



EcoStruxure Panel Server

Guida alla sicurezza informatica

Concentratore di dispositivi wireless e gateway Modbus, datalogger ed Energy Server

EcoStruxure offre architettura e piattaforma abilitata a IoT.

DOCA0211IT-11
01/2025



Informazioni di carattere legale

Le informazioni contenute nel presente documento contengono descrizioni generali, caratteristiche tecniche e/o raccomandazioni relative ai prodotti/soluzioni.

Il presente documento non è inteso come sostituto di uno studio dettagliato o piano schematico o sviluppo specifico del sito e operativo. Non deve essere utilizzato per determinare idoneità o affidabilità dei prodotti/soluzioni per applicazioni specifiche dell'utente. Spetta a ciascun utente eseguire o nominare un esperto professionista di sua scelta (integratore, specialista o simile) per eseguire un'analisi del rischio completa e appropriata, valutazione e test dei prodotti/soluzioni in relazione all'uso o all'applicazione specifica.

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nel presente documento sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari.

Il presente documento e il relativo contenuto sono protetti dalle leggi vigenti sul copyright e vengono forniti esclusivamente a titolo informativo. Si fa divieto di riprodurre o trasmettere il presente documento o parte di esso, in qualsiasi formato e con qualsiasi metodo (elettronico, meccanico, fotocopia, registrazione o altro modo), per qualsiasi scopo, senza previa autorizzazione scritta di Schneider Electric.

Schneider Electric non concede alcun diritto o licenza per uso commerciale del documento e del relativo contenuto, a eccezione di una licenza personale e non esclusiva per consultarli "così come sono".

Schneider Electric si riserva il diritto di apportare modifiche o aggiornamenti relativi al presente documento o ai suoi contenuti o al formato in qualsiasi momento senza preavviso.

Nella misura in cui sia consentito dalla legge vigente, Schneider Electric e le sue consociate non si assumono alcuna responsabilità od obbligo per eventuali errori od omissioni nel contenuto informativo del presente materiale, o per qualsiasi utilizzo non previsto o improprio delle informazioni ivi contenute.

Sommario

Informazioni di sicurezza	5
Informazioni sul documento	6
Introduzione alla sicurezza informatica	9
Caratteristiche del dispositivo	10
Caratteristiche del dispositivo	12
Sicurezza di rete	14
Sicurezza delle applicazioni cloud	17
Sicurezza fisica del dispositivo	18
Raccomandazioni sulla sicurezza per la manutenzione	19
Glossario	21

Informazioni di sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.



L'aggiunta di questo simbolo a un'etichetta di "Pericolo" o "Avvertimento" indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.



Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un **AVVISO** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

Nota

Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Informazioni sul documento

Ambito del documento

Questa guida fornisce informazioni sugli aspetti di sicurezza informatica per EcoStruxure™ Panel Server, per consentire agli operatori e ai progettisti di sistema di promuovere un ambiente operativo sicuro per il prodotto.

Questa guida non tratta l'argomento più generale relativo alla protezione della rete tecnologica operativa o della rete Ethernet aziendale. Per un'introduzione generale alle minacce alla sicurezza informatica e come affrontarle, vedere *Informazioni generali sulla sicurezza informatica*, pagina 6.

NOTA: in questa guida, il termine **sicurezza** è utilizzato per indicare la sicurezza informatica.

Nota sulla validità

Le informazioni contenute in questa guida sono relative a EcoStruxure Panel Server.

Informazioni online

Le informazioni contenute in questa guida potrebbero venire aggiornate in qualsiasi momento. Schneider Electric consiglia di avere la versione più recente e aggiornata disponibile su www.se.com/ww/en/download.

Le caratteristiche tecniche dei dispositivi descritti in questo documento sono consultabili anche online. Per accedere alle informazioni online, consultare la homepage di Schneider Electric a www.se.com.

Informazioni generali sulla sicurezza informatica

Negli ultimi anni, il numero crescente di macchine e impianti di produzione collegati in rete ha visto un corrispondente aumento del potenziale di minacce informatiche, come accessi non autorizzati, violazioni dei dati e interruzioni operative. È pertanto necessario prendere in considerazione tutte le possibili misure di sicurezza informatica per proteggere risorse e sistemi da tali minacce.

