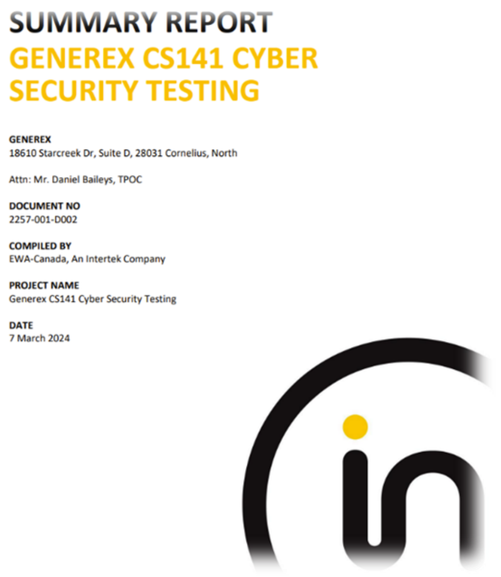
GENEREX User Manuals

English – Cyber Security Guide

Secure Your Systems with the CS141/BACS and This Hardening Guide



SUMMARY REPORT

GENEREX CS141 CYBER SECURITY TESTING

GENEREX
18610 Starcreek Dr, Suite D, 28031 Cornelius, North

Attn: Mr. Daniel Baileys, TPOC

DOCUMENT NO
2257-001-D002

COMPILED BY
EWA-Canada, An Intertek Company

PROJECT NAME
Generex CS141 Cyber Security Testing

DATE
7 March 2024

The CS141/BACS offers you extensive possibilities to implement your personal cybersecurity concept. Even in its basic configuration, the device guarantees a high level of security, which is compliant for use in high-security areas, according to UL2900.1.

With this hardening guide, we want to show you how to optimally utilize the diverse configuration options of the CS141/BACS to:

- Seamlessly integrate your CS141/BACS into your existing security concept without compromises
- Ensure comprehensive operational security for your systems

This guide provides a compact overview of all necessary steps. Detailed configuration instructions and tutorials, such as certificate creation, can be found in the official user manual for the CS141/BACS.

Benefits of the CS141/BACS for Increased Device Security:

- ✓ **High security standards:** The CS141/BACS meets stringent security requirements and is certified complying with UL2900.1 for use in high-security areas.

- ✓ **Comprehensive configuration options:** The device offers a variety of settings to adapt it to your individual security needs.

- ✓ **Regular security updates:** The manufacturer provides regular security updates to protect devices from new threats.

- ✓ **Certified hardware:** The CS141/BACS is based on certified hardware that prevents manipulation and unauthorized access.

With this hardening guide and the CS141/BACS, you are on the best path to comprehensively protect your systems from cyberattacks.

Table of Content

What is cybersecurity all about?

In common parlance, people often talk about "cybersecurity" while referring to a specific device that is supposed to provide "cybersecurity." In fact, however, "cybersecurity" is a much broader concept that goes far beyond simply securing individual devices.

This includes:

- Network topologies
- Access points to the network (laptops, computers, ports)
- Firewall solutions
- Password security
- Virus scanner
- Cleanly installed certificates
- Training of employees and users
- Reporting of hacker intrusions (depending on the area and the depth of the intrusion)
- Regular security audits and security screenings
- Self-critical handling of found abnormalities caused by one’s own fault

Attention companies: Cybersecurity is mandatory!

Both German federal laws and the EU-wide **European Cybersecurity Act (CSA)** require companies to take appropriate measures to ensure network security. This obligation aims to protect companies and their data from cyberattacks that can result in serious financial and reputational losses.

The specific requirements and legal regulations for network security vary depending on the country, industry and company size. In principle, however, the required measures include technical and organizational aspects such as the installation of firewalls and anti-virus software, training and raising awareness of cybersecurity among employees and the creation of emergency plans.

Companies that do not comply with these legal requirements must expect heavy fines. The implementation of cybersecurity measures is therefore not only a legal obligation, but also an investment in protecting corporate assets.

The CS141 is compliant with UL 2900.1 and meets or exceeds all security requirements stipulated by the USA and the EU. With the Cyber Security Guide, we want to help the operator to configure the CS141 / BACS in such a way that, in addition to optimal performance, all required IT security requirements can be met in the best possible way.

CS141 / BACS Hardening Guide

Each product of the CS141 product family (CS141/HW161 WEBMANANAGER, SITEMANAGAER and -MONITOR 6, BACSKIT B4) delivers numerous functions with standardized “out of the box” settings:

- Predefined and general ports
- If possible, pre-installed default certificates
- Quickly configured web access
- Commonly known standard passwords
- Standard community name (for example, “public” or “private” for SNMP)
- And much more …

Due to this fact, these devices can be set into operation and ported to an existing network in a short time and, above all, without in-depth knowledge of network and system administration if the according infrastructure follows generally accepted conventions.

However, a standardized out-of-the-box configuration also has the disadvantage that a network-compatible device cannot be considered "safe" in terms of cybersecurity, regardless of the manufacturer or its function, since just a glance at the manufacturer's manual can reveal many interesting features that can be used to eavesdrop on or even infiltrate a critical network part.

This manual is intended to show you what you can adjust to massively increase operational reliability.

