

EcoStruxure Automation Device Maintenance

Tool di aggiornamento firmware

Guida in linea

EIO0000004049.04
11/2022

Informazioni di carattere legale

Il marchio Schneider Electric e qualsiasi altro marchio registrato di Schneider Electric SE e delle sue consociate citati nella presente guida sono di proprietà di Schneider Electric SE o delle sue consociate. Tutti gli altri marchi possono essere marchi registrati dei rispettivi proprietari. La presente guida 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 la presente guida o parte di essa, in qualsiasi formato e con qualsiasi metodo (elettronico, meccanico, fotocopia, registrazione, o in altro modo), per qualsiasi scopo, senza previa autorizzazione scritta di Schneider Electric.

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

I prodotti e le apparecchiature di Schneider Electric devono essere installati, utilizzati, posti in assistenza e in manutenzione esclusivamente da personale qualificato.

Considerato che le normative, le specifiche e i progetti possono variare di volta in volta, le informazioni contenute nella presente guida possono essere soggette a modifica senza alcun 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 le conseguenze risultanti dall'uso delle informazioni ivi contenute.

Facendo parte di un gruppo di aziende responsabili e inclusive, stiamo aggiornando i contenuti della nostra comunicazione che potrebbero contenere una terminologia non inclusiva. Tuttavia, fino a quando il processo non sarà completato, potrebbero ancora essere presenti termini standard di business che alcuni dei nostri clienti potrebbero ritenere inappropriati.

© 2022 – Schneider Electric. Tutti i diritti riservati.

Sommario

Informazioni di sicurezza	5
Qualifica del personale.....	5
Uso adeguato.....	6
Prima di iniziare.....	6
Avviamento e verifica.....	7
Funzionamento e regolazioni.....	8
Precauzioni di sicurezza.....	8
Informazioni sul manuale.....	10
Introduzione	15
Panoramica	15
Requisiti di sistema.....	16
Installazione.....	17
Guida introduttiva.....	18
Schermata di benvenuto	18
Interfaccia utente di EcoStruxure Automation Device	
Maintenance	20
Pacchetto dati	20
Dispositivo/Caricamento	21
Aggiungi dispositivo.....	23
Configurazione delle impostazioni.....	25
Finestra degli errori e degli avvisi	26
Creazione di un nuovo progetto EcoStruxure Automation Device	
Maintenance	27
Salvataggio del progetto.....	28
Apertura del progetto	29
Configurazione del tool EcoStruxure Automation Device	
Maintenance	32
Configurazione della modalità di rilevamento del dispositivo	32
Configurazione dello scanner Modbus TCP	34
Configurazione dello scanner DPWS	36
Configurazione delle impostazioni di comunicazione	37
Configurazione delle ubicazioni dei pacchetti.....	37
Visualizzazione dei file di registro.....	38
Configurazione della lingua	40
Ripristino delle impostazioni dell'applicazione	40
Configurazione delle funzionalità di sicurezza	41
Funzionalità di sicurezza	41
Gestione dei certificati.....	43
Gestione dell'infrastruttura a chiave pubblica (PKI).....	48
Attivazione della registrazione dei messaggi Syslog	49
Pacchetto dati.....	51
Scheda Pacchetto dati	51
Dispositivo/Caricamento	55
Scheda Dispositivo/Caricamento	55
Raggruppamento di dispositivi nell'ELENCO DISPOSITIVI	56
Rimozione di un dispositivo	57

Gestione delle credenziali utente	61
Accesso alle estensioni.....	64
Monitoraggio dello stato di rilevamento del dispositivo	66
Visualizzazione/Conferma messaggi.....	67
Visualizzazione dei registri	68
Centro aggiornamenti	68
Aggiornamento del firmware	69
Aggiornamento del file di configurazione sicurezza	71
Sicurezza informatica	74
Definizione della sicurezza informatica	74
Linee guida Schneider Electric.....	76
Verifica della firma digitale	78
File che richiedono la disinstallazione manuale	79
Componenti utilizzati da EcoStruxure Automation Device	
Maintenance	80
Glossario	83
Indice	86

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.

Qualifica del personale

Una persona qualificata è una persona che ha le seguenti caratteristiche:

- Capacità e conoscenze relative alla costruzione e al funzionamento di apparecchiature elettriche e alla loro installazione.
- Conoscenze ed esperienza nella programmazione del controllo industriale.

- Ha ricevuto formazione relativa alla sicurezza, per riconoscere ed evitare i rischi correlati.

