Customer Web Portal

Access your own system whenever you need it.

Our Customer Web Portal puts the power of the Internet to work for you. You’ll be able to access your own fire protection, safety, security or building automation system any time from anywhere using our remote connection and your credentials. Once logged in, you’ll have access to your equipment and can make changes as if you were working directly on site on a management station. With 24/7 access, you can nip potential problems in the bud so that system availability is maintained.

siemens.com/bt/services
Secure access when you need it.

Save time with remote services
The Customer Web Portal uses the same remote connection that has been set up for our specialists. This secure connection gives you access to your systems and enables you to capture and/or adjust the most important parameters. With such ready access, you’ll be able to take a proactive approach so you can catch problems before they escalate, optimizing equipment uptime and increasing system performance.

Be independent
You can connect to the Customer Web Portal from anywhere you have the Internet. You’ll have 24/7 access to your equipment across all your locations. We also provide useful tools that can increase your productivity.

Customer-controlled access
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 United States ensure optimal availability of the Customer Web Portal.

Global support organization
Our specialists are available if you have questions or need additional support.

IT security
We ensure the highest level of security for the Customer Web Portal by conducting regular audits and maintaining ISO/IEC27001 information security approval.

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

cRSP
To read more about Siemens common Remote Service Platform (cRSP), please click on the following link to download the cRSP flyer: https://sie.ag/2jHU272

Published by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel +41 58 724 24 24

For the U.S. published by
Siemens Industry Inc.
100 Technology Drive
Alpharetta, GA 30005
United States

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.

© Siemens 2020