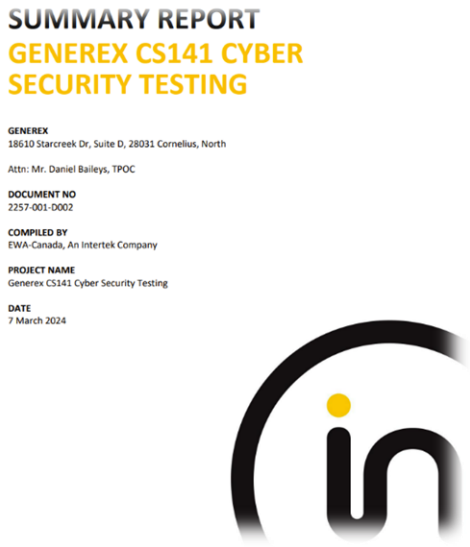
GENEREX Benutzerhandbücher

Deutsch – Cyber Security Guide

Sichern Sie Ihre Anlagen mit dem CS141/BACS gegen Hackerangriffe!

Der CS141/BACS bietet Ihnen umfassende Möglichkeiten, um Ihr persönliches Sicherheitskonzept im Bereich der Cybersecurity zu realisieren. Bereits in der Grundkonfiguration gewährleistet das Gerät ein hohes Maß an Sicherheit, welches sogar für den Einsatz in Hochsicherheitsbereichen nach UL2900.1 zertifiziert wurde.


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

Mit diesem Hardening Guide möchten wir Ihnen zeigen, wie Sie die vielfältigen Konfigurationsmöglichkeiten des CS141/BACS optimal nutzen können, um:

- Ihren CS141/BACS nahtlos und ohne Kompromisse in Ihr bestehendes Sicherheitskonzept zu integrieren
- Die Betriebssicherheit Ihrer Anlagen umfassend zu gewährleisten

Dieser Leitfaden bietet Ihnen einen kompakten Überblick über alle notwendigen Schritte. Detaillierte Konfigurationsanweisungen und Tutorials, beispielsweise zum Erstellen von Zertifikaten, finden Sie im offiziellen Benutzerhandbuch für den CS141/BACS.

Vorteile des CS141/BACS für die Erhöhung der Gerätesicherheit:

- ✓ **Hohe Sicherheitsstandards:** Der CS141/BACS erfüllt strenge Sicherheitsanforderungen und ist nach UL2900.1 für den Einsatz in Hochsicherheitsbereichen zertifiziert.
- ✓ **Umfassende Konfigurationsmöglichkeiten:** Das Gerät bietet vielfältige Einstellungsmöglichkeiten, um es an Ihre individuellen Sicherheitsbedürfnisse anzupassen
- ✓ **Regelmäßige Sicherheitsupdates:** Der Hersteller stellt regelmäßig Sicherheitsupdates zur Verfügung, um die Geräte vor neuen Bedrohungen zu schützen.
- ✓ **Zertifizierte Hardware:** Der CS141/BACS basiert auf zertifizierter Hardware, die Manipulationen und unbefugten Zugriff verhindert.

Mit diesem Hardening Guide und dem CS141/BACS sind Sie auf dem besten Weg, Ihre Anlagen umfassend vor Cyberangriffen zu schützen.

Inhaltsverzeichnis

Worum geht es bei „Cybersecurity“?

Im allgemeinen Sprachgebrauch wird oft von "der Cybersecurity" gesprochen und gleichzeitig auf ein bestimmtes Gerät verwiesen, das "Cybersecurity" bieten soll. Tatsächlich ist "Cybersecurity" jedoch ein weit umfassenderes Konzept, das weit über die reine Absicherung einzelner Geräte hinausgeht.

Das schließt ein:

- Netzwerktopologien
- Zugangspunkte zum Netzwerk (Laptops, Computer, Ports)
- Firewall-Lösungen
- Passwortsicherheit
- Virenscanner
- Sauber installierte Zertifikate
- Schulung der Mitarbeiter und Anwender
- Meldewesen bei Hackereinbrüchen (abhängig von der Brache und der Einbruchstiefe)
- Regelmäßige Security-Audits und Sicherheits-Screenings
- Selbstkritischer Umgang mit gefundenen Auffälligkeiten durch Eigenverschulden

Unternehmen aufgepasst: Cybersicherheit ist Pflicht!

Sowohl deutsche Bundesgesetze als auch der EU-weite **European Cybersecurity Act (CSA)** verpflichten Unternehmen dazu, geeignete Maßnahmen zur Gewährleistung der Netzwerksicherheit zu ergreifen. Diese Verpflichtung zielt darauf ab, Unternehmen und ihre Daten vor Cyberangriffen zu schützen, die gravierende finanzielle und Reputationsverluste nach sich ziehen können.

Die konkreten Anforderungen und Gesetzeslagen an die Netzwerksicherheit variieren je nach Land, Branche und Unternehmensgröße. Grundsätzlich umfassen die geforderten Maßnahmen jedoch technische und organisatorische Aspekte wie die Installation von Firewalls und Virenschutzsoftware, die Schulung und Sensibilisierung von Mitarbeitern im Bereich Cybersecurity sowie die Erstellung von Notfallplänen.

Unternehmen, die diesen gesetzlichen Vorgaben nicht nachkommen, müssen mit empfindlichen Bußgeldern rechnen. Die Umsetzung von Cybersicherheitsmaßnahmen ist daher nicht nur eine rechtliche Verpflichtung, sondern auch eine Investition in den Schutz der Unternehmenswerte.