Per consentire di mantenere i prodotti Schneider Electric sicuri e protetti, è nell'interesse dell'utente implementare le pratiche migliori di sicurezza informatica come indicato nel documento *Cybersecurity Best Practices*:

Schneider Electric fornisce ulteriori informazioni e assistenza:

- Iscrivere alla newsletter sulla sicurezza Schneider Electric.
- Visitare la pagina Web *Cybersecurity Support Portal* per:
 - Trovare notifiche di sicurezza.
 - Segnalare vulnerabilità e incidenti.
- Visitare la pagina Web *Schneider Electric Cybersecurity and Data Protection Posture* per:
 - Accedere alla postura di sicurezza informatica.
 - Ulteriori informazioni sulla sicurezza informatica nell'accademia di sicurezza informatica.
 - Esplorare i servizi di sicurezza informatica di Schneider Electric.

Informazioni relative alla sicurezza informatica del prodotto

⚠ AVVERTIMENTO
POSSIBILITÀ DI COMPROMETTERE LA DISPONIBILITÀ, L'INTEGRITÀ E LA CONFIDENZIALITÀ DEL SISTEMA. • Disattivare le porte/i servizi non utilizzati per ridurre al minimo i percorsi degli attacchi dannosi. • Inserire i dispositivi di rete all'interno di numerosi livelli di difesa (come firewall, segmentazione della rete e rilevamento e protezione dalle intrusioni nella rete). • Seguire le procedure consigliate per la sicurezza informatica (ad esempio, minimo privilegio, separazione delle mansioni) per evitare esposizione non autorizzata, perdita o malfunzionamento di dati e registri o interruzione dei servizi. Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Lingue disponibili per il documento

Il documento è disponibile nelle seguenti lingue:

- Inglese (DOCA0211EN)
- Francese (DOCA0211FR)
- Tedesco (DOCA0211DE)
- Italiano (DOCA0211IT)
- Portoghese (DOCA0211PT)
- Spagnolo (DOCA0211ES)

Documenti correlati

Titolo della documentazione	Codice prodotto
<i>EcoStruxure Panel Server - Guida utente</i>	DOCA0172EN DOCA0172DE DOCA0172ES DOCA0172FR DOCA0172IT DOCA0172PT
<i>Migliori prassi relative alla sicurezza informatica</i>	7EN52-0390
<i>EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide</i>	ESXP2TG003EN

Per scaricare queste pubblicazioni tecniche e altre informazioni di carattere tecnico, consultare il sito www.se.com/ww/en/download/.

Informazioni sulla terminologia non inclusiva o non sensibile

In qualità di azienda responsabile e inclusiva, Schneider Electric aggiorna costantemente le sue comunicazioni e i suoi prodotti che contengono una terminologia non inclusiva o indelicata. Tuttavia, nonostante questi sforzi, i nostri contenuti possono ancora contenere termini ritenuti inappropriati da alcuni clienti.

Marchi

QR Code è un marchio registrato di DENSO WAVE INCORPORATED in Giappone e in altri paesi.

Introduzione alla sicurezza informatica

EcoStruxure Gamma Master

EcoStruxure è un'architettura e una piattaforma abilitata all'IoT di Schneider Electric, plug-and-play, aperta e interoperabile, in ambienti domestici, edifici, data center, infrastruttura e industrie. Innovazione in ogni livello dai prodotti connessi a Edge Control, app, analisi e servizi.

Introduzione

La sicurezza informatica ha lo scopo di proteggere la rete di comunicazione e tutte le apparecchiature ad essa collegate da attacchi che potrebbero disturbare le operazioni (disponibilità), modificare i dati (integrità) o fornire informazioni riservate (riservatezza). L'obiettivo della sicurezza informatica è quello di garantire un livello più elevato di protezione dei dati e delle risorse fisiche da furti, danneggiamento, abusi o incidenti, pur mantenendo l'accesso per gli utenti a cui sono destinate. La sicurezza informatica presenta molti aspetti, tra cui la progettazione di sistemi sicuri, la limitazione dell'accesso mediante metodi fisici e digitali, l'identificazione degli utenti, l'implementazione di procedure di sicurezza e di procedure ottimali.

Linee guida Schneider Electric

Oltre alle raccomandazioni fornite in questa guida e specifiche per Panel Server, è necessario seguire l'approccio Schneider Electric di difesa in profondità alla sicurezza informatica e le informazioni generali sulla sicurezza informatica, pagina 6.