L'addetto qualificato deve essere in grado di individuare eventuali pericoli che possono derivare dalla parametrizzazione, dalla modifica dei valori dei parametri e in generale dall'impiego di apparecchiature meccaniche, elettriche ed elettroniche. Inoltre, deve avere familiarità con le normative, le disposizioni e i regolamenti antinfortunistici, che deve rispettare mentre progetta e implementa il sistema.

Uso adeguato

Questo prodotto è una libreria da utilizzare insieme con i sistemi di controllo e i segmenti del motore a statore lungo destinati esclusivamente agli scopi descritti nella presente documentazione e applicati nel settore industriale.

Attenersi sempre alle istruzioni di sicurezza applicabili, alle condizioni specificate e ai dati tecnici.

Effettuare una valutazione dei rischi rispetto all'uso specifico prima di utilizzare il prodotto. Adottare misure protettive in base al risultato.

Dato che il prodotto viene impiegato nell'ambito di un sistema globale, è necessario garantire la sicurezza del personale nella progettazione del sistema globale (ad esempio, la progettazione della macchina).

Ogni altro uso non è previsto e può essere pericoloso.

Prima di iniziare

Non utilizzare questo prodotto su macchinari privi di sorveglianza attiva del punto di funzionamento. La mancanza di un sistema di sorveglianza attivo sul punto di funzionamento può presentare gravi rischi per l'incolumità dell'operatore macchina.

⚠ AVVERTIMENTO

APPARECCHIATURA NON PROTETTA

- Non utilizzare questo software e la relativa apparecchiatura di automazione su macchinari privi di protezione per le zone pericolose.
- Non avvicinarsi ai macchinari durante il funzionamento.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Questa apparecchiatura di automazione con il relativo software permette di controllare processi industriali di vario tipo. Il tipo o il modello di apparecchiatura di automazione adatto per ogni applicazione varia in funzione di una serie di fattori, quali la funzione di controllo richiesta, il grado di protezione necessario, i metodi di produzione, eventuali condizioni particolari, la regolamentazione in vigore, ecc. Per alcune applicazioni può essere necessario utilizzare più di un processore, ad esempio nel caso in cui occorra garantire la ridondanza dell'esecuzione del programma.

Solo l'utente, il costruttore della macchina o l'integratore del sistema sono a conoscenza delle condizioni e dei fattori che entrano in gioco durante l'installazione, la configurazione, il funzionamento e la manutenzione della macchina e possono quindi determinare l'apparecchiatura di automazione e i relativi interblocchi e sistemi di sicurezza appropriati. La scelta dell'apparecchiatura di controllo e di automazione e del relativo software per un'applicazione particolare deve essere effettuata dall'utente nel rispetto degli standard locali e nazionali e della regolamentazione vigente. Per informazioni in merito, vedere anche la guida National Safety Council's Accident Prevention Manual (che indica gli standard di riferimento per gli Stati Uniti d'America).

Per alcune applicazioni, ad esempio per le macchine confezionatrici, è necessario prevedere misure di protezione aggiuntive, come un sistema di sorveglianza attivo sul punto di funzionamento. Questa precauzione è necessaria quando le mani e altre parti del corpo dell'operatore possono raggiungere aree con ingranaggi in movimento o altre zone pericolose, con conseguente pericolo di infortuni gravi. I prodotti software da soli non possono proteggere l'operatore dagli infortuni. Per questo motivo, il software non può in alcun modo costituire un'alternativa al sistema di sorveglianza sul punto di funzionamento.

Accertarsi che siano stati installati i sistemi di sicurezza e gli asservimenti elettrici/meccanici opportuni per la protezione delle zone pericolose e verificare il loro corretto funzionamento prima di mettere in funzione l'apparecchiatura. Tutti i dispositivi di blocco e di sicurezza relativi alla sorveglianza del punto di funzionamento devono essere coordinati con l'apparecchiatura di automazione e la programmazione software.

NOTA: Il coordinamento dei dispositivi di sicurezza e degli asservimenti meccanici/elettrici per la protezione delle zone pericolose non rientra nelle funzioni della libreria dei blocchi funzione, del manuale utente o di altre implementazioni indicate in questa documentazione.

Avviamento e verifica

Prima di utilizzare regolarmente l'apparecchiatura elettrica di controllo e automazione dopo l'installazione, l'impianto deve essere sottoposto ad un test di avviamento da parte di personale qualificato per verificare il corretto funzionamento dell'apparecchiatura. È importante programmare e organizzare questo tipo di controllo, dedicando ad esso il tempo necessario per eseguire un test completo e soddisfacente.

