SSC600 - CONTROLLO E PROTEZIONE DI SOTTOSTAZIONI INTELLIGENTI PER SISTEMI ELETTRICI ABB ABILITY™

SSC600

Linee guida per l'implementazione della Sicurezza Informatica

ID documento: 2NGA002113
Emesso: 30/11/2022
Revisione: A
Versione del prodotto: 1.0 FP4

© Copyright 2022 ABB. Tutti i diritti riservati

Copyright

Il presente documento non può essere riprodotto o copiato, interamente o parzialmente, senza autorizzazione scritta da parte di ABB e il relativo contenuto non può essere divulgato a terzi o utilizzato per scopi non autorizzati.

L'hardware o il software descritti in questo documento sono forniti sotto licenza e possono essere utilizzati, copiati o divulgati solo in conformità ai termini di tale licenza.

Marchi

ABB e Relion sono marchi registrati del Gruppo ABB. Tutti gli altri marchi o nomi di prodotti menzionati in questo documento possono essere marchi o marchi registrati dei rispettivi proprietari. SSC600 è una soluzione Intel® IoT Market Ready approvata.

Software open source

Questo prodotto contiene software open source. Per informazioni sulla licenza, fare riferimento alla documentazione sul prodotto all'indirizzo *www.abb.com*.

Garanzia

Per i termini della garanzia, si prega di rivolgersi a un rappresentante ABB.

www.abb.com/mediumvoltage

Dichiarazione di esclusione di responsabilità

I dati, gli esempi e i diagrammi contenuti in questo manuale sono presenti esclusivamente per la descrizione del concetto o del prodotto e non devono essere considerati come una dichiarazione di proprietà garantite. Tutte le persone responsabili dell'applicazione dell'attrezzatura trattata in questo manuale devono assicurarsi che ogni applicazione prevista sia adatta e accettabile, compreso il rispetto di qualsiasi requisito di sicurezza o di altri requisiti operativi applicabili. In particolare, qualsiasi rischio nelle applicazioni in cui un guasto del sistema e/o del prodotto creerebbe un rischio di danni a cose o persone (inclusi, ma non limitati a, lesioni personali o morte) sarà di esclusiva responsabilità della persona o dell'ente che applica l'attrezzatura, e coloro che hanno tale responsabilità sono tenuti ad assicurare che vengano prese tutte le misure per escludere o mitigare tali rischi.

Questo prodotto è stato progettato per essere collegato e comunicare dati e informazioni tramite un'interfaccia di rete che deve essere collegata a una rete sicura. È esclusiva responsabilità della persona o dell'entità responsabile dell'amministrazione della rete assicurare una connessione sicura alla rete e prendere le misure necessarie (come, ma non solo, l'installazione di firewall, l'applicazione di criteri di autenticazione, la crittografia di dati, l'installazione di programmi anti-virus, ecc.) al fine di proteggere il prodotto, la rete, il suo sistema e l'interfaccia contro qualsiasi forma di violazione della protezione, accesso non autorizzato, interferenza, intrusione, fuga e/o furto di dati o informazioni. ABB non è responsabile di tali danni e/o perdite.

Questo documento è stato accuratamente controllato da ABB, ma non è possibile escludere completamente eventuali deviazioni. Nel caso in cui vengano rilevati degli errori, il lettore è pregato di notificarli al produttore. Fatti salvi espliciti impegni contrattuali, in nessun caso ABB sarà responsabile di perdite o danni derivanti dall'uso di questo manuale o dall'applicazione dell'attrezzatura.

In caso di discrepanze tra la versione inglese e quella in qualsiasi altra lingua, farà fede il testo della versione inglese.

Conformità

Questo prodotto è conforme alla direttiva del Consiglio delle Comunità europee sul ravvicinamento delle legislazioni degli Stati membri in materia di compatibilità elettromagnetica (direttiva EMC 2014/30/UE) e riguardanti il materiale elettrico destinato a essere adoperato entro taluni limiti di tensione (Direttiva Bassa Tensione 2014/35/UE). La conformità è il risultato dei test condotti da ABB in ottemperanza alla norma di prodotto EN 60255-26 per la Direttiva EMC e alle norme di prodotto EN 60255-1 ed EN 60255-27 per la Direttiva Bassa Tensione. Il prodotto è progettato in conformità con le norme internazionali della serie IEC 60255 e IEC 61805-3:2013.

Indice generale

1 Introduzione ... 9

1.1 Questo manuale ... 9
1.2 Destinatari previsti ... 9
1.3 Documentazione sul prodotto ... 10
1.3.1 Set di documentazione del prodotto ... 10
1.3.2 Cronologia delle revisioni del documento ... 10
1.3.3 Documentazione correlata ... 10
1.4 Simboli e convenzioni ... 11
1.4.1 Simboli ... 11
1.4.2 Convenzioni nel documento ... 11

2 Sicurezza nell'automazione della distribuzione ... 12

2.1 Sicurezza generale nell'automazione della distribuzione ... 12
2.2 Documenti di riferimento ... 12

3 Configurazione sicura del sistema ... 14

3.1 Regole di base per il rafforzamento del sistema ... 14
3.2 Interfacce di comunicazione del dispositivo ... 15
3.3 Protocolli basati su TCP/IP e porte IP utilizzate ... 15
3.4 Comunicazione sicura ... 16
3.4.1 Gestione dei certificati ... 16
3.4.2 Caricamento di un certificato ... 17
3.4.3 Algoritmi di crittografia ... 18
3.5 HMI Web ... 18

4 Gestione degli utenti ... 19

4.1 Gestione account utente locali ... 19
4.1.1 Politiche relative alle password ... 23

5 Registrazione di sicurezza ... 26

5.1 Tracciamento di verifica ... 26
5.2 Central Activity Logging ... 27

6 Utilizzo di HMI Web ... 29

6.1 Inizio sessione ... 29
6.2 Termine sessione ... 30

7 Protezione della configurazione del dispositivo e del sistema..... 31

7.1 File di backup.....31

7.1.1 Creazione di un backup dalla configurazione del dispositivo..... 31

7.1.2 Creazione di un backup dal progetto PCM600.....31

7.2 Ripristino delle impostazioni di fabbrica.....31

7.3 Ripristino della password persa.....34

8 Glossario.....35

1 Introduzione

1.1 Questo manuale

Le linee guida per l'implementazione della sicurezza informatica ne descrivono il processo di gestione durante la comunicazione con il sistema di controllo e protezione di sottostazioni intelligenti ABB Ability™ per i sistemi elettrici SSC600 e SSC600 SW. Le linee guida per l'implementazione della sicurezza informatica forniscono informazioni su come proteggere il sistema su cui è installato il dispositivo. Le linee guida possono essere utilizzate come riferimento tecnico durante la fase di ingegnerizzazione, installazione e messa in servizio e durante il normale servizio.

1.2 Destinatari previsti

Queste linee guida sono destinate al personale addetto all'ingegnerizzazione del sistema, alla messa in servizio, al funzionamento e alla manutenzione, che si occupa della sicurezza informatica durante le fasi di ingegnerizzazione, installazione e messa in servizio e durante il normale funzionamento.

Ci si aspetta che il personale abbia una conoscenza generale su argomenti relativi alla sicurezza informatica.