Politiche e regole di sicurezza informatica di Schneider Electric

Schneider Electric utilizza un processo SDL (Secure Development Lifecycle), una struttura chiave basata sullo sviluppo dei prodotti che consente di garantire che i prodotti seguano processi di progettazione sicuri in tutte le fasi del ciclo di vita. Il processo SDL di Schneider Electric è conforme a IEC 62443-4.1.

Il processo SDL include:

- Procedure SDL applicate alle azioni di sviluppo interno, in tutta la catena di approvvigionamento.
- Verifica della sicurezza finale necessaria per la versione del progetto.
- Formazione sulla sicurezza per il personale coinvolto nello sviluppo del prodotto.

Caratteristiche del dispositivo

Panoramica

EcoStruxure Panel Server è dotato di funzionalità di sicurezza. Queste funzioni sono preconfigurate e possono essere modificate per rispondere alle esigenze di installazione. Panel Server deve essere configurato e impostato solo da personale qualificato, in quanto la disattivazione o la modifica delle impostazioni influisce sulla sicurezza generale di Panel Server e della sicurezza di rete.

Utilizzare questa guida insieme con DOCA0172•• *EcoStruxure Panel Server - Guida utente*, pagina 7 per una configurazione dettagliata delle funzioni e delle impostazioni di Panel Server.

Interfacce di EcoStruxure Panel Server

La tabella seguente riassume le architetture di comunicazione disponibili con Panel Server per modello:

Caratteristiche principali		EcoStruxure Panel Server								
		Entry	Universal					Advanced		
		PAS400	PAS600	PAS600T	PAS600L	PAS600LWD	PAS600PWD	PAS800	PAS800L	PAS800P
Ethernet 10/100BASE-T	Una porta RJ45	✓	-	-	-	-	-	-	-	-
	Due porte RJ45	-	✓	✓	✓	✓	✓	✓	✓	✓
Connettività Modbus TCP/IP a monte		✓	✓	✓	✓	✓	✓	✓	✓	✓
Connettività Wi-Fi a monte		✓	✓	✓	✓	-	-	✓	✓	✓
Connettività Modbus TCP/IP a valle		-	✓	✓	✓	✓	✓	✓	✓	✓
Connettività IEEE 802.15.4 a valle		✓	✓	✓	✓	-	-	✓	✓	✓
Connettività Modbus-SL a valle		-	✓	✓	✓	✓	✓	✓	✓	✓
Due ingressi digitali (per WAGES, ossia acqua, aria, gas, elettricità, vapore)		-	-	-	✓	✓	-	-	✓	-
Antenna esterna Wi-Fi		-	✓	✓	✓	-	-	✓	✓	✓
Antenna esterna IEEE 802.15.4		-	-	-	-	-	-	✓	✓	✓

Convenzione

EcoStruxure Panel Server di seguito è denominato Panel Server.

Protocolli supportati

EcoStruxure Panel Server supporta i protocolli seguenti:

- DHCP per indirizzamento IP di rete
- DNS per risoluzione del nome di rete
- DPWS per il rilevamento di rete

- HTTPS (TLS v1.2) per la configurazione tramite strumenti di configurazione e pagine Web integrate
- IEEE 802.15.4 per la comunicazione wireless che utilizza la comunicazione a radiofrequenza nella banda ISM 2.4 GHz (non disponibile per modelli Wired by Design)
- Modbus TCP e Modbus-SL per le comunicazioni con altri dispositivi OT (Operational Technology)
- NTP per sincronizzazione dell'ora
- RSTP per garantire robuste topologie ad anello Ethernet per applicazioni critiche
- SFTP per la pubblicazione di file CSV su un server SFTP
- Client VPN per accesso remoto (aperto al Centro assistenza clienti Schneider Electric)
- WPA2 e WPA per la comunicazione Wi-Fi (non disponibile per modelli Wired by Design)

Funzionalità di sicurezza

EcoStruxure Panel Server supporta le funzionalità di sicurezza seguenti:

- Su Schneider Electric è possibile installare solo firmware firmato digitalmente da Panel Server.
- A ogni avvio, la firma digitale del firmware viene convalidata prima dell'esecuzione, per assicurare che non sia stata manomessa.
- Le password utente vengono memorizzate come password salt e hash (SHA256).
- È possibile cancellare tutte le informazioni da Panel Server utilizzando il pulsante di riavvio.
- Il dispositivo è dotato di orologio interno e memorizza la data e l'ora per alcuni mesi senza alimentazione.
- La chiave di autenticità di Panel Server viene memorizzata in un chip EAL6+ CC Common Criteria estremamente sicuro.