AVVERTIMENTO

RISCHI RELATIVI AL FUNZIONAMENTO DELL'APPARECCHIATURA

- Verificare che tutte le procedure di installazione e di configurazione siano state completate.
- Prima di effettuare test sul funzionamento, rimuovere tutti i blocchi o altri mezzi di fissaggio dei dispositivi utilizzati per il trasporto.
- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Eseguire tutti i test di avviamento raccomandati sulla documentazione dell'apparecchiatura. Conservare con cura la documentazione dell'apparecchiatura per riferimenti futuri.

Il software deve essere testato sia in ambiente simulato che in ambiente di funzionamento reale..

Verificare che il sistema completamente montato e configurato sia esente da cortocircuiti e punti a massa, ad eccezione dei punti di messa a terra previsti dalle normative locali (ad esempio, in conformità al National Electrical Code per gli USA). Nel caso in cui sia necessario effettuare un test sull'alta tensione, seguire le raccomandazioni contenute nella documentazione dell'apparecchiatura al fine di evitare danni accidentali all'apparecchiatura stessa.

Prima di mettere sotto tensione l'apparecchiatura:

- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.
- Chiudere lo sportello del cabinet dell'apparecchiatura.
- Rimuovere tutte le messa a terra temporanee dalle linee di alimentazione in arrivo.
- Eseguire tutti i test di avviamento raccomandati dal costruttore.

Funzionamento e regolazioni

Le seguenti note relative alle precauzioni da adottare fanno riferimento alle norme NEMA Standards Publication ICS 7.1-1995 (fa testo la versione inglese):

- Indipendentemente dalla qualità e della precisione del progetto nonché della costruzione dell'apparecchiatura o del tipo e della qualità dei componenti scelti, possono sussistere dei rischi se l'apparecchiatura non viene utilizzata correttamente.
- Eventuali regolazioni involontarie possono provocare il funzionamento non soddisfacente o non sicuro dell'apparecchiatura. Per effettuare le regolazioni funzionali, attenersi sempre alle istruzioni contenute nel manuale fornito dal costruttore. Il personale incaricato di queste regolazioni deve avere esperienza con le istruzioni fornite dal costruttore delle apparecchiature e con i macchinari utilizzati con l'apparecchiatura elettrica.
- L'operatore deve avere accesso solo alle regolazioni relative al funzionamento delle apparecchiature. L'accesso agli altri organi di controllo deve essere riservato, al fine di impedire modifiche non autorizzate ai valori che definiscono le caratteristiche di funzionamento delle apparecchiature.

Precauzioni di sicurezza

Durante l'installazione o l'uso di questo software, prestare attenzione ai messaggi di sicurezza emessi nel software e inclusi nella documentazione. I seguenti messaggi di sicurezza valgono per questo software nella sua interezza.

⚠ AVVERTIMENTO

RISCHIO DI FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Non utilizzare il software per applicazioni di controllo o protezione critiche, nelle quali la sicurezza delle persone o delle apparecchiature dipende dal funzionamento dell'azione di controllo.
- Non utilizzare il software per il controllo di funzioni a criticità temporale. Tra l'istante in cui viene impartito un comando e l'istante in cui l'azione ha effetto possono verificarsi ritardi di comunicazione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

RISCHIO DI IMPRECISIONE DEI DATI

- Configurare il software correttamente in modo da ottenere report e/o dati corretti.
- Non basare le azioni di manutenzione o servizio soltanto sui messaggi e sulle informazioni visualizzate dal software.
- Non basarsi soltanto sui messaggi software e sui report per determinare se il sistema funziona correttamente o se soddisfa gli standard e i requisiti applicabili.
- Tenere conto delle ripercussioni dei ritardi di trasmissione involontari o degli errori dei link di comunicazione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

AVVERTIMENTO

POSSIBILE COMPROMISSIONE DELLA DISPONIBILITÀ, DELL'INTEGRITÀ E DELLA CONFIDENZIALITÀ DEL SISTEMA

Utilizzare le migliori prassi per la sicurezza informatica.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

NOTA: Per informazioni dettagliate sulla sicurezza informatica, vedere il capitolo *Sicurezza informatica*, pagina 74.