Der CS141 ist zertifiziert nach UL 2900.1, und erfüllt bzw. übertrifft sämtliche Sicherheitsanforderungen, die laut von den USA und der EU gefordert werden. Mit dem Cyber Security Guide möchten wir dem Betreiber helfen, den CS141 / BACS so zu konfigurieren, dass neben der optimalen Leistung bestmöglich alle geforderten Vorgaben an die IT-Sicherheit erfüllt werden können.

CS141 / BACS Hardening Guide

Jedes Produkt der CS141 Produktfamilie (CS141/HW161 WEBMANANAGER, SITEMANAGAER und -MONITOR 6, BACSKIT B4) liefert bei Auslieferung als Standardkonfiguration zahlreiche Funktionen mit einer standardisierten „Out oft he Box“ – Einstellungen:

- Vordefinierte und allgemeingültige Ports
- Sofern möglich, vorinstallierte Zertifikate
- Schnell konfigurierter Webzugriff
- Allgemein bekannte Standardpasswörte
- Standard Community Name (zum Beispiel “public” oder “private” für SNMP)
- Und vieles mehr …

Dadurch ist es möglich, diese Geräte in kurzer Zeit und vor allem ohne tiefgreifende Kenntnisse über Netzwerk- und Systemadministration in Betrieb zu nehmen und in ein bestehendes Netzwerk zu integrieren, solange es den allgemeingültigen Konventionen für eine Netzwerkinfrastruktur folgt.

Eine standardisierte Out-Of-The-Box- Konfigurationen hat allerdings auch den Nachteil, dass ein netzwerktaugliches Gerät unabhängig vom Hersteller oder seiner Funktion mit Blick auf die Cybersecurity nicht als „sicher“ betrachtet betrieben werden kann, da bereits Ein Blick in das Handbuch des Herstellers viele interessante Features offenbaren kann, mit denen ein Netzwerk ausgehorcht oder sogar infiltriert werden kann.

Dieses Kapitel soll Ihnen zeigen, was Sie einstellen können, um die Betriebssicherheit massiv zu erhöhen.

Tipp:

Dieses Hardening Guide beschreibt unter anderem, wie Sie Ports anpassen konnen – prüfen Sie vor der Änderung auf jeden Fall, ob die von Ihnen gewünschten Ports beides *sowohl frei als auch verfügbar* sind, da Sie ansonsten Kommunikationsprobleme riskieren. Beachten Sie bitte, dass die Änderung von Ports je nach Verwendungszweck Netzwerkweit umgesetzt werden müssen.

Nicht ALLE hier vorgestellten Möglichkeiten oder „empfohlenen Einstellungen“ sind zwangsläufig mit Ihrem Netzwerk kompatibel oder können im Rahmen der IT Security Richtlinien vor Ort 1:1 so umgesetzt werden. Sprechen Sie unbedingt vorher mit dem zuständigen Systembetreuer oder Administrator!

Generelle Empfehlungen:

1. Ändern Sie regelmäßig Passworte
2. Lassen Sie Backups nicht ungeschützt im Netzwerk liegen und minimieren Sie den Kreis berechtigter Personen
3. Beachten Sie die Gültigkeit der verwendeten Zertifikate
4. Verwenden Sie die aktuelle Firmware oder überprüfen Sie regelmäßig, ob neue Firmwareversionen Verbesserungen und neue Sicherheitsoptionen bereitstellen

Teil 1: Allgemeine Benutzeranmeldung Empfehlungen

Alle Geräte der CS141 – Produktfamilie bieten 2 grundlegende Anmeldemethoden an, die auf Wunsch miteinander kombiniert werden können. Beide Methoden haben ihre jeweiligen Vor- und Nachteile:

Lokales Benutzermanagement:

Der CS141 unterscheidet zwischen dem Namen und der „Nutzerrolle“. Der einzige Nutzer, der hardwareseitig vorgegeben ist und nicht deaktiviert werden kann, ist der Nutzer „admin“ mit der Nutzerrolle „Super User“:

Alle anderen Nutzer können geändert, angepasst und gelöscht werden:

Passwortempfehlung:

1. Ändern Sie das Passwort für den Super-User „admin“, um den Default-Zugang als Administrator zu sperren.

Als Grundregel für ein sicheres Passwort gilt:

- Ca. 8-16 Zeichen
- Groß- und Kleinschreibung
- Zahlen
- Sonderzeichen

Klicken Sie bei „admin“ auf „Benutzer bearbeiten:

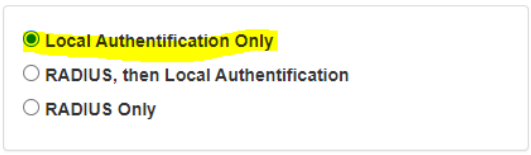
Damit ist der erste Schritt Richtung Betriebssicherheit erfolgt, nur noch der Benutzer „admin“ mit einem kryptischen Passwort ist aktiv der sich am Gerät anmelden kann.

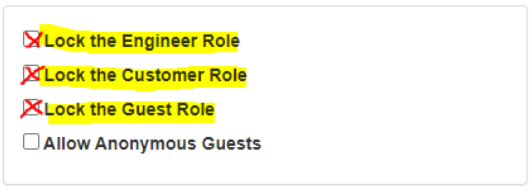
Sperren Sie nicht benötigte Nutzerrollen.

Wenn Sie die Nutzerrolle sperren, kann sich ein Benutzer, dem diese Rolle zugewiesen wurde, nicht mehr anmelden.