Caratteristiche del dispositivo

Aggiornamento firmware

Aggiornare EcoStruxure Panel Server alla versione più recente del firmware per ottenere le funzionalità più recenti e mantenerlo aggiornato con le patch di sicurezza. Tutto il firmware progettato per EcoStruxure Panel Server è firmato tramite la PKI (Public Key Infrastructure) di Schneider Electric per garantire l'integrità e l'autenticità del firmware in esecuzione su EcoStruxure Panel Server. Per un corretto funzionamento della PKI, mantenere sincronizzata la data del dispositivo (vedere [Data e ora](#), pagina 12).

Per informazioni sugli aggiornamenti relativi alla sicurezza, effettuare la registrazione alle [Security Notifications](#) sul portale per il supporto alla sicurezza informatica di Schneider Electric.

Data e ora

È importante mantenere la data e l'ora sincronizzate per i seguenti scopi:

- Evitare errori nei certificati e nelle firme digitali in EcoStruxure Panel Server
- Fornire una orodatazione precisa nei registri di audit per supporto della sicurezza legale

Per ulteriori informazioni su data e ora, vedere [DOCA0172• EcoStruxure Panel Server - Guida utente](#), pagina 7.

Disattivazione delle funzionalità non utilizzate

EcoStruxure Panel Server consente di disattivare porte/servizi non utilizzati per ridurre al minimo i percorsi degli attacchi dannosi.

Si consiglia di disattivare:

- Attivazione Wi-Fi e infrastruttura Wi-Fi. Wi-Fi può essere disattivato in modo permanente, se necessario.
- Punto di accesso Wi-Fi (attivato per impostazione predefinita). Quando il punto di accesso è disattivato, premendo il pulsante sul lato anteriore di Panel Server non si ottiene l'attivazione del punto di accesso. La disattivazione dell'attivazione Wi-Fi disattiva anche il punto di accesso Wi-Fi e interrompe qualsiasi connessione attiva.
- IEEE 802.15.4 (non attivo per impostazione predefinita) IEEE 802.15.4 può essere disattivato in modo permanente.
- Servizi gateway Modbus (attivi per impostazione predefinita). Può essere disattivato su ogni interfaccia (Ethernet 1, Ethernet 2 e/o Wi-Fi) nelle pagine Web di Panel Server.
- Protocollo di rilevamento DPWS su IP v4/6 (attivo per impostazione predefinita)
- RSTP (Rapid Spanning Tree Protocol, non attivo per impostazione predefinita)

NOTA: Wi-Fi e IEEE 802.15.4 non sono disponibili sui modelli Wired by Design (WD) privi di chipset wireless.

Per ulteriori informazioni sulla disattivazione delle funzionalità non utilizzate di EcoStruxure Panel Server, vedere [DOCA0172• EcoStruxure Panel Server - Guida utente](#), pagina 7.

Porte TCP

Le porte TCP seguenti sono utilizzate in EcoStruxure Panel Server:

- Porta 443: HTTPS
- Porta 502: Modbus
- Porta 5357: DPWS (modificabile)

NOTA: Panel Server non incorpora alcun tipo di server SSH.

Registri di controllo

EcoStruxure Panel Server genera registri di controllo che registrano eventi quali tentativi di accesso non validi e aggiornamento del firmware.

I registri non contengono informazioni personali.

Per rilevare comportamenti imprevisti (ad esempio riavvio frequente, aggiornamento firmware errato o tentativi di accesso non validi), si consiglia di monitorare regolarmente i registri di controllo. Per ulteriori informazioni sui registri di diagnostica, vedere DOCA0172• *EcoStruxure Panel Server - Guida utente*, pagina 7.

Smaltimento dei dispositivi

EcoStruxure Panel Server contiene informazioni riservate configurate durante la messa in servizio, valori e registri dei dati recenti. Ad esempio, queste informazioni possono includere la topologia del dispositivo Modbus, le reti wireless, le password Wi-Fi o i consumi energetici misurati.

È necessario eseguire un reset di fabbrica prima di smaltire EcoStruxure Panel Server. Durante l'esecuzione di questa procedura è necessario disporre dell'accesso fisico per spegnere e riaccendere EcoStruxure Panel Server. Vedere come ripristinare EcoStruxure Panel Server alle impostazioni di fabbrica in DOCA0172• *EcoStruxure Panel Server - Guida utente*, pagina 7.