- Relè di protezione e controllo, gateway e workstation Windows
- Networking, inclusi Ethernet e TCP/IP con il suo concetto di porte e servizi
- Politiche di sicurezza
- Firewall
- Protezione antivirus
- Whitelisting dell'applicazione
- Comunicazione remota sicura

1.3 Documentazione sul prodotto

1.3.1 Set di documentazione del prodotto

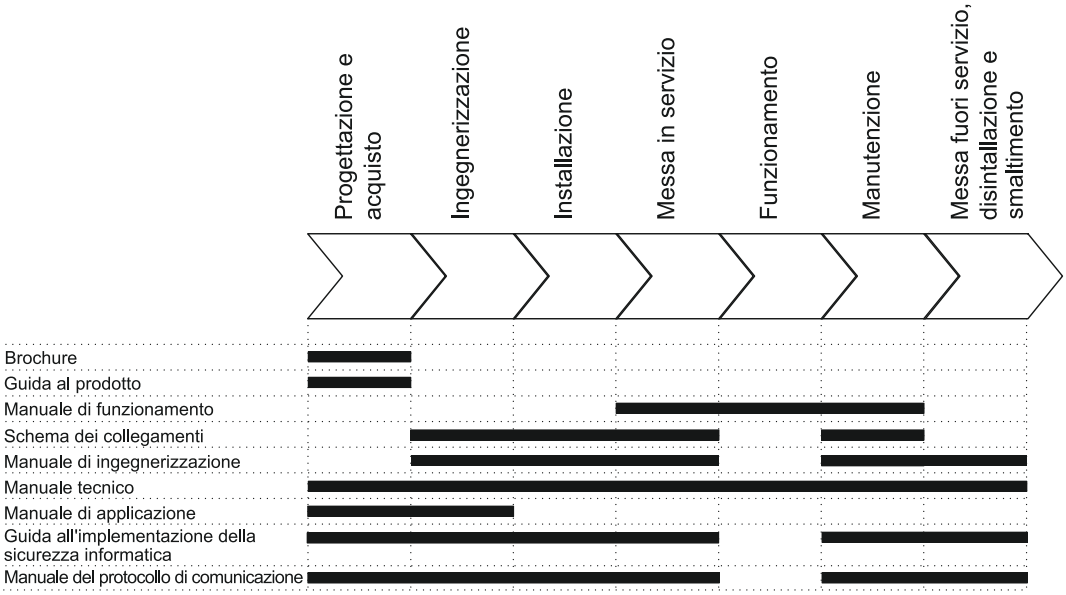


Figura 1. L'uso previsto dei documenti durante il ciclo di vita del prodotto

I manuali specifici per le serie e i prodotti possono essere scaricati dal sito Web ABB.

1.3.2 Cronologia delle revisioni del documento

Revisione/data del documento	Versione della serie del prodotto	Cronologia
A/13/05/2019	1.0	Primo rilascio
B/10/03/2020	1.0 FP1	Contenuto aggiornato
C/11/09/2020	1.0 FP2	Contenuto aggiornato
D/2021-11-08	1.0 FP3	Contenuto aggiornato
E/2022-11-30	1.0 FP4	Contenuto aggiornato per corrispondere al livello di connettività del prodotto

Scaricare i documenti più aggiornati dal sito Web ABB *www.abb.com/mediumvoltage*.

1.3.3 Documentazione correlata

I manuali specifici per i prodotti e per le serie di prodotti possono essere scaricati dal sito Web ABB *www.abb.com/mediumvoltage*.

1.4 Simboli e convenzioni

1.4.1 Simboli

L'icona di avvertenza indica la presenza di un pericolo che potrebbe provocare scossa elettrica o lesioni personali.

L'icona di attenzione indica informazioni importanti o un'avvertenza relative al concetto discusso nel testo. Potrebbe indicare la presenza di un pericolo che potrebbe provocare danni al software o alle attrezzature o alla proprietà.

L'icona delle informazioni avverte il lettore di fatti e condizioni importanti.

L'icona del suggerimento indica un consiglio, ad esempio, su come realizzare il progetto o usare una certa funzione.

Anche se i pericoli delle avvertenze sono legati alle lesioni personali, è necessario comprendere che in determinate condizioni operative il funzionamento dell'attrezzatura danneggiata può comportare il deterioramento delle prestazioni del processo, con conseguenti lesioni personali o morte. Occorre pertanto rispettare pienamente tutti gli avvisi e le avvertenze.

1.4.2 Convenzioni nel documento

È possibile che in questo manuale una particolare convenzione non venga usata.

- Abbreviazioni e acronimi sono spiegati nel glossario. Il glossario contiene anche definizioni di termini importanti.
- I percorsi dei menu sono presentati in grassetto.

  Selezionare **Main menu** > **Settings**.
- I nomi dei parametri sono in corsivo.

  La funzione può essere abilitata e disabilitata con l'impostazione *Operation*.
- I valori dei parametri sono indicati fra virgolette.

  I valori dei parametri corrispondenti sono "On" e "Off".
- I messaggi di input/output e i nomi dei dati monitorati sono presentati con caratteri Courier.

  Quando la funzione inizia, l'uscita `START` è impostata su TRUE.
- Questo documento presuppone che la visibilità delle impostazioni dei parametri sia "Advanced".

2 Sicurezza nell'automazione della distribuzione

2.1 Sicurezza generale nell'automazione della distribuzione

I progressi e le scoperte tecnologiche hanno portato a un'evoluzione significativa nella rete elettrica. L'emergente "rete intelligente" e "Internet delle cose" stanno pertanto diventando rapidamente una realtà. Al centro di questi progressi intelligenti ci sono sistemi IT specializzati: varie soluzioni di controllo e automazione come i sistemi di automazione della distribuzione. Per fornire agli utenti finali informazioni complete in tempo reale, consentendo una maggiore affidabilità e un maggiore controllo, i sistemi di automazione sono diventati sempre più interconnessi. Per contrastare i maggiori rischi associati a queste interconnessioni, ABB offre un'ampia scelta di prodotti e soluzioni di sicurezza informatica per sistemi di automazione e infrastrutture critiche.

La nuova generazione di sistemi di automazione utilizza standard aperti come IEC 60870-5-104, DNP3 e IEC 61850 e tecnologie commerciali, in particolare Ethernet e protocolli di comunicazione basati su TCP/IP Consente inoltre la connettività a reti esterne, come i sistemi Intranet dell'ufficio e Internet. Questi cambiamenti tecnologici, inclusa l'adozione di standard IT aperti, hanno portato enormi vantaggi dal punto di vista operativo, ma hanno anche introdotto problemi di sicurezza informatica che in precedenza interessavano solo i sistemi IT di uffici o aziende.

Per contrastare i rischi legati alla sicurezza informatica, gli standard IT aperti sono dotati di meccanismi di sicurezza informatica. Questi meccanismi, sviluppati in numerosi ambienti aziendali, sono tecnologie collaudate. Consentono la progettazione, lo sviluppo e il miglioramento continuo di soluzioni di sicurezza informatica anche per i sistemi di controllo, comprese le applicazioni di automazione della distribuzione.

ABB comprende l'importanza della sicurezza informatica e il suo ruolo nel promuovere la sicurezza delle reti di distribuzione. Un cliente che investe in nuove tecnologie ABB può fare affidamento su soluzioni di sistema in cui affidabilità e sicurezza hanno la massima priorità.

Vulnerabilità o problemi di sicurezza informatica relativi a qualsiasi prodotto ABB possono essere segnalati scrivendo a cybersecurity@ch.abb.com.

2.2 Documenti di riferimento

La sicurezza delle informazioni in infrastrutture critiche come le reti di distribuzione e trasmissione elettrica è stata al centro dell’attenzione sia dei fornitori che delle utility. Questo, insieme allo sviluppo della tecnologia, ad esempio, apparecchio di reti di comunicazione basate su Ethernet e IP in sottostazioni, centrali elettriche e

centri di controllo della rete crea la necessità di specificare sistemi con sicurezza informatica.

ABB è coinvolta nella standardizzazione e nella definizione di numerosi standard informatici, i più applicabili e di riferimento dei quali sono ISO 2700x, IEC 62443, IEEE P1686 e IEC 62351. Oltre agli sforzi di standardizzazione, ci sono anche diversi requisiti e pratiche avviati dai governi, come NERC CIP e BDEW. ABB comprende appieno l'importanza della sicurezza informatica per i sistemi di automazione delle sottostazioni e si impegna a supportare gli utenti negli sforzi per raggiungere o mantenere la conformità ad essi.

3 Configurazione sicura del sistema

3.1 Regole di base per il rafforzamento del sistema

Gli odierni sistemi di automazione della distribuzione sono fondamentalmente sistemi IT specializzati. Pertanto, anche a questi sistemi si applicano diverse regole di rafforzamento di un sistema di automazione. Dal punto di vista del sistema di automazione, i dispositivi di protezione e controllo si trovano al livello più basso e più vicino al processo primario vero e proprio. È importante applicare il concetto di garanzia delle informazioni di difesa profonda in cui ogni livello è in grado di proteggere il sistema di automazione; pertanto anche i dispositivi di protezione e controllo fanno parte di questo concetto. Quando si pianifica la protezione del sistema è necessario tenere conto di quanto segue.