Tip:

This hardening guide describes, among other things, how to adjust ports - before making any changes, be sure to check whether the ports you want to use are both, free and available to avoid the risk communication problems. Please note that port changes must be implemented network-wide, depending on the intended use.

Not all options or “recommended settings” presented here are necessarily compatible with your network or can be implemented 1:1 within the framework of the IT security guidelines on site. Be sure talking to the responsible system administrator or the according department beforehand!

General recommendations:

1. Change passwords regularly
2. Do not leave backups unprotected on the network and minimize the circle of authorized persons
3. Note the validity of the certificates used
4. Use the latest firmware or check regularly for new firmware versions that provide improvements and new security options

Part 1: General User Registration Recommendations

All devices in the CS141 product family offer 2 basic login methods, which can be combined if desired. Both methods have their respective advantages and disadvantages:

Local user management:

The CS141 distinguishes between the name and the "user role". The only user that is specified by the hardware and cannot be deactivated is the user "admin" with the user role "Super User":

All other users can be changed, adjusted and deleted:

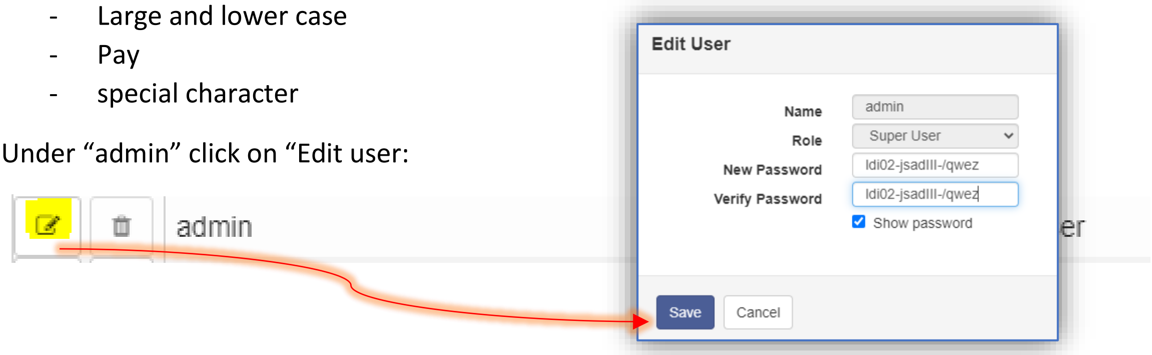
Password recommendation:

1. Change the password for the super user “admin” to block the default administrator access.

The basic rule for a secure password is:

- Approx. 8-16 characters
- Large and lower case
- Pay
- special character

Under “admin” click on “Edit user:



Edit User

Name: admin
Role: Super User
New Password: Idi02-jsadIII-/qwez
Verify Password: Idi02-jsadIII-/qwez
☑ Show password

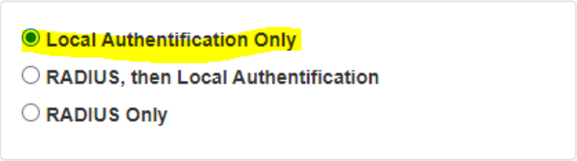
This is the first step towards operational security; only the user “admin” with a cryptic password is active and can log in to the device.

Block user roles that are not needed.

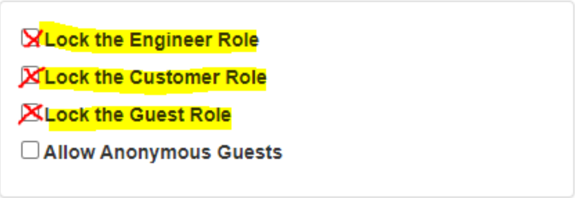
If you lock the user role, a user assigned to this role will no longer be able to log in.

Special feature Anonymous Guest:

This function is deactivated by default and is allowed when the checkbox is checked. The Anonymous Guest is only required if you use a UNMS or have implemented direct display of the monitoring screens using an i-Frame or similar.

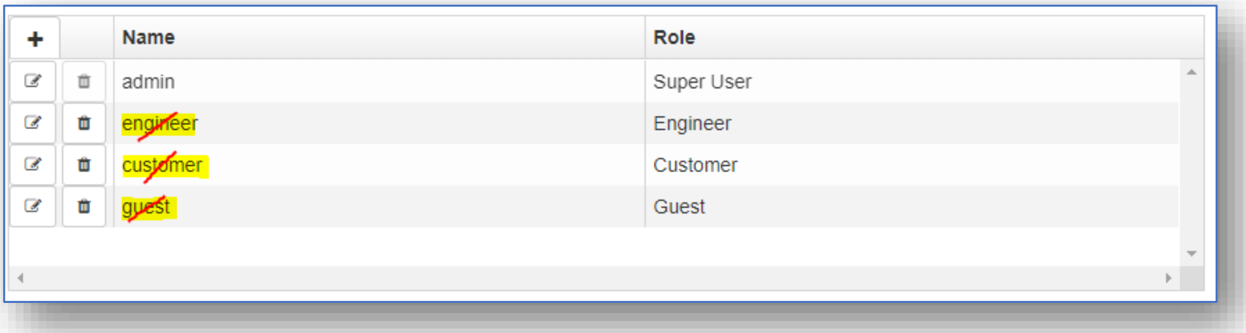


● Local Authentification Only
○ RADIUS, then Local Authentification
○ RADIUS Only



☒ Lock the Engineer Role
☒ Lock the Customer Role
☒ Lock the Guest Role
☐ Allow Anonymous Guests

Tip:
To "look", a user with the user role "guest" is sufficient. The user "Customer" can not only "look" but also download log files, but nothing else.