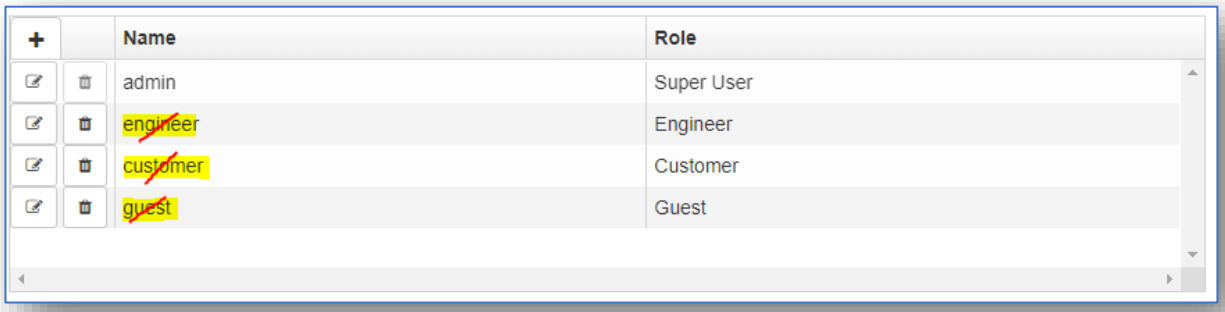
Sonderfunktion Anonymous Guest:

Diese Funktion ist standardmäßig deaktiviert, und wird mit dem Setzen des Hakens erlaubt. Der Anonymous Guest wird nur benötigt, wenn Sie eine UNMS verwenden oder z.B. mit einem iFrame oder ähnlichem direkte Anzeigen der Monitoring Screens realisiert haben.





Tipp: Zum „Gucken“ reicht ein Benutzer mit der Nutzerrolle „Guest“ aus. Der Benutzer „Customer“ darf neben „Gucken“ auch Logfiles herunterladen, aber sonst nichts.



2. Löschen oder ändern Sie Benutzername und Passwort:

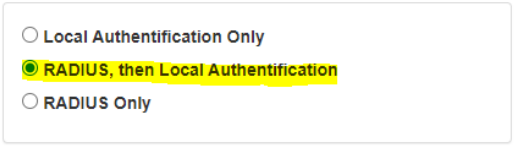
Ändern Sie sowohl Namen als auch Passwort für die ab Werk vorgegeneben Nutzer „engineer“, „customer“ und „guest“.

Netzwerkverwaltete Passwörter und Nutzernamen

Alle Geräte der CS141 Produktfamilie bieten ab der Firmware 2.04 die Möglichkeit, das Nutzermanagement über einen RADIUS- Server verwalten zu lassen. Das ermöglicht 2 unterschiedliche Sicherheitskonzepte:

Zugriffsoptimierte Sicherheit: RADIUS, danach lokale Nutzerauthentifizierung

In diesem Modus wird die Benutzerfreigabe exklusiv über einen RADIUS-Server verwaltet, wie dieser Verfügbar ist. Wenn der RADIUS-Server nicht antwortet, kann man sich über einen lokal verwalteten Nutzer anmelden – der Zugriff auf die Konfigurationsmenüs ist jederzeit gewährleistet.



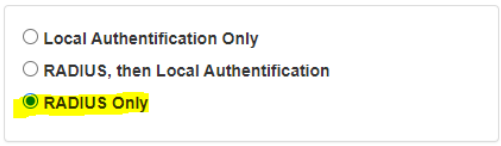
Empfehlung für maximale Sicherheit:

1. Deaktivieren Sie wieder die nicht benötigten Nutzerrollen
   Vom RADIUS-Server verteilte unnötige Nutzerrollen werden dann vom CS141 abgelehnt.
2. Ändern oder löschen Sie die lokal ab Werk vorgegebenen Nutzer.
   Sollte der RADIUS-Server nicht erreichbar sein, gelten ausschließlich lokal hinterlegte Nutzer.
3. Konfigurieren Sie den CS141, dass er RADIUS- danach Lokale Nutzerauthentifizierung. Verwendet.

Tipp:

Bei diesem Betriebsmodus müssen Sie manuell die lokal gespeicherten Passwörter zyklisch ändern!

Cyber-Security-optimierte Sicherheit: Exklusiver RADIUS-Modus

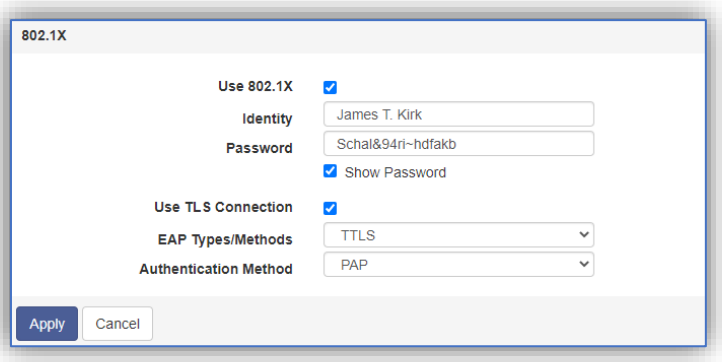


Bei diesem Betriebsmodus wird die lokale Benutzerdatenbank im regulären Betriebsmodus vollständig deaktiviert und nur noch die von einem RADIUS verwalteten User zugelassen. Sollten Sie lokalen Zugriff benötigen, muss vor Ort der Schiebeschalter in Mittelstellung (Konfigurationsmodus) und der CS141 neu gestartet werden.

Tipp:

Der Vorteil vom exklusiven RADIUS Login ist, dass Sie über einen zentralen RADIUS-Server Nutzernamen und Passworte direkt verwalten. Wenn der RADIUS-Server nicht erreichbar ist, kann sich kein Nutzer anmelden. Der lokale Zugriff erfordert die Anwesenheit vor Ort.