- Riconoscere e familiarizzare con tutte le parti del sistema e con i suoi collegamenti di comunicazione
- Rimuovere dal sistema tutti i collegamenti di comunicazione non necessari
- Valutare il livello di sicurezza delle connessioni rimanenti e migliorarlo con i metodi applicabili
- Considerare la sicurezza fisica degli asset, ad esempio dispositivi di protezione, supporti rimovibili e cavi di comunicazione
- Rafforzare il sistema rimuovendo o disattivando tutti i processi, le porte di comunicazione e i servizi inutilizzati
- Controllare che l'intero sistema abbia backup disponibili da tutte le parti applicabili
- Raccogliere e archiviare backup dei componenti del sistema e mantenerli aggiornati
- Rimuovere tutti gli account utente non necessari
- Cambiare le password predefinite e utilizzare password sufficientemente complesse
- Verificare che il collegamento dalla sottostazione al sistema di livello superiore utilizzi una crittografia e un'autenticazione sufficientemente forti
- Separare la rete pubblica dalla rete di automazione
- Segmentare il traffico e le reti, incluso l'ambiente di virtualizzazione quando si utilizza SSC600 SW
- Utilizzare firewall e zone demilitarizzate
- Valutare periodicamente il sistema
- Utilizzare software antivirus nelle workstation e mantenerle aggiornate
- Mantenere aggiornati i componenti software. Includere SSC600 e l'ambiente correlato, ad esempio hypervisor.

Quando si progetta la sicurezza di un sistema di automazione, è importante utilizzare il concetto di difesa profonda. Non è consigliabile collegare direttamente a Internet un dispositivo senza adeguati componenti aggiuntivi di sicurezza. I diversi livelli e le interfacce del sistema dovrebbero utilizzare controlli di sicurezza. Sicurezza robusta significa abilitare e utilizzare le funzionalità disponibili (oltre a quelle del prodotto) e anche imporne l'uso secondo le politiche aziendali. È inoltre necessaria una formazione adeguata del personale che accede al sistema e lo utilizza.

Quando si utilizza SSC600 SW, è necessario considerare il rafforzamento dell'hypervisor. Occorre seguire le migliori pratiche relative all'hypervisor scelto. Il rafforzamento di SSC600 SW segue le stesse pratiche di SSC600.

3.2 Interfacce di comunicazione del dispositivo

Tutte le porte fisiche dedicate alla comunicazione del bus della stazione e del bus di processo, ad eccezione della porta locale, possono essere aperte e chiuse nella configurazione del dispositivo. La porta locale viene utilizzata per l'ingegnerizzazione e può essere utilizzata solo per l'accesso alla configurazione punto-punto con PCM600 o WHMI. La porta locale non deve essere collegata ad alcuna rete Ethernet.

Tabella 1: Porte fisiche sulle schede di comunicazione del dispositivo

ID della porta	Tipo	Stato predefinito	Descrizione
LAN1	RJ-45	Abilitato	Porta locale
LAN2	RJ-45	Disabilitato	Porta remota (per ingegnerizzazione)
LAN3	RJ-45 o fibra ottica	Disabilitato	Bus di processo A
LAN4	RJ-45 o fibra ottica	Disabilitato	Bus di processo B
LAN5	RJ-45	Abilitato	Porta posteriore
LAN6	RJ-45	Disabilitato	Non in uso
LAN7	RJ-45	Disabilitato	Porta di servizio
LAN8	RJ-45	Disabilitato	Non in uso

Il protocollo IEC 61850 e le porte LAN1 e LAN5 sono attivati per impostazione predefinita, in quanto utilizzati per l'ingegnerizzazione del dispositivo di protezione.

3.3 Protocolli basati su TCP/IP e porte IP utilizzate

La sicurezza della porta IP dipende dall'installazione, dai requisiti e dall'infrastruttura specifica esistente. Le apparecchiature esterne richieste possono essere dispositivi separati o dispositivi che combinano firewall, router e funzionalità VPN sicura. Quando la rete è divisa in zone di sicurezza, ciò avviene con dispositivi di sottostazione dotati di funzionalità firewall o con prodotti firewall dedicati. I confini della zona di sicurezza sono all'interno della sottostazione o tra la sottostazione e il mondo esterno.

Il dispositivo supporta un'opzione con porte Ethernet di comunicazione per più stazioni. In questo caso tutte le porte utilizzano lo stesso indirizzo IP indipendentemente dall'opzione di ridondanza attivata nella configurazione del dispositivo.

Per impostare un firewall IP, la tabella seguente riassume le porte IP utilizzate dal dispositivo. Le porte aperte per impostazione predefinita vengono utilizzate per configurare il dispositivo di protezione.

Tabella 2: Porte IP utilizzate dal dispositivo

Numero porta	Tipo	Stato predefinito	Descrizione
20, 21	TCP	Aperto	Protocollo di trasferimento file (FTPS)
102	TCP	Aperto	IEC 61850
80, 443	TCP	Aperto	Server Web HTTPS
5001	TCP	Aperto	Aggiornamento del firmware tramite HTTPS, gestione degli account utente e aggiornamenti dei certificati.
2404	TCP	Chiuso	TCP IEC 60870-5-104
67	UDP	Aperto	Server DHCP su LAN1 e LAN2

FTPS e IEC 61850 sono servizi primari necessari per la configurazione del dispositivo e non possono essere disabilitati. Inoltre, il dispositivo di protezione utilizza R-GOOSE (multicast IP/UDP) e comunicazioni di livello 2 in servizi di supervisione GOOSE, SMV, IEEE 1588 (PTP) e PRP, di cui tenere conto nella progettazione della rete.

Oltre ai protocolli HTTPS e FTPS, il dispositivo supporta il protocollo di comunicazione di automazione delle sottostazioni basato su Ethernet IEC 61850. IEC 61850 è sempre abilitato.

3.4 Comunicazione sicura

Il dispositivo di protezione supporta la comunicazione crittografata secondo i principi dello standard IEC 62351 nella comunicazione protetta per WHMI e trasferimento file. *Secure Communication* è abilitata per impostazione predefinita e pertanto i protocolli richiedono il supporto del metodo di crittografia basato su protocollo TLS da parte dei client. In questo caso WHMI deve essere connesso da un browser Web utilizzando protocollo HTTPS. In caso di trasferimento di file, il client deve utilizzare FTPS. PCM600 supporta FTPS ed è in grado di scaricare e caricare file di configurazione nel canale di comunicazione crittografato dal dispositivo. Alcuni protocolli del settore industriale come IEC 60870-5-104 e MMS sono implementati secondo i rispettivi standard senza comunicazione sicura. È essenziale prendere in considerazione il rafforzamento descritto in *Capitolo 3.1 Regole di base per il rafforzamento del sistema*.

3.4.1 Gestione dei certificati

Per la crittografia e l'identificazione sicure, i protocolli HTTPS e FTPS nel dispositivo di protezione utilizzano certificati a chiave pubblica che associano una chiave pubblica a un'identità, ovvero informazioni come il nome di un'organizzazione, il suo indirizzo e così via. Il certificato server utilizzato dal dispositivo di protezione è generato dal dispositivo stesso come certificato autofirmato e non emesso da alcuna autorità di certificazione (CA).

I certificati utilizzano la crittografia per fornire comunicazioni sicure sulla rete. Il dispositivo di protezione genera un certificato X.509 autofirmato e una coppia di chiavi RSA con una lunghezza di 2048 bit. La chiave RSA memorizzata nel certificato viene utilizzata per stabilire una comunicazione sicura.

Il certificato viene utilizzato per verificare che una chiave pubblica appartenga a un'identità. In caso di HTTPS, il server WHMI nel dispositivo di protezione presenta il certificato al client Web fornendogli la chiave pubblica e l'identità del server. La chiave pubblica è una parte di un algoritmo a chiave asimmetrica in cui una chiave viene utilizzata per crittografare un messaggio e un'altra chiave per decrittografarlo. La coppia di chiavi pubblica-privata (chiave asimmetrica) viene utilizzata per scambiare la chiave simmetrica, che viene utilizzata per crittografare e decrittografare i dati scambiati tra server e client.