Informazioni sul manuale

Ambito del documento

Questo documento descrive il tool EcoStruxure Automation Device Maintenance. EcoStruxure Automation Device Maintenance permette di trasferire il firmware da un PC ai dispositivi Schneider Electric supportati. Il tool supporta il rilevamento dei dispositivi presenti in rete e consente anche di identificarli manualmente qualora il rilevamento non fosse possibile.

Nota di validità

Il presente documento è stato aggiornato per EcoStruxure Automation Device Maintenance versione 3.1.

Le caratteristiche descritte nel presente documento, nonché quelle descritte nei documenti inclusi nella sezione Documenti correlati seguente, sono disponibili online. Per accedere alle informazioni online, andare alla home page di Schneider Electric www.se.com/ww/en/download/. Per la documentazione di EcoStruxure Automation Device Maintenance, digitare *EcoStruxure Automation Device Maintenance* nella casella di testo di ricerca e premere il tasto **Invio**.

Le caratteristiche descritte nel presente documento dovrebbero essere uguali a quelle che appaiono online. In base alla nostra politica di continuo miglioramento, è possibile che il contenuto della documentazione sia revisionato nel tempo per migliorare la chiarezza e la precisione. Nell'eventualità in cui si noti una differenza tra il documento e le informazioni online, utilizzare come riferimento le informazioni online.

Documenti correlati

Titolo della documentazione	Codice di riferimento
Firmware Compatibility Rules, Modicon M580, Modicon Momentum, and Modicon X80 I/O Modules	EIO0000002634 (English)
Piattaforma controller Modicon - Sicurezza informatica, Manuale di riferimento	EIO0000001999 (English) EIO0000002001 (French) EIO0000002000 (German) EIO0000002003 (Spanish) EIO0000002002 (Italian) EIO0000002004 (Chinese)
Specifiche Modbus e istruzioni di implementazione, Manuale di riferimento	Modbus Application Protocol Specification
Profilo dei dispositivi per i servizi Web, Manuale di riferimento	WSDD-DPWS

Titolo della documentazione	Codice di riferimento
EcoStruxure™ Control Expert, Modalità di funzionamento	33003101 (English)
	33003102 (French)
	33003103 (German)
	33003104 (Spanish)
	33003696 (Italian)
	33003697 (Chinese)
EcoStruxure Automation Device Maintenance Altivar, Manuale dell'utente	JYT50472 (English)
	JYT50474 (French)
	JYT50482 (German)
	JYT50476 (Spanish)
	JYT50478 (Italian)
	JYT50483 (Chinese)
	JYT50484 (Turkish)
	JYT50485 (Portuguese)

Informazioni relative al prodotto

AVVERTIMENTO

PERDITA DI CONTROLLO

- Il progettista degli schemi di controllo deve prendere in considerazione le potenziali modalità di errore dei vari percorsi di controllo e, per alcune funzioni di controllo particolarmente critiche, deve fornire i mezzi per raggiungere uno stato di sicurezza durante e dopo un errore di percorso. Esempi di funzioni di controllo critiche sono ad esempio l'arresto di emergenza e l'arresto di finecorsa, l'interruzione dell'alimentazione e il riavvio.
- Per le funzioni di controllo critiche occorre prevedere sequenze di controllo separate o ridondanti.
- Le sequenze di controllo del sistema possono includere link di comunicazione. È necessario fare alcune considerazioni sulle implicazioni di ritardi improvvisi nelle comunicazioni del collegamento.
- Osservare tutte le norme per la prevenzione degli incidenti e le normative di sicurezza locali.¹
- Prima della messa in servizio dell'apparecchiatura, controllare singolarmente e integralmente il funzionamento di ciascun controller.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

¹ Per ulteriori informazioni, fare riferimento a NEMA ICS 1.1 (ultima edizione), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" e a NEMA ICS 7.1 (ultima edizione), "Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems" o alla pubblicazione equivalente valida nel proprio paese.

Prima di tentare di fornire una soluzione (macchina o processo) per un'applicazione specifica utilizzando i POU presenti nella libreria, è opportuno considerare l'utilizzo di procedure ottimali che comprendono, tra le altre cose, analisi dei rischi, sicurezza funzionale, compatibilità dei componenti, test e convalida del sistema in relazione a questa libreria.