RADIUS - R802.1X Port Access



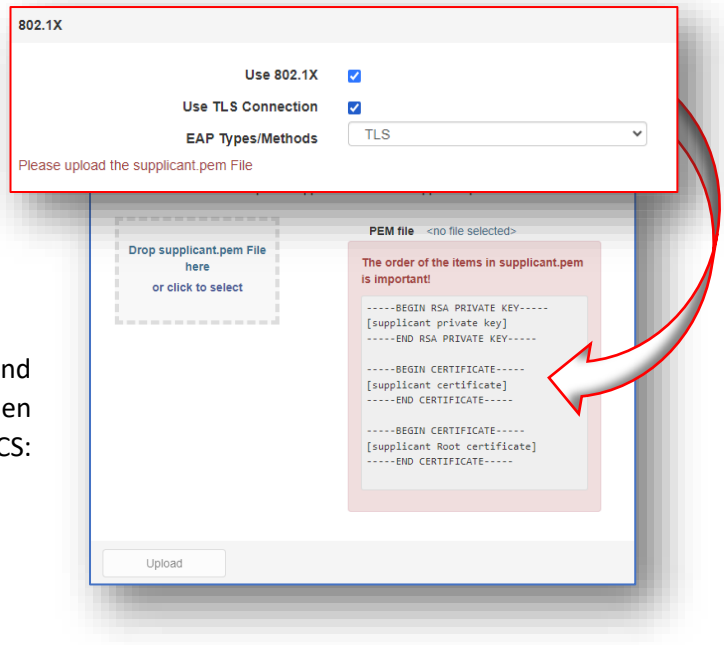
Unter System>Sicherheit finden Sie zusätzlich die Möglichkeit als Zugangskontrolle den Zugriff per R802.1X zu aktivieren. In dem Fall wird der Zugang über den Port des Netzwerkswitches und dessen Konfiguration geregelt.

Alle zum derzeitigen Stand angebotenen Verschlüsselungsmethoden und Authentifizierungsmethoden gelten zum derzeitigen Stand (April / 2022) als „sicher“. Sollte es neue Methoden geben, werden diese über entsprechende Updates nachgepflegt werden.

Cyber-Security-optimierte Sicherheit: Login via Certificate

Wo Passworte eingegeben werden können, besteht das Risiko, dass diese z.B. durch einen Keylogger ausgelesen werden können.

Ander ist es, wenn Sie einfach einen PEM-File hochladen, und dieser dann für den PAE-Login verwendet wird:



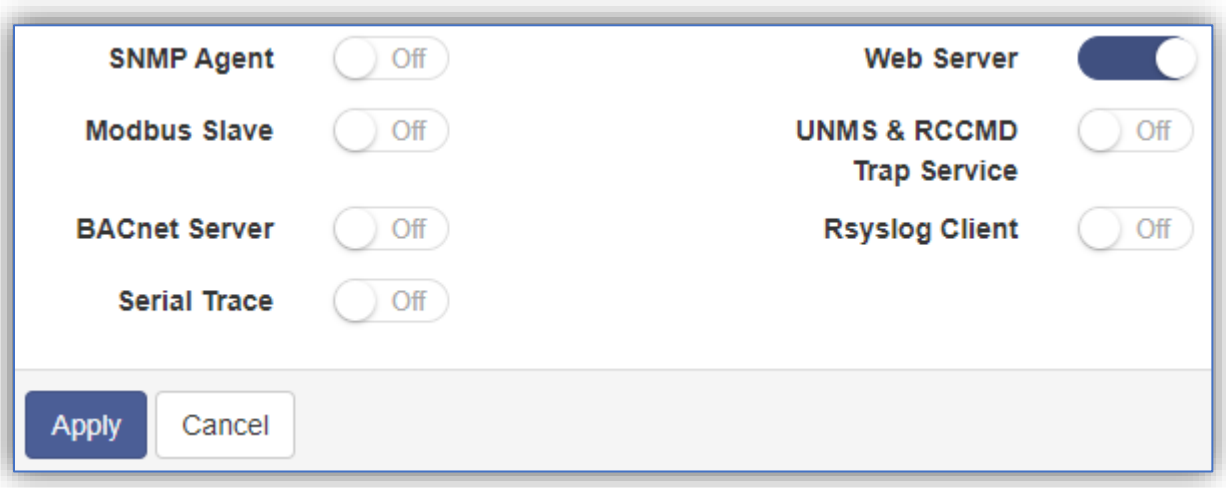
Stellen Sie als EAP Types/Method TLS ein, und laden Sie das notwendige Zertifkat in den speziell geschützten Speicher des CS141 / BACS:

Teil 2: Systemdienste

Überflüssig laufende Systemdienste sind vielleicht nicht unbedingt ein Einfallstor für Hacker, aber sie stellen latent eine Gefahr dar, weil die Möglichkeit besteht, den Datenverkehr abzufangen und auf diesen Weg etwas über ein Netzwerk herauszufinden. Ab Werk sind daher alle Dienste mit Ausnahme des Webservers auf OFF.