I messaggi crittografati con la chiave pubblica possono essere decrittografati solo con l'altra parte dell'algoritmo, la chiave privata. La chiave pubblica e quella privata sono correlate matematicamente e rappresentano una coppia di chiavi crittografiche. La chiave privata viene mantenuta segreta e custodita in modo sicuro nel dispositivo di protezione, mentre quella pubblica può essere ampiamente diffusa.

Una volta considerato attendibile manualmente il certificato del dispositivo di protezione in una finestra di dialogo separata, il certificato risulta attendibile nella comunicazione tra il dispositivo e PCM600. Per l'utilizzo di WHMI è necessario che il certificato firmato dal dispositivo di protezione venga accettato nel browser Web all'apertura della connessione a WHMI.

Il browser Web visualizza un'avvertenza, perché WHMI utilizza certificati autofirmati.

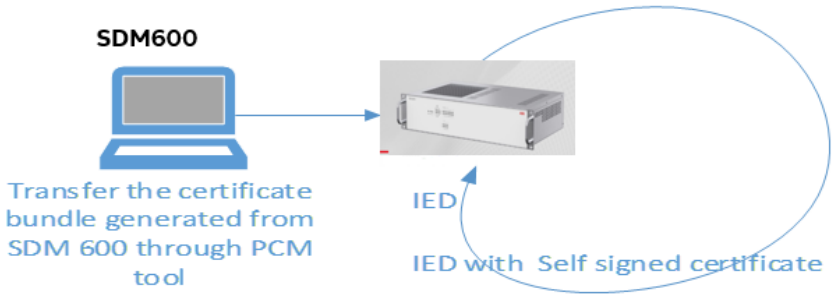
3.4.2 Caricamento di un certificato

- Certificato esterno:

  Per impostazione predefinita, SSC600 supporta la funzionalità di sicurezza della comunicazione basata su certificato autofirmato. Per una maggiore sicurezza supporta anche il certificato firmato da un'autorità di certificazione attendibile. L'aggiornamento del certificato esterno supporta l'importazione manuale di certificati attendibili di terze parti.

- Metodologia:

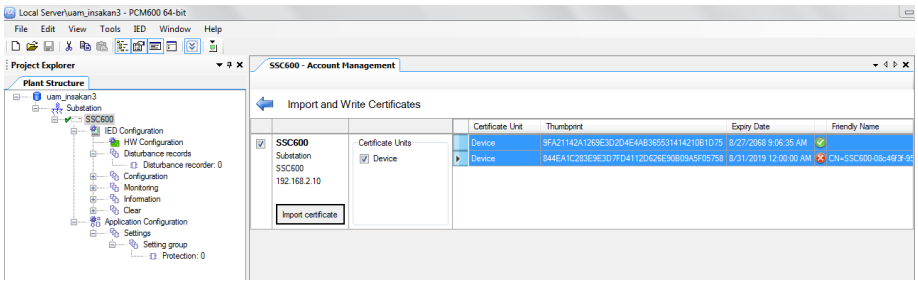
  SSC600 può utilizzare qualsiasi certificato in formato .p12. I certificati vengono messi in servizio in SSC600. Informazioni dettagliate sulla scrittura dei certificati su SSC600 sono riportate nella "Guida per l'utente di PCM600".



Inizialmente il dispositivo SSC600 funziona con un certificato autofirmato. Una volta ricevuto il certificato attendibile, autorizza il dispositivo con il certificato esterno.

- Estrazione del certificato:

  Il pacchetto di certificati (.p12) importato in SSC600 e i certificati vengono estratti e quindi caricati in SSC600.



- L'aggiornamento del certificato può essere verificato su WHMI del dispositivo, facendo clic sull'icona del lucchetto sul lato sinistro della barra degli indirizzi (anche se ci sono piccole differenze tra i browser).

3.4.3 Algoritmi di crittografia

Le connessioni TLS sono crittografate con AES a 256 o 128 bit. All'avvio una negoziazione decide tra queste due opzioni.

Nessuna password viene memorizzata in chiaro all'interno dello IED. Nello IED è memorizzata una rappresentazione con hash delle password con SHA 512. Non sono accessibili dall'esterno tramite nessuna porta.

3.5 HMI Web

WHMI è l'unico servizio di accesso utente nel dispositivo di protezione. Per fornire crittografia e identificazione sicura nella comunicazione con WHMI, il dispositivo supporta il protocollo HTTPS. In questo caso la richiesta di connessione HTTP semplice viene automaticamente cambiata in HTTPS.

WHMI richiede un browser Web moderno, con supporto per HTML5 ed ECMAScript 6. Tenere presente che Internet Explorer non è supportato. È richiesta una comunicazione sicura con TLS v1.2 o v1.3.

WHMI è verificato con le ultime versioni di Microsoft Edge, Firefox e Google Chrome.

WHMI richiede sempre l'autenticazione utente. Dopo aver effettuato con successo l'accesso, l'utente deve selezionare il ruolo con il quale desidera procedere.

4 Gestione degli utenti

4.1 Gestione account utente locali

La gestione degli account utente e il controllo degli accessi in base al ruolo nel relè di protezione sono stati gestiti come specificato in IEC 62351-8.

Per WHMI sono stati prestabiliti quattro account utente predefiniti di fabbrica, ciascuno con diritti e password predefinite diversi. I ruoli per questi quattro account utente corrispondono ai nomi utente.

Tabella 3: Mostra quattro utenti predefiniti di fabbrica, i rispettivi ruoli e le rispettive password predefinite

Quattro utenti predefiniti di fabbrica	Ruolo	Password predefinita
VIEWER	VIEWER	remote0001
OPERATOR	OPERATOR	remote0002
ENGINEER	ENGINEER	remote0003
ADMINISTRATOR	ADMINISTRATOR	remote0004

Le password predefinite nel relè di protezione fornito dalla fabbrica possono essere modificate con diritti utente amministratore o dagli utenti stessi.

Le password utente del relè possono essere cambiate tramite WHMI o lo strumento IED Users in PCM600.

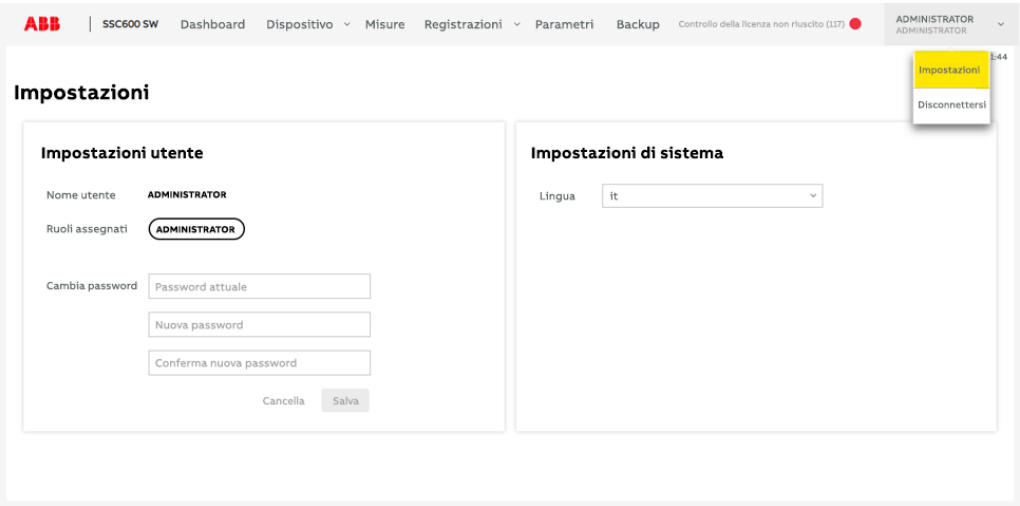


Figura 2. Visualizzazione dell'opzione Change password in WHMI (gli utenti stessi possono cambiarla qui)