Sicurezza di rete

Introduzione

EcoStruxure Panel Server non è progettato per resistere all'esposizione diretta a Internet. Deve essere installato almeno dietro NAT (Network Address Translation) o preferibilmente dietro più firewall. Per ulteriori informazioni, consultare i seguenti siti Web:

- Servizi di consulenza Schneider Electric per la sicurezza informatica
- National Institute of Standards and Technology (NIST)
- Agenzia dell'Unione europea per la sicurezza informatica (ENISA)

Segmentazione della rete

EcoStruxure Panel Server è un gateway e crea un bridge tra reti diverse. La segmentazione della rete contribuisce ad assicurare la difesa dagli attacchi informatici. Per migliorare la segmentazione della rete, Panel Server Universal e Advanced dispongono di due porte Ethernet che possono essere sfruttate in modalità separata per avere una porta dedicata al settore IT (Information Technology) e una porta dedicata alla tecnologia operativa (OT). La segmentazione della rete consente di mantenere segmentate le reti OT e IT, poiché i pacchetti di rete non vengono inoltrati da una all'altra.

Si consiglia di configurare la rete in modalità separata (per ulteriori informazioni sulle impostazioni di rete, vedere DOCA0172•• *EcoStruxure Panel Server - Guida utente*, pagina 7).

In questo modo è possibile collegare Panel Server a:

- Dispositivi OT a valle tramite Modbus TCP su una porta Ethernet.
- PC IT a monte con SCADA e applicazioni software di messa in servizio sull'altra porta Ethernet.

HTTPS e Modbus sono disponibili su Wi-Fi e interfacce Ethernet Panel Server (ETH1, ETH2).

La tabella seguente presenta l'impostazione predefinita per ogni interfaccia:

Interfaccia		Modbus
Ethernet in topologia commutata		Attivato
Ethernet in topologia separata	Porta ETH1	Attivato
	Porta ETH2	Disattivato
Infrastruttura Wi-Fi		Disattivato
Punto di accesso Wi-Fi		Non disponibile

Si consiglia di disattivare il servizio Modbus sulle reti in cui non è utilizzato. Per ulteriori informazioni sull'attivazione del servizio, vedere DOCA0172•• *EcoStruxure Panel Server - Guida utente*, pagina 7.

Certificato server Web del prodotto

Per supportare le comunicazioni protette HTTP, EcoStruxure Panel Server è dotato di un certificato X.509v3 predefinito. Questo certificato garantisce l'integrità e la riservatezza per impostare la comunicazione HTTPS.

I browser Web riconoscono solo i certificati per i siti Web pubblici. Poiché Panel Server è installato in una rete LAN (Local Area Network), i browser Web non sono

in grado di distinguere un Panel Server da un altro. Perciò, quando ci si collega a Panel Server, viene visualizzato un messaggio di sicurezza sul browser Web.

Una connessione cablata diretta consente di proteggere il percorso di comunicazione con il Panel Server. Per ulteriori informazioni sul primo accesso alle pagine Web di EcoStruxure Panel Server tramite PC, vedere DOCA0172** *EcoStruxure Panel Server - Guida utente*, pagina 7.

Impronta della chiave del server SFTP

Se si pubblicano i dati su un server SFTP, assicurarsi che l'impronta della chiave, visualizzata durante la configurazione dell'indirizzo del server, corrisponda alla chiave SFTP del server.

Se si rinnova la chiave SFTP sul server, Panel Server non sarà più in grado di inviare i file, poiché la connessione non verrà autenticata. È necessario riconfigurare la pubblicazione per Panel Server registrare la nuova impronta della chiave SFTP.

Rete wireless

I protocolli radio sono vulnerabili alle violazioni di sicurezza fisica. Ad esempio, un attacco Denial of Service può bloccare il segnale radio con un potente emettitore radio situato nelle vicinanze.

Si consiglia pertanto di adattare la propria sicurezza fisica alla criticità delle informazioni che si basano sui protocolli radio. A questo scopo, le reti wireless (Wi-Fi e IEEE 802.15.4) possono essere disattivate in modo permanente in Panel Server. Se si è certi che non saranno mai necessarie le reti wireless (Wi-Fi e IEEE 802.15.4), e solo in questo caso, è possibile disattivarle definitivamente. Per ulteriori informazioni sulla disattivazione permanente e simultanea delle reti wireless, vedere DOCA0172** *EcoStruxure Panel Server - Guida utente*, pagina 7.