Empfehlung für maximale Sicherheit:

Schalten Sie daher überflüssig laufende Dienste aus, wenn Sie nicht vorhaben, diese zu verwenden:

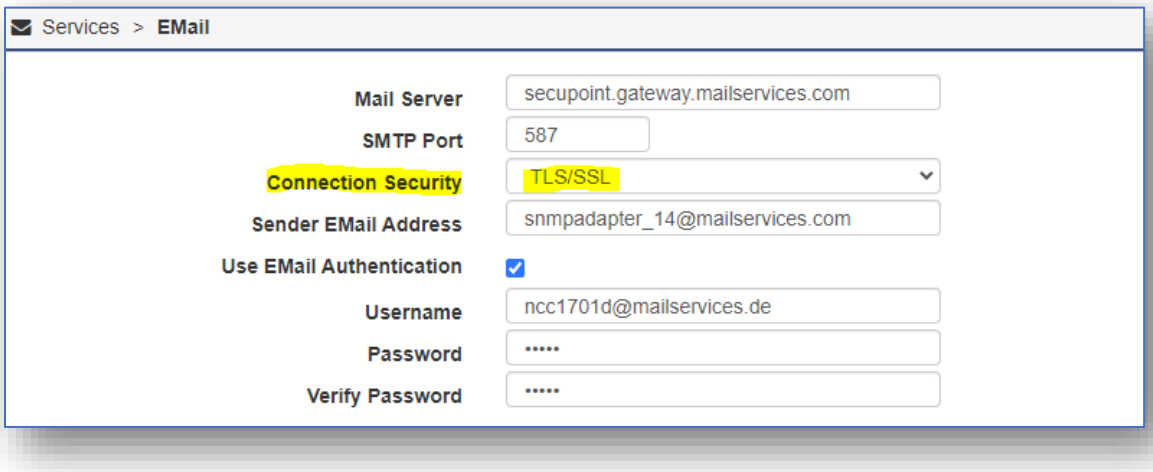


Je weniger mitteilungsbedürftige Systemdienste in einem Netzwerk laufen, desto weniger Datenverkehr kann abgehört werden.

Details zu den Services

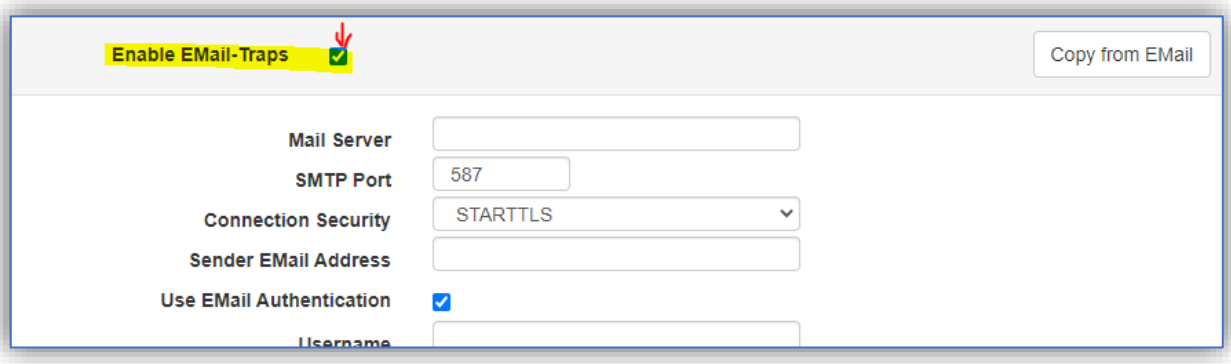
Der integrierte Mail-Client

Für die maximale Sicherheit empfehlen wir, einen internen Mailserver zu verwenden, um zu verhindern, dass Statusmeldungen von 3rd Party Dienstleistern verarbeitet und verfolgt werden können. Beim CS141 empfehlen wir die Verwendung von TLS/SSL, um die Kommunikation zwischen CS141 und Mailserver direkt zu verschlüsseln.



Email Traps

Diese Funktion benötigen Sie ausschließlich, wenn Sie eine UNMS mit EmailTraps verwenden und diese per EMail Trapnachrichten empfangen soll. In allen anderen Betriebsszenarien können Sie die Mail-Traps „ausschalten“, indem Sie den Haken entfernen.



Empfehlung für Mail-traps:

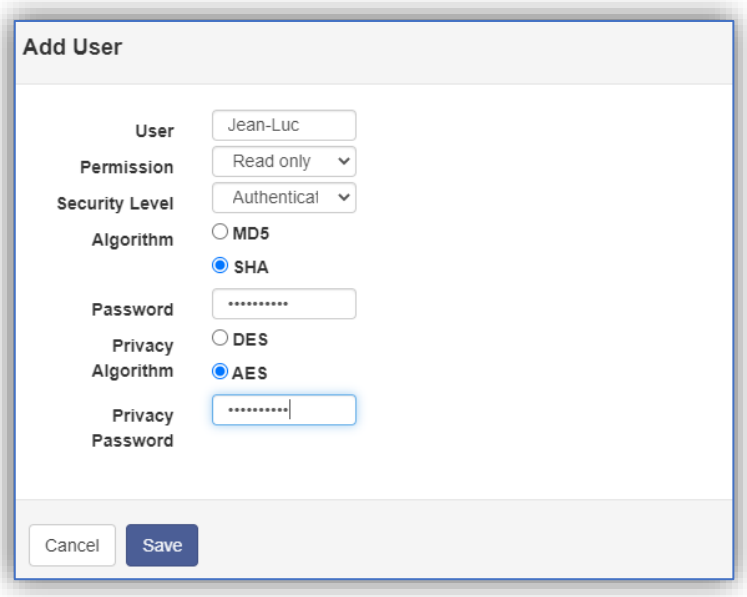
Schalten Sie die Email-Traps aus, wenn Sie keine UNMS verwenden. Es werden nur unnötig Daten per Mail versendet.

Der SNMP Agent

Mit SNMP (Simple Network Management Protocol) bietet alle Geräte der CS141-Produktfamilie eine standardisierte und beliebte Möglichkeit für die Integration in Gebäudeleitsysteme an. Dabei unterscheiden sich die Versionen 2 und 3 in der Zugriffsicherheit und im Zugriffskonzept.