+		Name	Role
✎	🗑	admin	Super User
✎	🗑	~~engineer~~	Engineer
✎	🗑	~~customer~~	Customer
✎	🗑	~~guest~~	Guest

2. Delete or change username and password:

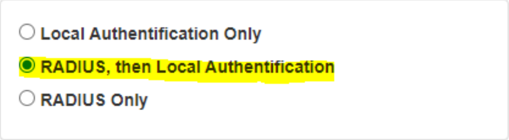
Change both the name and password for the factory default users “engineer”, “customer” and “guest”.

Network-managed passwords and usernames

All devices in the CS141 product family offer the option of managing user management via a RADIUS server starting with firmware 2.04. This enables two different security concepts:

Access-optimized security: RADIUS, then local user authentication

In this mode, user authorization is managed exclusively via a RADIUS server, as available. If the RADIUS server does not respond, you can log in using a locally managed user - access to the configuration menus is always guaranteed.



○ Local Authentification Only
● RADIUS, then Local Authentification
○ RADIUS Only

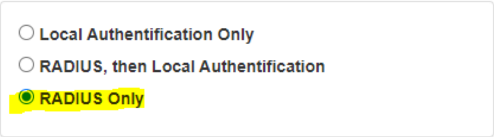
Recommendation for maximum security:

1. Deactivate the user roles you do not need
   Unnecessary user roles distributed by the RADIUS server are then rejected by the CS141.
2. Change or delete the local factory default users.
   If the RADIUS server cannot be reached, only locally stored users apply.
3. Configure the CS141 to use RADIUS then Local User Authentication.

Tip:

In this operating mode, you must manually change the locally stored passwords cyclically!

Cyber security optimized security: Exclusive RADIUS mode



○ Local Authentification Only
○ RADIUS, then Local Authentification
● RADIUS Only

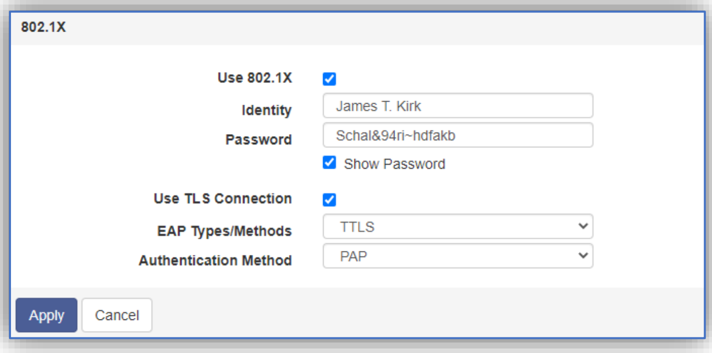
In this operating mode, the local user database is completely deactivated in regular operating mode and only users managed by RADIUS are permitted. If you need local access, the slide switch must be set to centre position (configuration mode) and the CS141 must be restarted.

> **Tip:**
>
> The advantage of the exclusive RADIUS login is that you can manage usernames and passwords directly via a central RADIUS server. If the RADIUS server is not accessible, no user can log in. Local access requires exclusive on-site presence.

RADIUS - 802.1X Port Access Entity

Under System>Security you will also find the option to activate access via R802.1X as access control. In this case, access is controlled via the port of the network switch and its configuration.

All encryption and authentication methods currently offered are considered "secure" as of now (April / 2022). If there are new methods, these will be updated accordingly.



802.1X

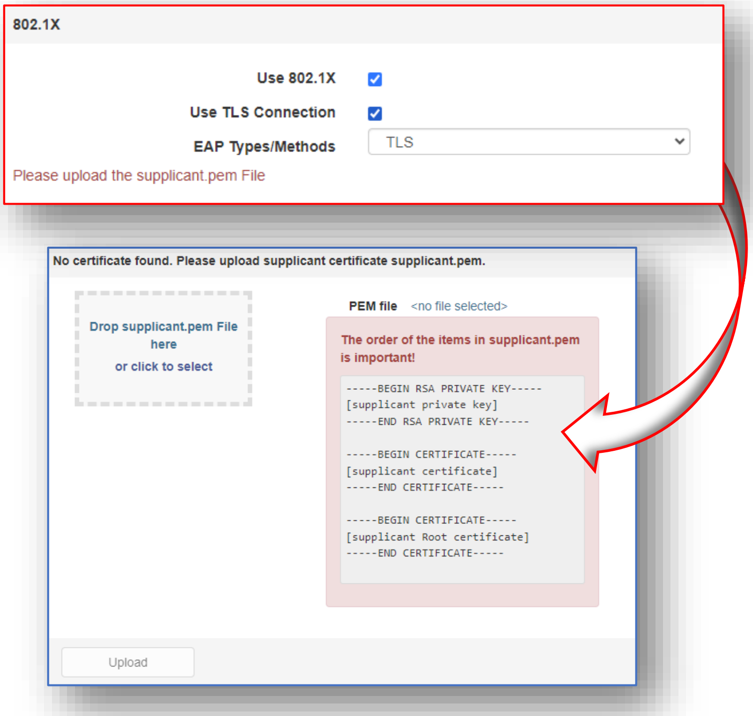
Use 802.1X ☑
Identity: James T. Kirk
Password: Schal&94ri~hdfakb
☑ Show Password
Use TLS Connection ☑
EAP Types/Methods: TTLS
Authentication Method: PAP

Cyber security optimized security: Login via certificate

Where passwords can be entered, there is a risk that they can be read by a keylogger, for example.

