we can monitor, maintain and service your systems securely and efficiently. Subject to system review, we can take the next steps towards smarter service delivery.**