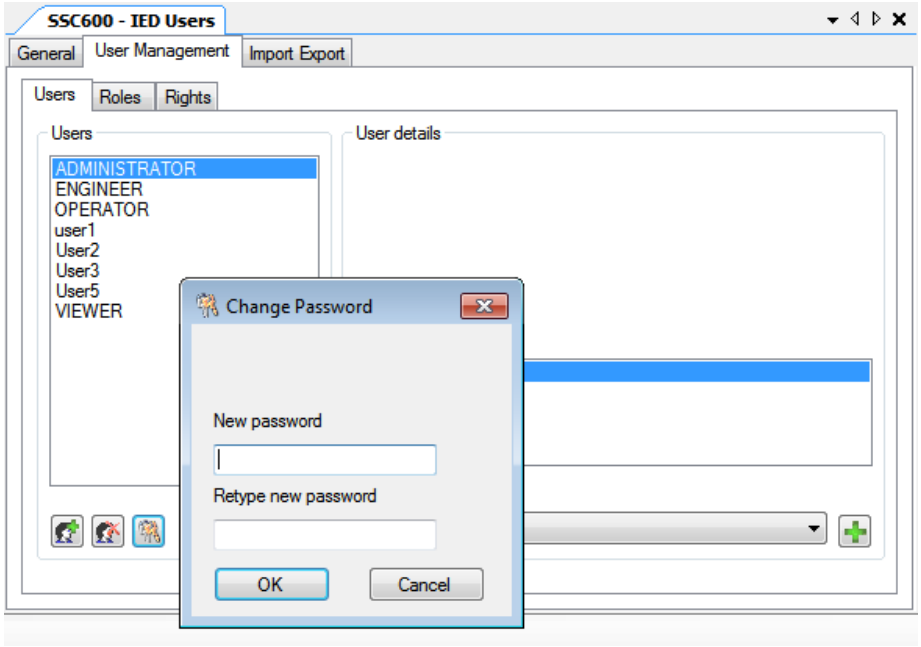


Figura 3. Visualizzazione dell'opzione Change password in PCM600. (l'utente con diritto di gestione utenti può cambiarla qui)

Oltre agli account utente predefiniti, è possibile aggiungerne altri con otto ruoli predefiniti per il relè di protezione da IED Users in PCM600.

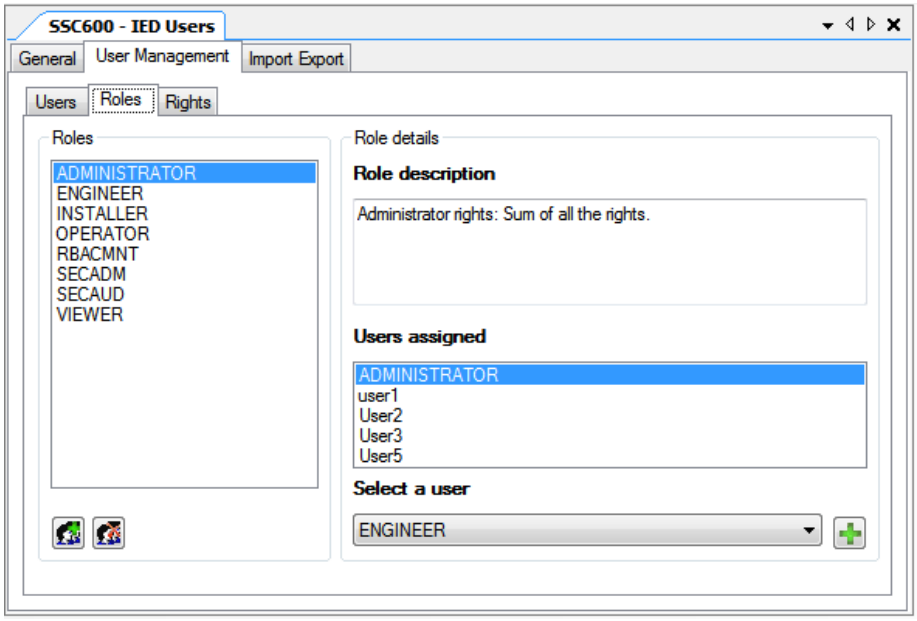


Figura 4. Visualizzazione di otto ruoli predefiniti in PCM600

Questi ruoli vengono quindi associati ai diritti utente.

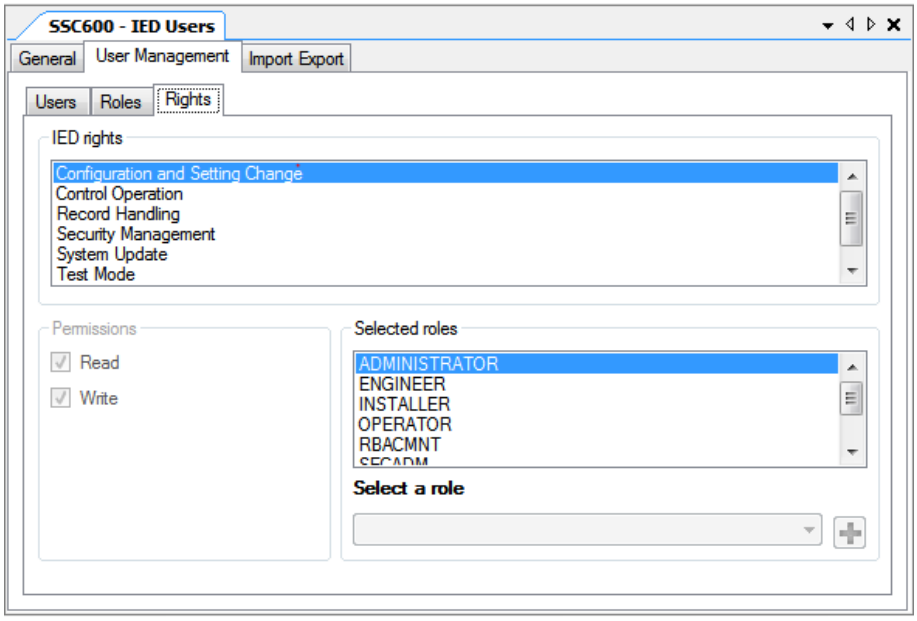


Figura 5. Visualizzazione della mappatura dei ruoli e dei diritti

Per poter aggiungere ulteriori ruoli predefiniti e mapparli sui diritti utente, è necessario accedere come utente con ruolo che dispone del diritto di gestione utenti in PCM600. I ruoli definiti dell'utente possono essere aggiunti al relè di protezione.

Ciascun relè di protezione supporta otto ruoli fissi e 50 account utente appartenenti a uno qualsiasi di questi ruoli. Ciascun account utente può essere mappato su un massimo di otto ruoli.

Lo strumento IED Users in PCM600 è utilizzato per gestire gli account utente locali.

- Gli account utente possono essere creati e assegnati con qualsiasi ruolo predefinito (VIEWER, OPERATOR, ENGINEER e ADMINISTRATOR) o ruoli aggiuntivi (INSTALLER, SECADM, SECAUD e RBACMNT)
- L'utente con ruolo (ruolo mappato sul diritto di gestione utenti) può creare account utente e aggiornare la mappatura dei diritti rispetto ai ruoli.
- L'utente con ruolo (ruolo mappato sul diritto di gestione utenti) deve condividere con gli utenti la password predefinita generata dallo strumento per l'account utente e consigliare all'utente di cambiarla.
- La password degli account utente può essere cambiata dagli utenti stessi da PCM600 o da WHMI.
- L'utente con ruolo (ruolo mappato sul diritto di gestione utenti) può reimpostare le password degli utenti.

Le informazioni sull'account utente vengono quindi scritte sul relè di protezione da IED Users in PCM600. Le informazioni sull'account utente sono conservate al sicuro nel relè di protezione.

Qualsiasi utente che accede al relè di protezione da WHMI (HTTPS) o PCM600 (FTPS) viene autenticato in base alle informazioni sull'account utente nel relè.

Tabella 4: Ruoli utente predefiniti

Ruolo	Descrizione
VIEWER	Può essere utilizzato per visualizzare quali oggetti sono presenti all'interno del dispositivo logico
SECAUD	Può essere utilizzato per la gestione dei record e per visualizzare i registri di verifica
OPERATOR	Può essere utilizzato per visualizzare quali oggetti sono presenti all'interno del dispositivo logico nonché per eseguire operazioni di controllo come l'apertura o la chiusura dell'interruttore.
INSTALLER	Può essere utilizzato per visualizzare quali oggetti sono presenti all'interno del dispositivo logico nonché per scrivere file e configurare il server localmente o in remoto.
ENGINEER	Può essere utilizzato per visualizzare quali oggetti sono presenti all'interno del dispositivo logico nonché per apportare modifiche alle impostazioni dei parametri e alla configurazione, oltre ad avere pieno accesso ai set di dati e ai file.
RBACMNT	Può essere utilizzato per gestire la mappatura dei diritti rispetto ai ruoli.
SECADM	Può essere utilizzato per eseguire la gestione della sicurezza come la mappatura dei diritti rispetto ai ruoli e per modificare impostazioni di sicurezza come i certificati per l'autenticazione del soggetto.
ADMINISTRATOR	Ha a disposizione tutti i ruoli

La *Tabella 5* descrive la mappatura predefinita di tutti i diritti utente associati a tutti i ruoli del relè di protezione. Questa mappatura può essere modificata in base alle esigenze dell'utente.