If you simply upload a PEM file to for the PAE login, there is no risk, a keylogger my log your keyboard entries:

Set EAP Types/Method to TLS, and load the necessary certificate into the specially protected memory of the CS141 / BACS:



802.1X

Use 802.1X ☑
Use TLS Connection ☑
EAP Types/Methods: TLS

Please upload the supplicant.pem File

No certificate found. Please upload supplicant certificate supplicant.pem.

The order of the items in supplicant.pem is important!

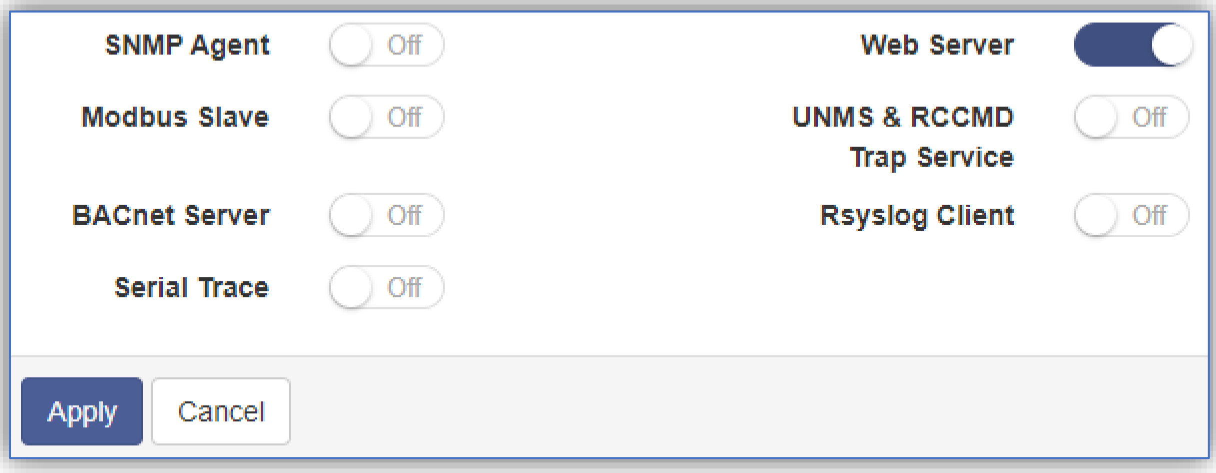
```
-----BEGIN RSA PRIVATE KEY-----
[supplicant private key]
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
[supplicant certificate]
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
[supplicant Root certificate]
-----END CERTIFICATE-----
```

Part 2: System services

Unused but enabled system services may not necessarily be a gateway for hackers, but they pose a latent danger because it is possible to intercept data traffic to for evaluating interesting information about a network this way. All services except the web server are therefore set to OFF by default.

Recommendation for maximum security:

Therefore, turn off unnecessary running services if you do not plan to use them:



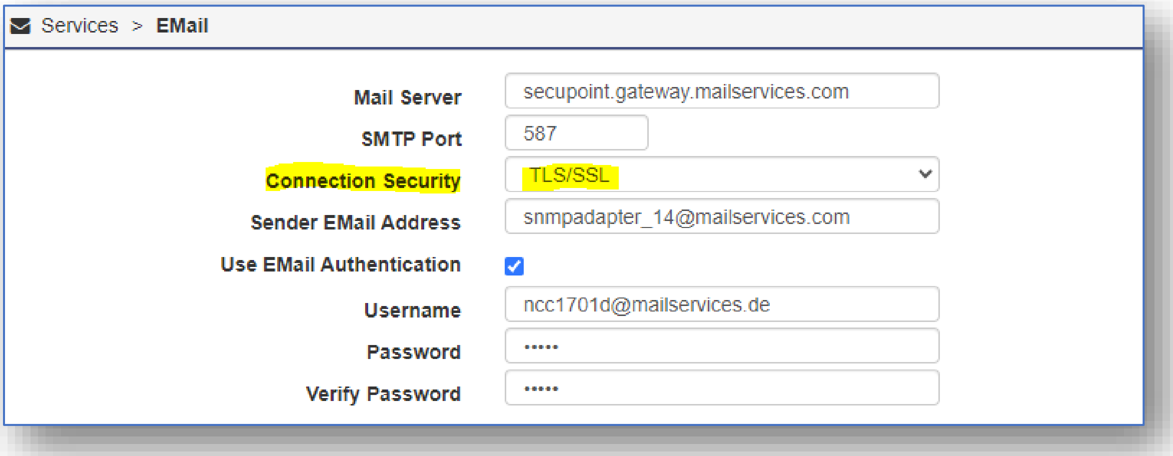
SNMP Agent: Off
Modbus Slave: Off
BACnet Server: Off
Serial Trace: Off
Web Server: On
UNMS & RCCMD Trap Service: Off
Rsyslog Client: Off

The fewer system services that require notification are running in a network, the less data traffic can be intercepted.