NOTA: I modelli Wired by Design (WD) di Panel Server consentono di rispettare i criteri wireless in quanto non contengono chipset wireless.

Si consiglia di eseguire la messa in servizio dei dispositivi wireless IEEE 802.15.4 in un luogo protetto da trasmettitori radio non autorizzati, ad esempio una sala di amministrazione.

Per la rete Wi-Fi, si consiglia di utilizzare WPA2 (Wi-Fi Protected Access versione 2).

NOTA: TKIP (Temporal Key Integrity Protocol) non supportato.

Accesso remoto (VPN)

Panel Server fornisce una funzione di accesso remoto che consente di collegare il Centro assistenza clienti (CCC) Schneider Electric alle pagine Web Panel Server.

Per impostazione predefinita, l'accesso non è attivato e richiede il firewall per attivare la connessione. Per ulteriori informazioni, vedere *Endpoint previsti*, pagina 17.

La funzione di accesso remoto si basa su una VPN di livello 3 che, per progettazione, non fornisce accesso alla rete, ma solo a Panel Server. Inoltre, solo HTTPS è autorizzato per il tunneling tramite questa VPN.

Dispositivi collegati

Si consiglia di controllare regolarmente l'elenco dei dispositivi collegati alla rete IEEE 802.15.4 del Panel Server. Nel caso di un dispositivo collegato sconosciuto, individuarlo e rimuoverlo. È inoltre possibile ricostruire la rete e riconnettere solo i dispositivi identificati.

Sicurezza delle applicazioni cloud

Sicurezza dei dati in movimento

Schneider Electric con applicazioni cloud EcoStruxure implementano le pratiche migliori come:

- Tutte le comunicazioni da e verso EcoStruxure Panel Server con sistemi interni Schneider Electric o sistemi esterni di terze parti sono crittografate con HTTPS (il livello minimo richiesto è TLS 1.2).
- Il certificato coinvolto in queste sessioni crittografate utilizza l'algoritmo hash sicuro SHA 256. Questo vale per le comunicazioni tra l'applicazione Panel Server e i server nelle piattaforme cloud di Microsoft Azure.

Sicurezza dei dati a riposo

Schneider Electric segue le pratiche migliori per creare soluzioni sicure e limitare il rischio di grave compromissione dei dati proteggendo al tempo stesso la privacy, il controllo e l'autonomia dei dati di ogni cliente indipendentemente dagli altri.

Tutte le credenziali e i token di sistema vengono archiviati e crittografati nelle piattaforme cloud di Microsoft Azure.

Endpoint previsti

Schneider Electric consiglia di consentire l'accesso solo ai domini richiesti in base alle proprie esigenze.

Nella tabella seguente sono elencati i nomi di dominio e i protocolli utilizzati quando Panel Server si connette al cloud.

Nome di dominio	Protocollo	Descrizione
cbBootStrap.gl.StruXureWareCloud.com	HTTPS (TCP porta 443)	Utilizzato alla prima connessione di Panel Server al cloud (o dopo un reset di fabbrica) per autenticare e registrare Panel Server.
etp.prod.StruXureWareCloud.com	HTTPS (TCP porta 443)	Utilizzato per scaricare l'aggiornamento del firmware.
cnm-ih-na.Azure-devices.net	HTTPS (TCP porta 443)	Utilizzato per la comunicazione di Panel Server con servizi cloud Schneider Electric come configurazione, dati o allarmi.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (TCP porta 443)	Consente al Centro assistenza clienti Schneider Electric di accedere da remoto alle pagine Web di Panel Server tramite VPN.
cnmdapiappstna.Blob.Core.Windows.net	HTTPS (TCP porta 443)	Consente a Panel Server di caricare i registri e i file di diagnostica su richiesta del Centro assistenza clienti Schneider Electric.
cnmiothubappstna.Blob.Core.Windows.net/file-upload	HTTPS (TCP porta 443)	Consente a Panel Server di caricare una topologia nei servizi cloud Schneider Electric.
time.gl.StruXureWareCloud.com	NTP (porta UDP) 123)	Il server NTP consente di mantenere la sincronizzazione dell'orologio di Panel Server.

NOTA: i nomi di dominio non fanno distinzione tra maiuscole e minuscole.