Tabella 5: Mappatura Dai ruoli predefiniti ai diritti

Possibili azioni/ diritti dell'utente	VIEWER	SECAUD	OPERATOR	INSTALLER	ENGINEER	RBACMNT	SECADM	ADMINISTRATOR
Configurazione e modifica delle impostazioni	No	No	No	No	Sì	No	No	Sì
Operazioni di controllo	No	No	Sì	No	No	No	No	Sì
Gestione degli utenti	No	No	No	No	No	Sì	Sì	Sì

La tabella continua nella pagina successiva

Possibili azioni/ diritti dell'utente	VIEWER	SECAUD	OPERATOR	INSTALLER	ENGINEER	RBACMNT	SECADM	ADMINISTRATOR
Gestione della sicurezza	No	Sì	No	No	No	No	Sì	Sì
Modalità Test	No	No	No	No	Sì	No	No	Sì
Gestione delle registrazioni	No	Sì	No	No	No	No	No	Sì
Aggiornamento del sistema	No	No	No	No	No	No	Sì	Sì

Le autorizzazioni e i diritti menzionati nello standard IEC 62351-8 sono coperti direttamente o da una combinazione dei diritti menzionati in *Tabella 5*. In PCM600 i diritti vengono gestiti come Read/Write/None (Lettura/Scrittura/Nessuno) anziché Sì/No. Se il diritto None non è applicabile per un'azione (ad esempio la modalità Test), verrà impostato automaticamente il diritto di lettura.

Le informazioni sull'account utente possono essere esportate da IED Users in PCM600 in un file criptato che può essere importato in un altro relè di protezione.

WHMI richiede sempre l'autenticazione. Le modifiche alle impostazioni di *gestione degli utenti* non causano il riavvio del relè di protezione. Le modifiche vengono applicate immediatamente dopo la conferma delle impostazioni modificate a livello principale del menu.

Nome utente e password sono sempre obbligatori per la comunicazione con il relè sui protocolli FTP/FTPS e HTTPS.

Se l'autenticazione PCM600 è stata abilitata nelle impostazioni di sistema PCM600, un utente del relè può essere collegato all'utente PCM600 corrente selezionando la casella di controllo Remember me nella finestra di dialogo Login. In seguito, le credenziali dell'utente non vengono più richieste durante la comunicazione con lo strumento, poiché l'accesso a PCM600 fornisce anche le credenziali di autenticazione al relè di protezione.

All'utente con diritto di gestione utenti non sarà consentito eliminare l'ultimo utente con diritto di gestione utenti e sé stesso. Il login FTP/FTPS si effettua inserendo il nome utente e la password; non è richiesta la selezione del ruolo. Il ruolo più alto per il nome utente viene selezionato automaticamente dal relè di protezione. Eseguendo l'operazione di ripristino delle *impostazioni di fabbrica* in IED Users in PCM600, gli account utente vengono ripristinati su quelli di fabbrica. I diritti di lettura nella mappatura dei diritti rispetto ai ruoli possono essere disabilitati ma vengono sempre ripristinati quando i ruoli vengono letti dal relè di protezione nella sezione sulla mappatura dei ruoli sui diritti di IED Users o dello strumento Account Management in PCM600.

4.1.1 Politiche relative alle password

Le password sono impostabili per gli account utente in tutti i ruoli. Sono accettati solo i seguenti caratteri.

- Numeri da 0 a 9
- Lettere a-z, A-Z
- Spazio
- Caratteri speciali !"#%&'()*+´-./:;<=>?@[\]^_`{|}~

Per impostazione predefinita, i criteri relativi alle password nel relè di protezione sono i seguenti:

- Lunghezza minima della password: 9
- Lunghezza massima della password: 20
- Caratteri minimi maiuscoli: 0
- Minimo numerico: 0
- Caratteri minimi speciali: 0

I relè di protezione vengono forniti dalla fabbrica con password predefinite. È necessario cambiare le password predefinite.

Tabella 6: Ruoli predefiniti e password predefinite

Nome utente	Password (client remoti/WHMI)
VIEWER	remote0001
OPERATOR	remote0002
ENGINEER	remote0003
ADMINISTRATOR	remote0004

I seguenti aspetti delle politiche relative alle password possono essere personalizzati in IED Users in PCM600.

- Possibilità di abilitare o disabilitare i criteri delle password (disabilitare i criteri predefiniti come descritto sopra)
- Lunghezza minima della password
- Lunghezza massima della password
- Uso di caratteri maiuscoli
- Uso di caratteri minuscoli
- Uso di numeri
- Uso di caratteri speciali

Per modificare le politiche delle password, è necessario accedere come utente (che dispone del diritto di gestione utenti) in PCM600.

Ogni utente può cambiare la propria password, ma solo l'utente con diritto di gestione utenti può reimpostare le password degli altri utenti.

Con il ripristino di fabbrica, vengono ripristinati i nomi utente, le password e i criteri di password predefiniti.

Per l'autorizzazione utente per PCM600, vedere la documentazione su PCM600.

Non è consentito cambiare il criterio e la configurazione utente quando il relè di protezione è in modalità offline in PCM600.

Se si perde l'ultimo utente con la password del diritto di gestione utenti, contattare l'assistenza tecnica clienti di ABB.

5 Registrazione di sicurezza

5.1 Tracciamento di verifica

Il dispositivo di protezione offre un'ampia serie di funzioni di registrazione degli eventi. Gli eventi critici relativi alla sicurezza del sistema e del dispositivo di protezione vengono registrati in un tracciamento di verifica non volatile separato per l'amministratore.

Il tracciamento di verifica è una registrazione cronologica delle attività del sistema che consente di ricostruire ed esaminare la sequenza degli eventi e delle modifiche del sistema e della sicurezza nel dispositivo di protezione. Sia gli eventi del tracciamento di verifica che quelli relativi al processo possono essere esaminati e analizzati in modo coerente con l'aiuto di Event List in WHMI e di Event Viewer in PCM600.

Il dispositivo di protezione memorizza 2048 eventi del tracciamento di verifica nel tracciamento di verifica non volatile. Inoltre, 8192 eventi di processo vengono memorizzati in un elenco di eventi non volatile. Sia il tracciamento di verifica che l'elenco degli eventi funzionano secondo il principio FIFO. La memoria non volatile si basa su un tipo di memoria che non ha bisogno di batterie di backup né di cambiare regolarmente i componenti per mantenere la memoria.

Gli eventi del tracciamento di verifica relativi all'autorizzazione dell'utente (login, logout, violazione remota e violazione locale) sono definiti in base all'insieme selezionato di requisiti da IEEE 1686. La registrazione si basa su nomi utenti o categorie di utenti predefiniti. Gli eventi di tracciamento di verifica dell'utente sono accessibili con IEC 61850-8-1, PCM600 e WHMI.

Gli eventi che accadono senza utente autenticato verranno registrati con un nome utente generico.