Details about the services

The integrated mail client

For maximum security, we recommend using an internal mail server to prevent status messages from being processed and tracked by 3rd party service providers. For the CS141, we recommend using TLS/SSL to directly encrypt the communication between the CS141 and the mail server.

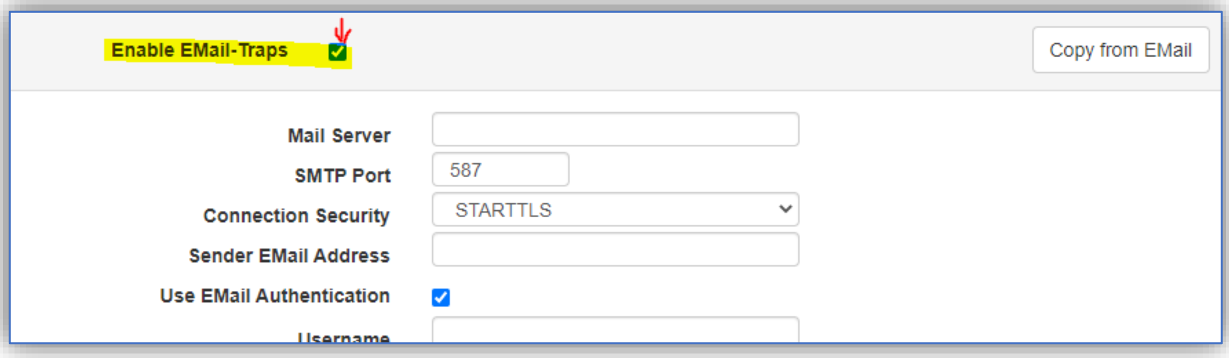


Services > EMail

Mail Server: secupoint.gateway.mailservices.com
SMTP Port: 587
Connection Security: TLS/SSL
Sender EMail Address: snmpadapter_14@mailservices.com
Use EMail Authentication: ☑
Username: ncc1701d@mailservices.de
Password: •••••
Verify Password: •••••

Email Traps

Email Traps is a unique function from GENEREX to send status information about a UPS via mail to a monitoring system. This function is only needed if a UNMS is in used that holds functionality. In all other operating scenarios, uncheck "Enable EMAIL-Traps" to prevent email traffic with UPS data.



Enable EMail-Traps ☑

Mail Server

SMTP Port 587

Connection Security STARTTLS

Sender EMail Address

Use EMail Authentication ☑

Username

Recommendation for mail traps:

Turn off email traps if you are not using UNMS. They will only send unnecessary data via email.

The SNMP Agent

With SNMP (Simple Network Management Protocol), all devices in the CS141 product family offer a standardized and popular option for integration into building management systems. Versions 2 and 3 differ in terms of access security and the access concept.

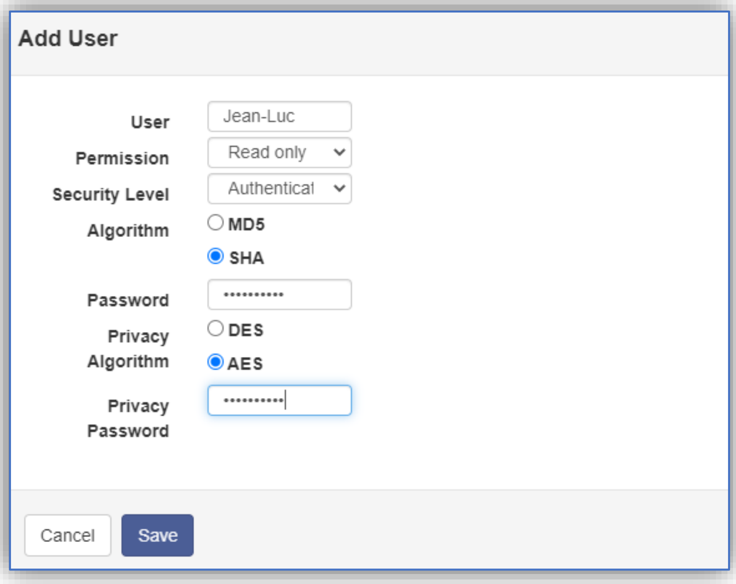
Recommendation for maximum security:

For maximum security, we recommend setting the SNMP agent to **version 3** and setting the permission to **“Read only”.**

SNMP v3 offers a user-based access method where you can freely define the passwords.

All methods offered for securing data traffic are considered “secure” based on the current state of the art (April 2022), but we recommend the SHA / AES combination because they use the more modern encryption methods.

Please note: MD5 / SHA and DES / AES are not compatible with each other. Which method must be configured in this case depends on the network in which you want to operate the CS141.