Empfehlung für maximale Sicherheit:

Für die maximale Sicherheit empfehlen wir, den SNMP-Agenten auf **Version 3** zu stellen und **als Erlaubnis „Read only“** zu setzen.



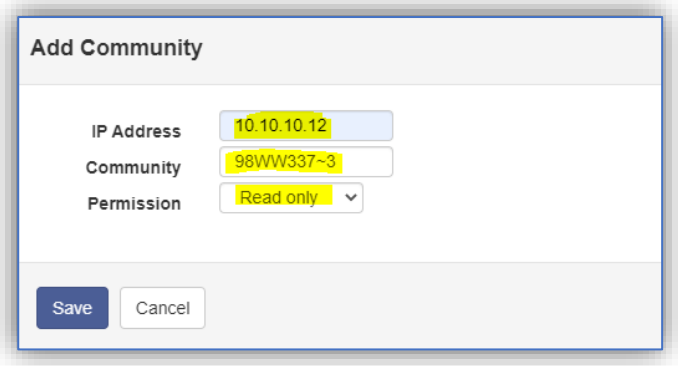
SNMP v3 bietet ein nutzerbasiertes Zugriffsverfahren, bei dem Sie die Passworte frei definieren können.

Alle angebotenen Verfahren zur Absicherung des Datenverkehrs gelten zum derzeitigen Stand der Technik (April 2022) als „sicher“ werden, wir empfehlen hier jedoch die Kombination SHA / AES, weil diese die moderneren Methoden zur Verschlüsselung verwenden.

Bitte beachten Sie: MD5 / SHA bzw. DES / AES sind nicht kompatibel zueinander. Welches Verfahren Sie in diesem Fall benutzen müssen, hängt daher von dem Netzwerk ab, in dem Sie den CS141 betreiben möchten.

Wenn Sie SNMP v2 verwenden müssen…

SNMP v2 bietet Zugriffsmöglichkeiten über Communities an. Zusätzlich kann über die IP-Adresse definiert werden, welcher Sender überhaupt berechtigt ist.



Empfehlung für Sicherheit mit SNMP v.2

1. Ändern Sie wenn möglich die Communitynamen (Standard „public“ für Lesen und „private“ für Schreiben)
2. Definieren über die IP-Adresse, welche Nutzer überhaupt berechtigt sind, Daten zu erhalten.
3. Stellen Sie die Erlaubnis auf „nur lesen“ ein.

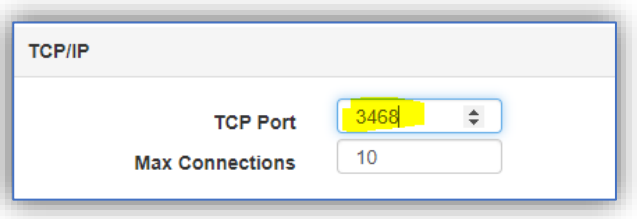
Modbus over TCP

Modbus kann seit vielen Jahren auch über TCP angefragt werden, was zahlreiche Möglichkeiten bietet, ein Gerät der CS141 Produktfamilie an ein Gebäudeleitsystem anzuschließen und Statusmeldungen abzufragen. Darüber lassen sich viele interessante Informationen über den Betriebszustand von Infrastrukturmaßnahmen wie USV-Anlagen oder Batterien in Erfahrung bringen.

Standardmäßig wird der Port P502 verwendet.

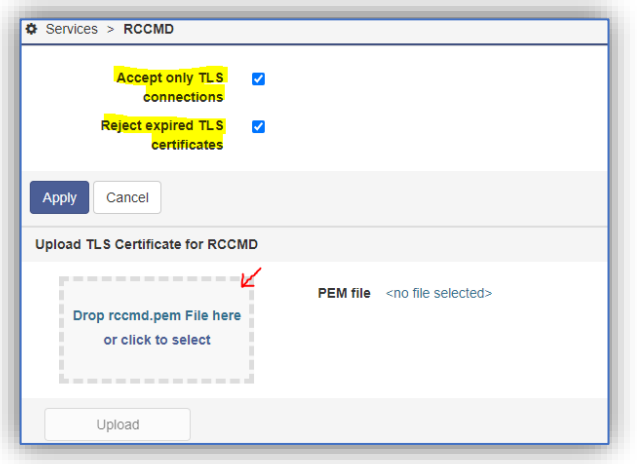
Empfehlung: Ändern Sie den Port

Der Port P502 ist eine Standardeinstellung, den viele Geräte für Modbus verwenden, wenn Sie den Port ändern, erschweren Sie die Auffindbarkeit durch unbefugte Eindringlinge.



RCCMD

RCCMD (Remote Control and Command) stellt für sich eine sehr sichere Methode dar, um bei einem Zwischenfall Zielsysteme zu informieren und gegebenenfalls automatisiert herunter zu fahren.



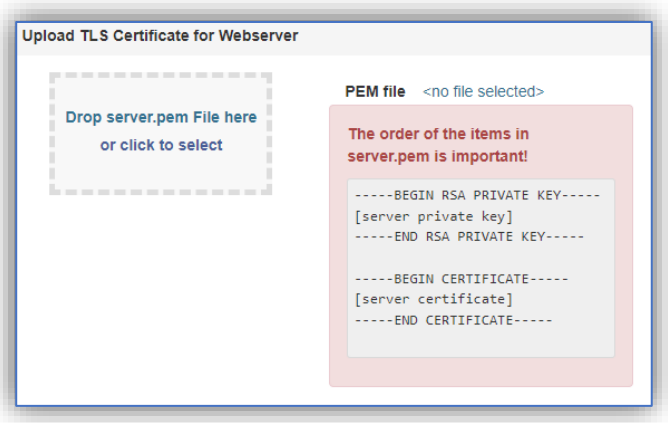
Im Normalfall wird RCCMD passiv im Hintergrund liegen und keinen sinnlosen Datenverkehr, der abgehört werden könnte, produzieren. Die damit alleine schon durch die Betriebsart vorgegebene Sicherheit ist in den meisten Netzwerken ausreichend, kann aber noch verschärft werden. Empfehlung zur Erhöhung der Sicherheit:

1. Lassen Sie nur TLS-Verbindungen zu
2. Lehnen Sie abgelaufene Zertifikate ab
3. Verwenden Sie ein eigenes Zertifikat.

Webserver

Alle Geräte der CS141 Produktfamilie verfügen über ein modernes Web-Interface, in dessen Hintergrund ein speziell gehärteter Webserver läuft. Neben dem Konfigurations-Interface werden hier auch die verfügbaren Monitoring Screens angezeigt.

Empfehlung für maximale Sicherheit

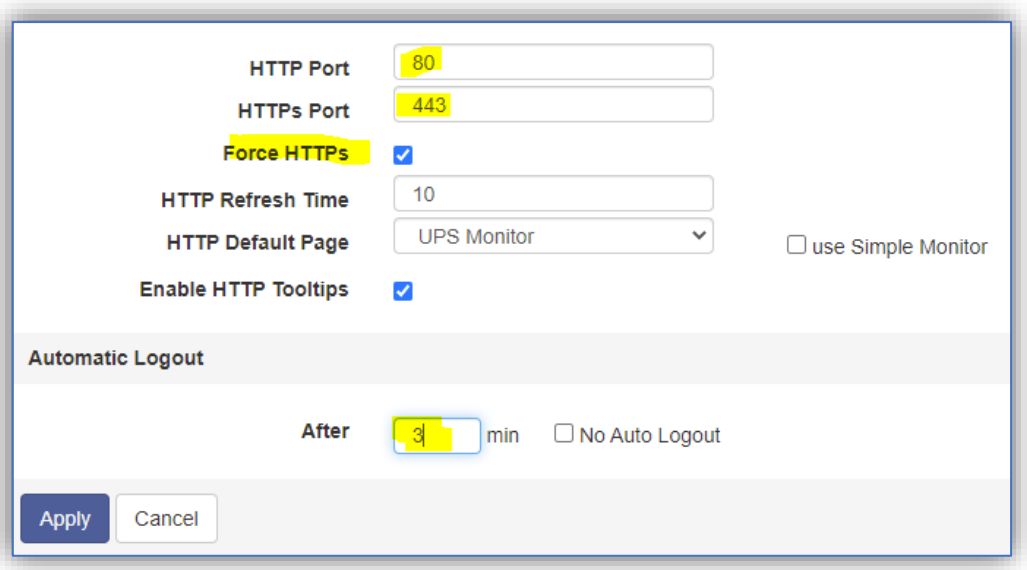


1. Stellen Sie „HTTPS erzwingen“ ein Damit wird die Standard-Methode über http deaktiviert und die Kommunikation läuft ausschließlich über die Verschlüsselte Kommunikationsart https.

2. Tauschen Sie das ab Werk mitgelieferte Zertifikat durch Ihr eigenes Zertifikat aus.

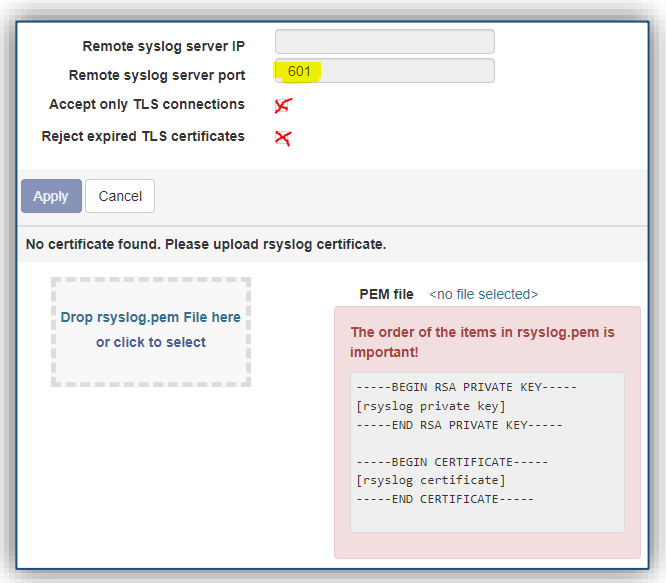
3. Ändern Sie die Ports, auf denen der Webserver läuft: Standardmäßig wird das Webinterface auf Port 80 und Port 443 aufgerufen.

4. Reduzieren Sie das Zeitfenster für den Auto-Logout auf ein Minimum, um Nutzer bei Inaktivität automatisch und schnellstmöglich vom CS141.abzumelden.



Remote Syslog

Standardmäßig läuft auf Port 601 der Remote Syslog Client mit einem vorinstallierten Zertifikat. Ziel dieses Service ist, dass die lokal gespeicherten Logfiles als Kopie direkt in einem Netzwerk zentral abgelegt werden, wo automatische Diagnosetools zahlreiche Auswertungen vornehmen können.