Tabella 7: Eventi del tracciamento di verifica

ID evento	Descrizione	Gravità
1110	Login riuscito	Evento
1130	Login non riuscito - Credenziali errate	Evento
1210	Logout (l'utente ha effettuato il logout)	Evento
1320	Download/scrittura configurazione riusciti	Evento
1370	Registri eventi di sicurezza visualizzati correttamente	Allarme
1380	Modifica parametro riuscita	Evento
1420	Download/scrittura configurazione non riusciti	Evento
1520	Aggiornamento software riuscito	Evento
1610	Modifica firmware non riuscita	Evento

La tabella continua nella pagina successiva

ID evento	Descrizione	Gravità
1710	Ripristino dell'impostazione predefinita del dispositivo	Evento
2110	Account utente creato correttamente	Allarme
2120	Account utente eliminato correttamente	Allarme
2180	Nuovo ruolo creato correttamente	Allarme
2190	Cancellazione del ruolo riuscita	Allarme
2210	Password utente modificata correttamente	Evento
2220	Modifica della password utente non riuscita	Evento
5110	Reset firmware	Allarme
5140	Ripristino software	Allarme
5270	Avvio del sistema	Allarme
6110	Modalità di test avviata correttamente	Allarme
6120	Modalità di test terminata correttamente	Allarme
6130	Operazione di controllo eseguita correttamente	Allarme
6220	Ora sincronizzata correttamente	Evento
6320	Sincronizzazione dell'ora non riuscita	Evento
8020	Data e ora impostate correttamente	Evento
9020	Rilevato un attacco di flooding	Allarme
13520	Certificati trasferiti al dispositivo correttamente	Evento
14520	Impossibile trasferire i certificati nel dispositivo	Evento

Lo strumento Event Viewer di PCM600 può essere utilizzato per visualizzare gli eventi tracciamento di verifica e quelli relativi al processo. Gli eventi tracciamento di verifica sono visibili dalla vista Security events dedicata. L'utente con diritto di gestione della sicurezza può leggere il tracciamento di verifica. Il tracciamento di verifica non può essere resettato ma Event Viewer PCM600 può filtrare i dati. Gli eventi tracciamento di verifica possono essere configurati per essere visibili anche nell'elenco degli eventi WHMI insieme agli eventi relativi al processo.

In WHMI, gli eventi tracciamento di verifica vengono visualizzati in base ai diritti utente. Un utente con diritti di gestione della sicurezza può visualizzare i registri dei tracciamenti di verifica

5.2 Central Activity Logging

Gli eventi di tracciamento di verifica possono essere segnalati dal relè a un server CAL (Central Activity Logging) in formato Syslog. Il relè è il client CAL e invia gli eventi a un server CAL che può essere SDM600 o qualsiasi altro strumento in grado di gestire il formato Syslog.

Al relè di protezione possono essere collegati al massimo due server CAL. Per abilitare la registrazione degli eventi di verifica di tracciamento su un server Syslog, la funzione di registrazione dell'attività dell'utente deve essere abilitata nel relè di protezione e i parametri devono essere impostati per ciascun server UAL a cui è richiesto di inviare gli eventi di tracciamento di verifica.

Tabella 8: Configurazione di Central Activity Logging

Parametro	Opzioni	Descrizione
Enable UAL	Enable	Abilita la registrazione dell'attività dell'utente sul server CAL
	Disable (impostazione predefinita)	Disabilita la registrazione dell'attività dell'utente sul server CAL
Server IP	User-entered value	Indirizzo IP del server CAL
Communication type	UDP (predefinito)	Utilizza UDP per la comunicazione con il server CAL
	TCP	Utilizza TCP per la comunicazione con il server CAL
Communication port	514 (predefinito)	Porta utilizzata per UDP
	1468	Porta utilizzata per TCP

Può essere fatto in **Main menu** > **Configuration** > **User Activity Log** da LHMI, WHMI o Parameter Setting in PCM600. Anche il server CAL deve essere configurato con i dettagli del relè.

- Port number: Uguale al numero di porta impostato nel relè
- IP address: Indirizzo IP del relè da cui il server CAL riceve gli eventi del registro

Per la sicurezza complessiva del sistema, è importante garantire una comunicazione sicura tra SSC600 e il server CAL. Ulteriori informazioni sul rafforzamento del sistema sono disponibili in *Capitolo 3.1 Regole di base per il rafforzamento del sistema*.

Gli eventi registrati nel server Syslog contengono le seguenti informazioni:

- Data e ora in cui si è verificato l'evento
- ID evento: Ogni evento ha un ID di sicurezza univoco
- Numero di serie (numero SOE): Si tratta di un numero progressivo che indica la sequenza in cui si è verificato l'evento
- Nome utente e ruolo: L'utente che ha eseguito l'evento e il ruolo associato a tale utente
- Gravità: Se si tratta di un evento di sicurezza o di un avviso
- Informazioni aggiuntive: Contiene ulteriori informazioni utili sull'evento

Se un evento si verifica mentre la comunicazione con il server CAL non è accessibile, gli eventi non verranno ritrasmessi. In questo caso, utilizzare Event Viewer in PCM600 per leggere la registrazione dell'attività dal relè di protezione.

Il relè di protezione supporta solo la versione 1 di Syslog.

6 Utilizzo di HMI Web

Poiché la comunicazione sicura è abilitata per impostazione predefinita, è necessario accedere a WHMI da un browser Web tramite il protocollo HTTPS. Accedere con i diritti utente appropriati per utilizzare WHMI.

Per stabilire una connessione WHMI remota allo IED, contattare l'amministratore di rete per verificare le regole aziendali per IP e connessioni remote.

Disabilitare le impostazioni proxy del browser Web o fare un'eccezione alle regole proxy per consentire la connessione WHMI dello IED, ad esempio includendo l'indirizzo IP dello IED in **Internet Options** > **Connections** > **LAN Settings** > **Advanced** > **Exceptions**.

6.1 Inizio sessione

1. Aprire un browser Web supportato.
2. Digitare l'indirizzo IP dello IED nella barra degli indirizzi e premere INVIO.
3. Digitare il nome utente con le lettere maiuscole.
4. Digitare la password.

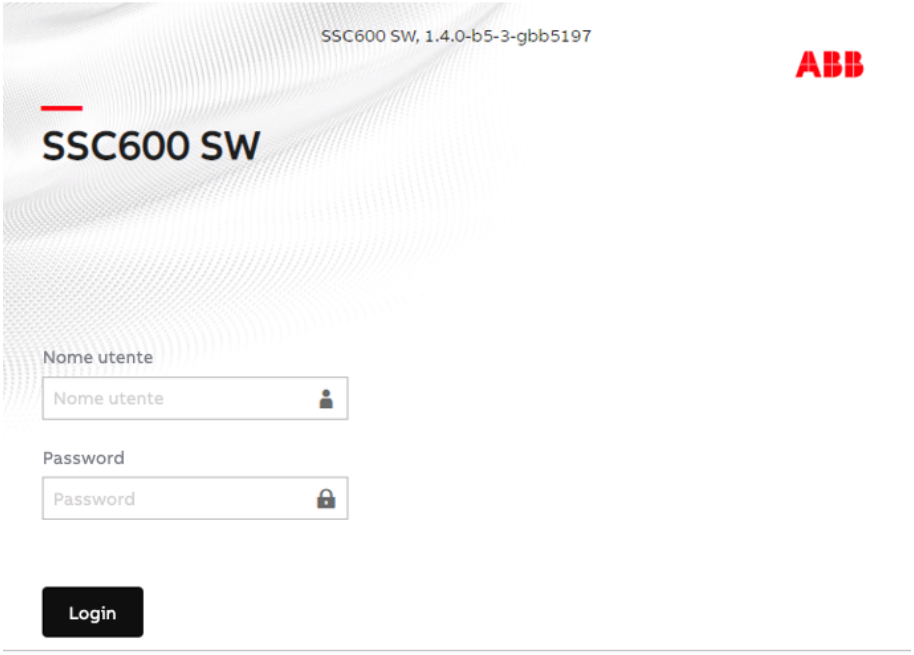


Figura 6. Immissione di nome utente e password per utilizzare WHMI

5. Fare clic su **OK**.
6. Selezionare dall'elenco degli utenti disponibili il ruolo da utilizzare. Nel caso in cui sia disponibile un solo ruolo, verrà selezionato automaticamente.

6.2 Termine sessione

L'utente viene disconnesso allo scadere della sessione. È possibile impostare il timeout in **IED Configuration** > **HMI** > **Web HMI timeout**.

- Per disconnettersi manualmente, selezionare **Logout** nella barra View.

7 Protezione della configurazione del dispositivo e del sistema

7.1 File di backup

I backup non fanno direttamente parte della sicurezza informatica ma sono importanti per velocizzare il processo di ripristino, ad esempio in caso di guasto del dispositivo di protezione. Quando vengono apportate modifiche alla configurazione, i backup devono essere aggiornati.