Add User

User Jean-Luc

Permission Read only

Security Level Authentical

Algorithm ○ MD5 ● SHA

Password ••••••••••

Privacy Algorithm ○ DES ● AES

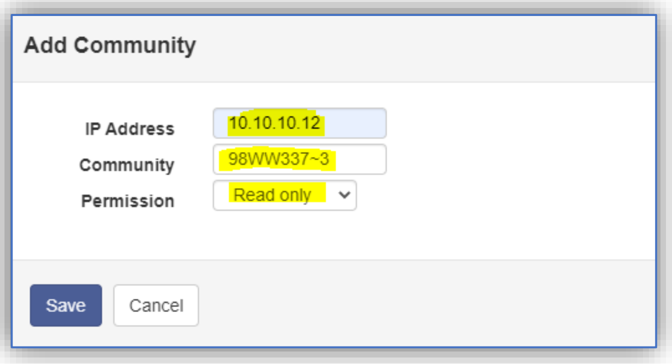
Privacy Password ••••••••••

If you need to use SNMP v2…

SNMP v2 offers access options via communities. In addition, the IP address can be used to define which sender is authorized.

Recommendation for safety with SNMP v2

1. If possible, change the community names (default “public” for reading and “private” for writing)
2. Use the IP address to define which users are authorized to receive data.
3. Set the permission to “read only”.



Add Community

IP Address: 10.10.10.12
Community: 98WW337~3
Permission: Read only

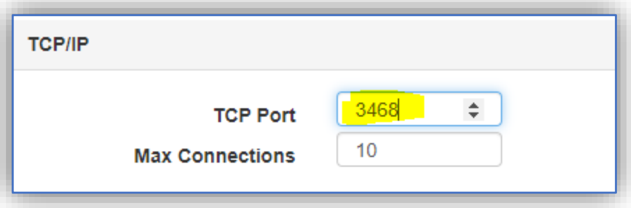
Modbus over TCP

For many years, Modbus has also been able to be queried via TCP, which offers numerous possibilities for connecting a device from the CS141 product family to a building management system and querying status messages. This can provide a lot of interesting information about the operating status of infrastructure measures such as UPS systems or batteries.

By default, port P502 is used.

Recommendation: Change the port

Port P502 is a default setting that many devices use for Modbus, if you change the port you make it more difficult for unauthorized intruders to discover.



TCP/IP

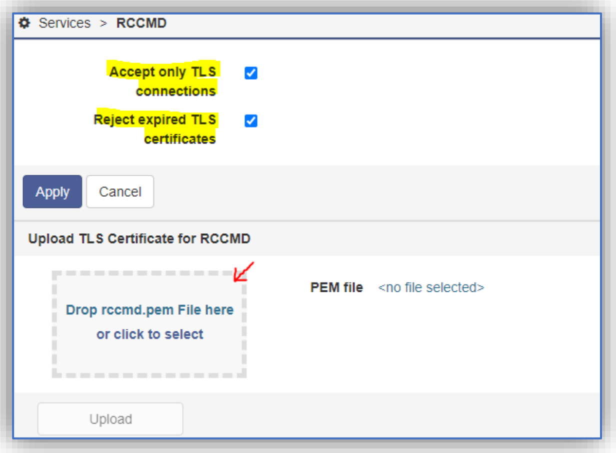
TCP Port: 3468
Max Connections: 10

RCCMD

RCCMD (Remote Control and Command) is a very secure method for informing target systems in the event of an incident and, if necessary, shutting them down automatically.

Normally, RCCMD will remain passive in the background and will not produce any pointless data traffic that could be intercepted. The security provided by the operating mode alone is sufficient in most networks but can be tightened. Recommendation for increasing security:

1. Only allow TLS connections
2. Reject expired certificates
3. Use your own certificate.



Services > RCCMD

Accept only TLS connections ☑
Reject expired TLS certificates ☑

Upload TLS Certificate for RCCMD

PEM file <no file selected>

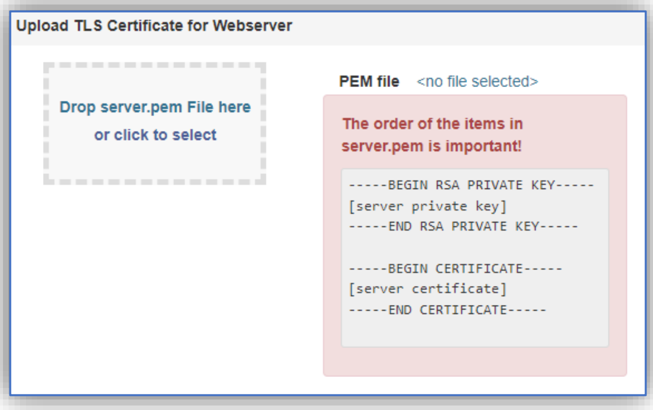
Web server

All devices in the CS141 product family have a modern web interface with a specially hardened web server running in the background. In addition to the configuration interface, the available monitoring screens are also displayed here.

Recommendation for maximum security

1. Set “Force HTTPS”
   This deactivates the standard method via http and communication runs exclusively via the encrypted communication method https.