Empfehlung für maximale Sicherheit:

- Aktivieren Sie diese Funktion lediglich, wenn sie einen Syslog Receiver im Netzwerk verwenden.
- Aktivieren Sie „Nur TLS-Verbindungen akzeptieren“
- Abgelaufene TLS-Zertifikate ablehnen
- Ändern Sie den Port, der ist ab Werk auf Port 601 vorgegeben

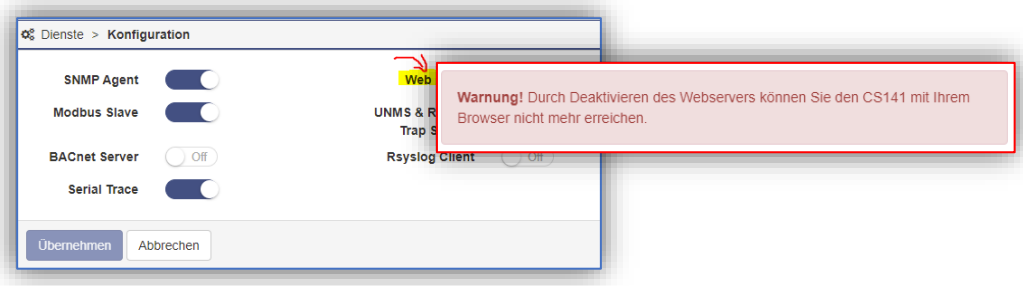
Teil 3: Manipulationsversuche über den Webserver vollständig ausschließen

Nur in einer besonders exponierten und gefährdeten Installation kommt diese Lösung zum Einsatz.

Alle Geräte der CS141 Produktfamilie bieten die Funktion an, ein Gerät vollständig „abzuschließen“ und den weiteren Zugriff auf das Konfigurationsinterface zu verbieten. Interne Watchdogs übernehmen dabei die Aufgabe, bei Bedarf einzelne Dienste oder ggfs. das gesamte Gerät komplett neu zu starten.

Das Gerät läuft in dem Fall zu 100% autonom „wie konfiguriert“ – ist aber nicht mehr komfortabel umzukonfigurieren.

Mit dieser Konfiguration verhindern Sie, dass Unbekannte Einstellungen manipulieren können, um zum Beispiel wichtige Einstellungen im Notfallmanagement gezielt zu sabotieren.



Wichtig: In diesem Betriebsszenario spielt die BACKUP/Restore-Funktion eine zentrale Rolle!

Da der Zugriff über das Webinterface abgeschaltet wird, sind Konfigurationsmöglichkeiten sind stark eingeschränkt! Für die Änderungen in der Konfiguration muss der CS141 in den Auslieferungszustand zurückgesetzt und ein Backup der letzten Konfiguration eingespielt werden.

Nach den Anpassungen muss vor dem Deaktivieren des Webservers ein neues Backup erstellt werden!

Wenn Sie einen Webmanager aus der CS141 Produktfamilie in den autonomen Modus versetzen möchten, fertigen Sie unbedingt ein BACKUP Ihrer Konfiguration an, *bevor Sie den Webserver deaktivieren:*

Änderungen und Anpassungen der Konfiguration erfolgen in diesem Betriebsszenario stets nach diesem Muster:

1. Schiebeschalter in Mittelstellung bringen (Konfigurationsmodus) und CS141 neu starten
2. Mit 10.10.10.10/ update den Updatedialog direkt aufrufen und ein Firmwareupdate aufspielen
3. BACKUP einspielen
4. Konfigurationsänderungen durchführen
5. Schiebeschalter wieder in die gewünschte Betriebsposition bringen
6. Testen der Einstellungen
7. Backup erstellen (!)
8. Erst dann den Webserver wieder deaktivieren.

Sobald der Webserver abgeschaltet wurde, läuft der CS141 in einem vollautonomen Betriebsmodus. Alle aktiv konfigurierten Schnittstellen sind verfügbar, und es ist keine Anmeldung am CS141/BACS über das Netzwerk mehr möglich.

Urheberrechts-Erklärung zum geistigen Eigentum und Umgang mit vertraulichen Informationen

Die Informationen in diesem Benutzerhandbuch sind nicht bedingte Anweisungen und können ohne Ankündigung verändert werden. Obwohl GENEREX versucht hat, präzise Informationen in diesem Dokument bereitzustellen, übernimmt GENEREX keine Verantwortung für die Genauigkeit dieser Informationen.

GENEREX ist nicht verantwortlich für jeden indirekten, speziellen, daraus folgenden oder unbeabsichtigten Schaden, ohne Einschränkungen, verlorener Gewinne oder Einkommen, Kosten von Austausch Gütern, Verlust oder Beschädigung von Daten, die sich durch den Gebrauch dieses Dokumentes oder das hier beschriebenen Produkt ergeben.

GENEREX als Hersteller der genannten Produkte, übernimmt keine Verpflichtungen mit diesen Informationen. Die Produkte, die in diesem Handbuch beschrieben werden, wurden auf der alleinigen Basis von Informationen für Geschäftspartner gegeben, damit diese ein besseres Verständnis für die GENEREX Produkte erhalten.

GENEREX erlaubt seinen Geschäftspartnern die Informationen, die in diesem Dokument enthalten sind, an Dritte weiterzugeben, ebenso an das Personal in deren Firma oder ihren eigenen Kunden, elektronisch, manuell, in Form von Fotokopien oder Ähnlichem. GENEREX gibt an, dass der Inhalt nicht verändert oder angepasst werden darf, ohne schriftliche Genehmigung von GENEREX.

Alle Rechte, Titel und Interessen am GENEREX Markenzeichen BACS oder Firmenzeichen (registriert oder nicht registriert) oder der Geschäftswert bzw. das geistige Eigentum von GENEREX, das Urheberrecht und die Produkt-Patente sind exklusiv und ohne Einschränkungen im Eigentum von GENEREX.

GENEREX wird jede Beanstandung über den Inhalt dieses Dokumentes zeitnah abwickeln. Kommentare oder Beanstandungen zu diesem Dokument sollten an die GENEREX Systems Vertriebsgesellschaft mbH adressiert werden.