7.1.1 Creazione di un backup dalla configurazione del dispositivo

1. Utilizzare la funzione "Read from IED" dal menu contestuale dello IED in PCM600 per eseguire il backup della configurazione del dispositivo.

   Per poter utilizzare lo strumento, è richiesta l'autorizzazione utente.

2. Se la password amministratore predefinita è stata modificata, immettere le credenziali utente.

   Per l'autorizzazione sono richieste le credenziali di un utente con diritto di impostazioni di configurazione.

7.1.2 Creazione di un backup dal progetto PCM600

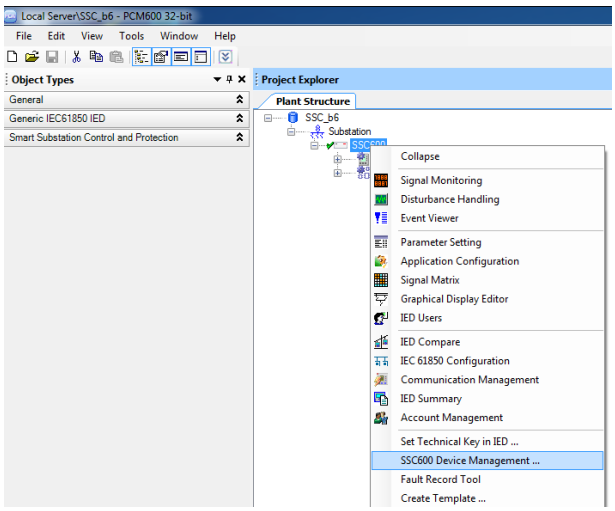
Il backup dal progetto PCM600 viene realizzato esportando il progetto.

1. Sul menu **File**, fare clic su **Open** > **Manage Project** per aprire la gestione del progetto.
2. Selezionare il progetto dalla finestra di dialogo **Currently available projects**.
3. Fare clic con il pulsante destro del mouse sul progetto e selezionare **Export Project** per aprire la finestra di dialogo **Create target file for the project export**.
4. Sfogliare la posizione di destinazione e digitare il nome del file esportato. Tutti i dati relativi al progetto vengono compressi e salvati in un file, denominato e posizionato in base alle definizioni.

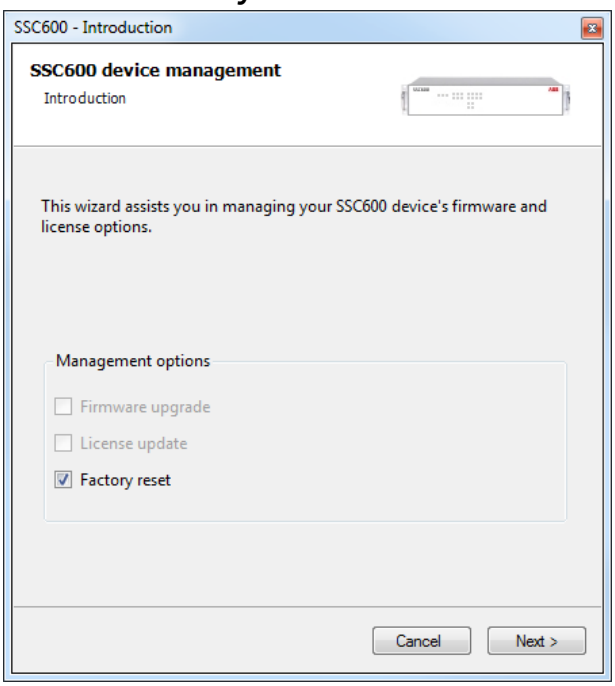
7.2 Ripristino delle impostazioni di fabbrica

In caso di perdita di dati di configurazione o di qualsiasi altro errore del file system che impedisca il corretto funzionamento del dispositivo di protezione, è possibile riportare l'intero file system allo stato originale di fabbrica. Vengono ripristinati tutti i file di configurazione e tutte le impostazioni predefinite memorizzate in fabbrica. Solo un utente con diritto di aggiornamento del sistema (fare riferimento alla tabella Dai ruoli predefiniti ai diritti nelle Linee guida per la distribuzione della sicurezza informatica) (ad esempio ADMINISTRATOR) può ripristinare le impostazioni di *fabbrica*.

1. Nella vista **Plant Structure**, fare clic con il pulsante destro del mouse sul dispositivo e selezionare **SSC600 Device Management**.



2. Selezionare **Factory reset** e fare clic su **Next**.



3. Fare clic su **Reset**.

4. Fare clic su **Finish**.

Il dispositivo di protezione ripristina le impostazioni di fabbrica e si riavvia. Il ripristino richiede 1...3 minuti. La conferma del ripristino delle impostazioni di fabbrica viene visualizzata sul display per alcuni secondi, dopodiché il dispositivo si riavvia.

Evitare di ripristinare impostazioni di fabbrica inutili, perché tutte le impostazioni dei parametri scritte in precedenza sul dispositivo saranno

sovrascritte con i valori predefiniti. Durante il normale utilizzo, una modifica improvvisa delle impostazioni può causare l'intervento di una funzione di protezione.

7.3 Ripristino della password persa

Se l'autenticazione è abilitata nel dispositivo di protezione e l'ultimo utente con password User Management Right va perso, non è più possibile modificare le password.

- Contattare il supporto tecnico clienti ABB per ripristinare l'accesso a livello di gestione utenti al dispositivo di protezione.

8 Glossario

AD	Directory attiva
BDEW	Bundesverband der Energie- und Wasserwirtschaft
CA	Autorità certificativa
CAL	Central Activity Logging
CAM	Centralized Account Management
DAA	HTTP Digest Access Authentication
DNP3	Un protocollo di rete distribuito sviluppato originariamente da Westronic. Il DNP3 Users Group ha la proprietà del protocollo e si assume la responsabilità della sua evoluzione.
DOM	Modulo di uscita binaria, quattro canali
DPC	Double-Point Control
EMC	Compatibilità elettromagnetica
Ethernet	Uno standard per collegare una famiglia di tecnologie di rete per computer basate su frame in una LAN
FIFO	First In, First Out
FTP	Protocollo di trasferimento file
FTPS	FTP Sicuro
GOOSE	Generic Object-Oriented Substation Event
HMI	Interfaccia uomo-macchina
HTML	HyperText Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IEC 60870-5-104	Accesso di rete secondo IEC 60870-5-104 (IEC 104)
IEC 61850	Standard internazionale per la comunicazione e la modellazione delle sottostazioni
IEC 61850-8-1	Un protocollo di comunicazione basato sulla serie di norme IEC 61850
IED	Intelligent Electronic Device (dispositivo di protezione e controllo)
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEEE 1588 v2	Standard per un protocollo di sincronizzazione dell'orologio di precisione per sistemi di misurazione e controllo in rete
IEEE 1686	Standard per le capacità di sicurezza informatica dei dispositivi elettronici intelligenti (IED) delle sottostazioni
IP	Protocollo Internet
Indirizzo IP	Una serie di quattro numeri compresi tra 0 e 255, separati da punti. A ogni server connesso a Internet viene assegnato un indirizzo IP esclusivo che specifica la posizione per il protocollo TCP/IP.
ISO	International Standard Organization
LHMI	Interfaccia uomo-macchina locale
MMS	1. Manufacturing Message Specification 2. Metering Management System

NERC CIP	North American Electric Reliability Corporation - Critical Infrastructure Protection
PCM600	Protection and Control IED Manager
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
R-GOOSE	Routable GOOSE
RJ-45	Tipo di connettore galvanico
SDM600	Una soluzione software per la gestione automatica dei dati rilevanti per il servizio e la sicurezza informatica nelle sottostazioni
SMV	Sampled Measured Values (valori misurati campionati)
SNTP	Simple Network Time Protocol
TCP	Protocollo di controllo della trasmissione
TCP/IP	Protocollo di controllo della trasmissione/protocollo Internet
UDP	User Datagram Protocol
VPN	Virtual Private Network (rete privata virtuale)
WHMI	Interfaccia uomo-macchina basata su Web

—
ABB Distribution Solutions
Digital Substation Products
P.O. Box 699
FI-65101 VAASA, Finland
Phone +358 10 22 11

www.abb.com/mediumvoltage
www.abb.com/relion
www.abb.com/substationautomation

© Copyright 2023 ABB. All rights reserved.

2NGA002113 A