2. Replace the certificate supplied from the factory with your own certificate.



Upload TLS Certificate for Webserver

Drop server.pem File here
or click to select

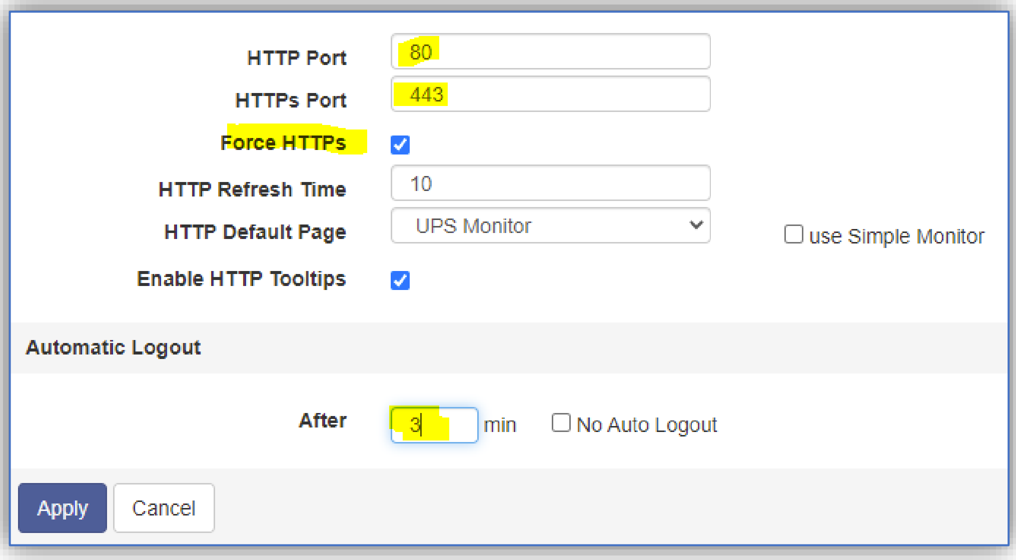
PEM file <no file selected>

The order of the items in server.pem is important!

```
-----BEGIN RSA PRIVATE KEY-----
[server private key]
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
[server certificate]
-----END CERTIFICATE-----
```

3. Change the ports on which the web server runs: By default, the web interface is accessed on port 80 and port 443.

4. Reduce the time window for auto-logout to a minimum to automatically log users out of CS141 as quickly as possible when they are inactive.



HTTP Port: 80
HTTPs Port: 443
Force HTTPs: ☑
HTTP Refresh Time: 10
HTTP Default Page: UPS Monitor ☐ use Simple Monitor
Enable HTTP Tooltips: ☑

Automatic Logout

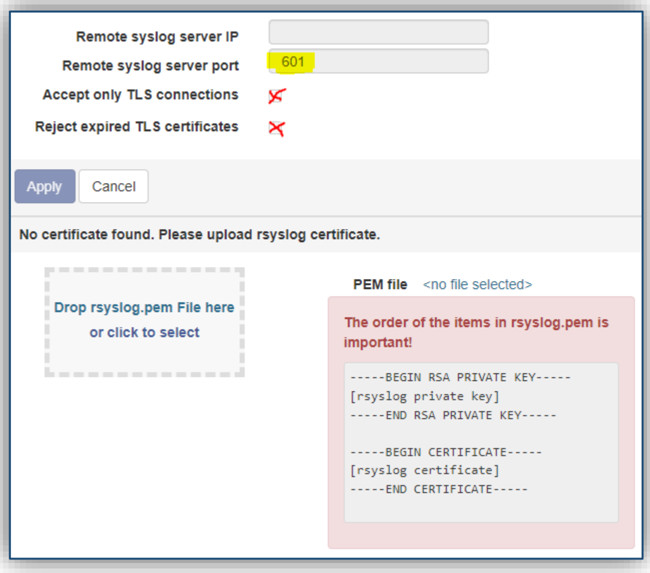
After: 3 min ☐ No Auto Logout

Remote Syslog

By default, the Remote Syslog Client runs on port 601 with a pre-installed certificate. The aim of this service is to store a copy of the locally stored log files centrally in a network, where automatic diagnostic tools can perform numerous evaluations.

Recommendation for maximum security:

- Only enable this function if you use a Syslog Receiver in the network.
- Enable "Accept only TLS connections"
- Reject expired TLS certificates
- Change the port, which is factory defaulted to port 601



Remote syslog server IP:

Remote syslog server port: 601

Accept only TLS connections: ✗

Reject expired TLS certificates: ✗

No certificate found. Please upload rsyslog certificate.