Sicurezza fisica del dispositivo

Etichetta con indicazione di manomissione

EcoStruxure Panel Server dispone di un'etichetta di indicazione di eventuali manomissioni che consente di proteggere la sicurezza fisica del dispositivo. Deve essere pulita e non deve presentare segni di manomissione (ad esempio strappi, lacerazioni o graffi). Schneider Electric consiglia di non utilizzare un dispositivo visibilmente alterato.

Installazione

Per proteggere la sicurezza fisica del dispositivo, si consiglia di effettuare le seguenti operazioni di installazione:

- Installare EcoStruxure Panel Server in un cabinet protetto in modo appropriato al livello di rischio dell'installazione (ad esempio, un cabinet con lucchetto o chiave).
- Se EcoStruxure Panel Server è montato in un quadro elettrico, installare il quadro in un ambiente protetto (ad esempio, con sportello bloccato o fotocamera).

NOTA: La protezione della sicurezza fisica del dispositivo include la protezione del codice QR. Il codice QR permette di accedere al codice dispositivo di Panel Server, che deve essere considerato come credenziale per il dispositivo. Si utilizza:

- Nella richiesta di sicurezza del dispositivo per le applicazioni cloud
- Come password per la connessione al punto di accesso Wi-Fi

Gestione password

Per proteggere il dispositivo da attacchi dannosi, modificare la password del punto di accesso Wi-Fi di Panel Server utilizzando le pagine Web di Panel Server.

La password deve rispettare le regole seguenti:

- Tra 8 e 32 caratteri
- Almeno un carattere maiuscolo
- Almeno un carattere minuscolo
- Non deve contenere caratteri speciali diversi da: ! " # \$ % & ' () * + - , . : ; / ~ < > = ? @ [] \ ^ _ ` { } |
- Il carattere spazio è consentito

Raccomandazioni sulla sicurezza per la manutenzione

Operazioni di manutenzione

Durante il ciclo di vita di EcoStruxure Panel Server, si raccomanda di eseguire regolarmente le operazioni seguenti:

- Controllare la sicurezza fisica di EcoStruxure Panel Server (vedere l'etichetta che indica eventuali manomissioni, pagina 18).
- Assicurarsi di disporre dell'aggiornamento firmware più recente. È necessario registrarsi per ricevere le notifiche di sicurezza, pagina 12.
- Controllare la presenza di dispositivi sconosciuti tra i dispositivi collegati, pagina 16.
- Controllare i registri di controllo, pagina 13 per individuare eventuali comportamenti imprevisti, ad esempio tentativi di accesso non validi o riavvio frequente.
- Controllare la data e l'ora, pagina 12 per evitare di spostarsi dalla data corrente.
- Verificare che tutti i servizi e le funzionalità non necessari sono disattivati, pagina 12.

Verifica della funzionalità di sicurezza

I test seguenti consentono di verificare il corretto funzionamento delle funzionalità di sicurezza tramite le pagine Web di EcoStruxure Panel Server.

Autenticazione Web

1. Provare ad accedere alle pagine Web di EcoStruxure Panel Server senza password o immettere una password errata.
Risultato: EcoStruxure Panel Server non fornisce l'accesso alle pagine Web.
2. Ripetere l'operazione altre 9 volte.
Risultato: EcoStruxure Panel Server si blocca per 10 minuti.
3. Riprovare 5 volte.
Risultato: EcoStruxure Panel Server si blocca per 60 minuti.

Autorizzazione Web

1. Accedere alle pagine Web di EcoStruxure Panel Server.
2. Contrassegnare una pagina Web (ad esempio, **Impostazioni**)
3. Aprire una finestra di navigazione privata nel browser e aprire la pagina Web contrassegnata in precedenza.
Risultato: non è possibile accedere alla pagina Web, tuttavia si viene reindirizzati alla pagina di accesso.

Verifica

1. Dopo alcuni o tutti i test precedenti, accedere alla pagina Web dei registri.

2. Scaricare i file di registro.
3. Verificare che nei registri siano presenti i tentativi falliti.

Aggiornamento del firmware

1. Accedere alla pagina Web **Aggiornamento firmware**.
2. Caricare un file casuale (ad esempio un'immagine o un documento di testo).
Risultato: EcoStruxure Panel Server segnala una firma errata.
3. Accedere ai registri di controllo.
4. Verificare che nei registri sia presente l'aggiornamento del firmware non riuscito.