PEM file <no file selected>

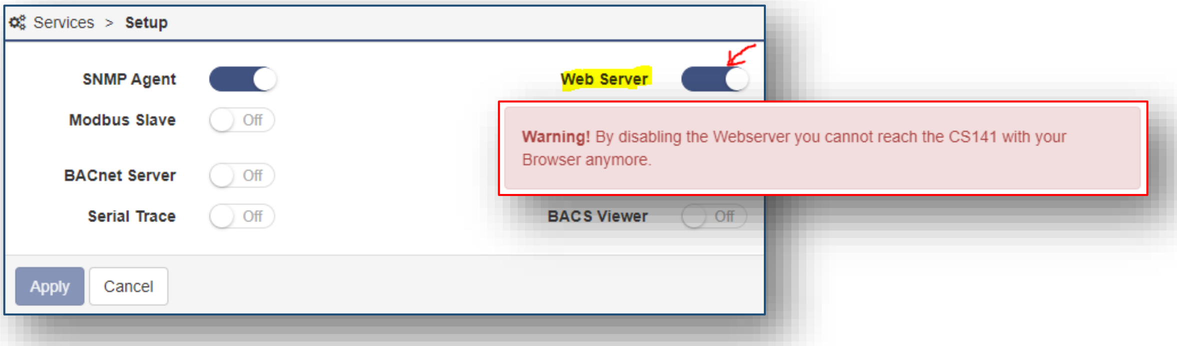
The order of the items in rsyslog.pem is important!

```
-----BEGIN RSA PRIVATE KEY-----
[rsyslog private key]
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
[rsyslog certificate]
-----END CERTIFICATE-----
```

Part 3: How to reject login attempts to manipulate the CS141 / BACS WEBMANAGER

This solution is only used in particularly exposed and therefore vulnerable installations.

All devices in the CS141 product family offer the function of completely "locking down" a device and prohibiting further access via configuration interface or API. Internal watchdogs take on the task of restarting individual services or, if necessary, the entire device.



SNMP Agent: On

Modbus Slave: Off

BACnet Server: Off

Serial Trace: Off

Web Server: On

BACS Viewer: Off

Warning! By disabling the Webserver you cannot reach the CS141 with your Browser anymore.

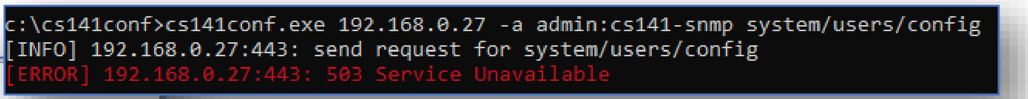
In this case, the device runs autonomously "as configured" – but can no longer be conveniently reconfigured. With this configuration, it is possible to prevent unknown persons from manipulating settings, for example to deliberately sabotage important settings in emergency management.

Important: In this operating scenario, the BACKUP/Restore function plays a central role!

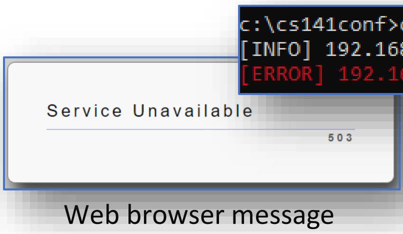
Since default access via the web interface and API is disabled, configuration options are severely limited! To make changes to the configuration, the CS141 must be set and reboot into configuration mode to access the update routine directly via 10.10.10.10/reset. In this operation mode, the update window will only provide a factory reset during flashing to restore the web server service and therefore allow an access the backup/restore – function.

After the adjustments, a new backup must be created before deactivating the web server!

Disabling the web server service will prevent any user access to the configuration menus, either via web browser or via config tool:



```
c:\cs141conf>cs141conf.exe 192.168.0.27 -a admin:cs141-snmp system/users/config
[INFO] 192.168.0.27:443: send request for system/users/config
[ERROR] 192.168.0.27:443: 503 Service Unavailable
```



Service Unavailable

503

Web browser message

CS141 Config Command Line Tool message

Both methods will reject the connection / Login attempt.

Before putting a web manager from the CS141 product family into autonomous mode, be sure to make a backup of your configuration *before disabling the web server* - *In this operating scenario, changes and adjustments to the configuration can only be carried out this way:*

1. Set the slide switch to the middle position (configuration mode) and restart the CS141
2. Use 10.10.10.10/update to open the update dialog directly, and install a firmware update
3. Log in and restore data via BACKUP/ Restore functionality.
4. Make configuration changes
5. Return the slide switch to the desired operating position
6. Test the settings
7. Create a new backup (!)
8. After this, disable the web server and API again.

As soon as the web server has been switched off, the CS141 runs in a fully autonomous operating mode. All configured interfaces and services are available, and it is no longer possible to log in to the CS141/BACS via the network.

Copyright statement on intellectual property and handling of confidential information

The information in this user manual is not intended to be a guarantee of accuracy and is subject to change without notice. Although GENEREX has attempted to provide accurate information in this document, GENEREX assumes no responsibility for the accuracy of this information.

GENEREX shall not be liable for any indirect, special, consequential or incidental damages, including, without limitation, lost profits or revenues, cost of replacement goods, loss or corruption of data arising out of the use of this document or the product described herein.

GENEREX, as the manufacturer of the products mentioned, assumes no liability with this information. The products described in this manual have been given solely as information for business partners to help them gain a better understanding of GENEREX products.

GENEREX authorizes its business partners to transmit the information contained in this document to third parties, as well as to personnel in their company or their own customers, electronically, manually, in the form of photocopies or similar. GENEREX states that the content may not be modified or adapted without the written permission of GENEREX.

All right, title and interest in the GENEREX trademark BACS or logo (registered or unregistered) or the goodwill and/or intellectual property of GENEREX, copyright and product patents are owned exclusively and without restriction by GENEREX.

GENEREX will promptly resolve any complaint regarding the content of this document. Comments or complaints regarding this document should be addressed to GENEREX Systems Vertriebsgesellschaft mbH.