Disabilitazione dei servizi

1. Per accedere al menu e disabilitare i servizi, selezionare **Impostazioni > Comunicazione di rete > DPWS**.
2. Collegare un PC con sistema operativo Windows alla stessa rete locale.
3. Fare clic su Rete da Esplora file.
Risultato: EcoStruxure Panel Server non viene rilevato, quindi, non viene visualizzato nell'elenco dei dispositivi nella rete.

Disabilitazione dei servizi wireless

Per accedere ai menu per disattivare temporaneamente i servizi wireless:

- Per la rete Wi-Fi, passare a **Impostazioni > Comunicazione di rete > Wi-Fi**, fare clic sul cursore **Attivazione Wi-Fi** e salvare le modifiche.
Risultato: nell'interfaccia di gestione del punto di accesso Wi-Fi, non è presente alcun EcoStruxure Panel Server connesso.
- Per IEEE 802.15.4, passare a **Impostazioni > Dispositivi wireless > Configurazione di rete**, fare clic sul cursore **Attivazione wireless** e salvare le modifiche.
Risultato: tutti i dispositivi wireless elencati in **Impostazioni > Dispositivi wireless > Dispositivi wireless** indicano uno stato **Non collegato** dopo un determinato periodo di tempo, in base al dispositivo wireless (per ulteriori informazioni, vedere la documentazione del dispositivo).

Glossario

D

DPWS - Profilo dispositivi per servizi Web:

Insieme minimo di vincoli di implementazione che consentono di attivare messaggistica, individuazione, descrizione ed eventi del servizio Web protetti sui dispositivi con risorse limitate.

H

HTTP - Hypertext Transfer Protocol:

Protocollo di rete che gestisce il recapito di file e dati sul World Wide Web.

HTTPS - Hypertext Transfer Protocol Secure:

Variante del protocollo HTTP (Web Transfer Protocol) standard che aggiunge un livello di protezione ai dati in transito attraverso una connessione al protocollo SSL (Secure Socket Layer) o TLS (Transport Layer Security).

I

IP - Internet protocol, Protocollo Internet:

Gli indirizzi IP vengono utilizzati per identificare i dispositivi collegati all'intranet aziendale o a Internet.

IT - Information technology, tecnologia dell'informazione:

Si riferisce ai sistemi informatici e alla rete informatica dell'azienda, rispetto alla rete OT (tecnologia operativa).

L

LAN - Local area network, rete area locale:

Si riferisce all'intranet aziendale o alla rete IT.

M

Modbus TCP/IP:

Un protocollo che fornisce la comunicazione client/server tra dispositivi e TCP/IP che fornisce le comunicazioni su una connessione Ethernet.

O

OT - Operational technology, tecnologia operativa:

Si riferisce ai sistemi hardware e software utilizzati dall'azienda per monitorare e controllare direttamente i processi e le apparecchiature di produzione, denominata anche rete di controllo industriale (IC). OT viene spesso utilizzato per fare riferimento alla rete operativa aziendale anziché alla rete IT.

P

PKI - Public key infrastructure, Infrastruttura a chiave pubblica:

Definisce un insieme di servizi utilizzati per generare e autenticare le firme digitali. Un'infrastruttura a chiave pubblica è progettata per garantire la riservatezza, l'integrità e l'autenticità delle informazioni.

Policy di sicurezza:

Una policy di sicurezza del sistema è rappresentata dalle impostazioni di protezione applicate all'intero sistema protetto. Una policy di sicurezza generalmente si riferisce all'uso di norme. Permette di definire qualsiasi configurazione di sicurezza condivisa tra tutti i dispositivi.

S**SCADA - Supervisory control and data acquisition:**

Si riferisce a sistemi progettati per ottenere dati in tempo reale su processi di produzione e apparecchiature per il monitoraggio e il controllo remoto.

SFTP - Secure File Transfer Protocol:

Versione sicura del protocollo di trasferimento file (FTP) che facilita l'accesso ai dati e il trasferimento dei dati su un flusso di dati SSH (Secure Shell).

T**TCP/IP - Transmission control protocol/Internet protocol:**

Si riferisce alla suite di protocolli utilizzati per le comunicazioni via Internet.

V**VPN - Virtual private network, rete privata virtuale:**

La VPN viene utilizzata per stabilire un "tunnel" protetto/privato tra un punto di accesso esterno autenticato e la rete aziendale attendibile.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
Francia

+ 33 (0) 1 41 29 70 00

www.se.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

© 2025 Schneider Electric. Tutti i diritti sono riservati.

DOCA0211IT-11