⚠ AVVERTIMENTO

UTILIZZO INAPPROPRIATO DELLE UNITÀ DI ORGANIZZAZIONE DEI PROGRAMMI

- Eseguire un'analisi in tema di sicurezza per l'applicazione e i dispositivi installati.
- Verificare che le unità di organizzazione dei programmi (POU) siano compatibili con i dispositivi nel sistema e non abbiano effetti indesiderati sul funzionamento del sistema.
- Utilizzare parametri appropriati, in particolare valori limite, e osservare l'usura della macchina e il comportamento di arresto.
- Verificare che tutti i sensori e gli attuatori siano compatibili con i POU selezionati.
- Testare in modo approfondito tutte le funzioni durante la verifica e la messa in servizio in tutte le modalità di funzionamento.
- Fornire metodi indipendenti per le funzioni di controllo critiche (arresto di emergenza, condizioni per superamento dei valori limite, ecc.) in base a un'analisi di sicurezza, regole rispettive e normative.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠ AVVERTIMENTO

FUNZIONAMENTO ANOMALO DELL'APPARECCHIATURA

- Con questa apparecchiatura utilizzare esclusivamente il software approvato da Schneider Electric.
- Aggiornare il programma applicativo per ogni modifica della configurazione fisica dell'hardware.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

I trasferimenti incompleti dei file, ad esempio file di dati, file dell'applicazione e/o file del firmware, possono avere gravi conseguenze per la macchina o il controller. Se si disattiva l'alimentazione, o in caso di assenza di alimentazione o di interruzione della comunicazione durante un trasferimento di file, la macchina può diventare non operativa, oppure l'applicazione potrebbe tentare di operare su un file dati danneggiato. Se si verifica un'interruzione, riprovare il trasferimento. Verificare di includere nell'analisi del rischio l'impatto dei file di dati danneggiati.

⚠ AVVERTIMENTO

FUNZIONAMENTO ANOMALO DELL'APPARECCHIATURA, PERDITA DI DATI O DANNEGGIAMENTO DEI FILE

- Non interrompere un trasferimento in corso.
- Se si interrompe il trasferimento per qualsiasi motivo, riavviare il trasferimento.
- Non mettere la macchina in servizio fino al completamento del trasferimento del file, a meno che nell'analisi del rischio non siano stati presi in considerazione i file danneggiati e si siano prese precauzioni adeguate per impedire conseguenze potenzialmente pericolose dovute a trasferimenti di file non riusciti.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Adottare le misure adeguate per l'utilizzo di questa libreria per il controllo della macchina al fine di evitare conseguenze indesiderate del funzionamento della macchina controllata, cambiamenti di stato o alterazione della memoria dati o degli elementi di funzionamento della macchina.

⚠ AVVERTIMENTO

FUNZIONAMENTO ANOMALO DELL'APPARECCHIATURA

- Collocare i dispositivi operatore del sistema di controllo accanto alla macchina o in una posizione dalla quale si abbia una visuale completa sulla macchina.
- Proteggere i comandi operatore contro l'accesso non autorizzato.
- Se il controllo in remoto è un aspetto necessario del progetto applicazione, accertarsi che nella località remota sia presente un osservatore competente e qualificato.
- Configurare e installare l'ingresso Run/Stop, se presente, oppure, altri mezzi esterni nell'applicazione, in modo che il controllo locale su avvio e arresto del dispositivo possa essere mantenuto indipendentemente dai comandi remoti inviati.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Terminologia derivata dagli standard

I termini tecnici, la terminologia, i simboli e le descrizioni corrispondenti in questo manuale o che compaiono nei o sui prodotti stessi, derivano in genere dai termini o dalle definizioni degli standard internazionali.

Nell'ambito dei sistemi di sicurezza funzionale, degli azionamenti e dell'automazione generale, questi includono anche espressioni come *sicurezza*, *funzione di sicurezza*, *stato sicuro*, *anomalia*, *reset anomalie*, *malfunzionamento*, *guasto*, *errore*, *messaggio di errore*, *pericoloso*, ecc.

Tra gli altri, questi standard includono:

Standard	Descrizione
IEC 61131-2:2007	Controller programmabili, parte 2: Requisiti e test delle apparecchiature.
ISO 13849-1:2015	Sicurezza del macchinario – Parti dei sistemi di comando legate alla sicurezza Principi generali per la progettazione.
EN 61496-1:2013	Sicurezza del macchinario – Apparecchiature elettrosensibili di protezione Parte 1: Requisiti generali e test
ISO 12100:2010	Sicurezza dei macchinari - Principi generali di progettazione - Valutazione e riduzione dei rischi
EN 60204-1:2006	Sicurezza dei macchinari - Apparecchiature elettriche dei macchinari - Parte 1: Requisiti generali
ISO 14119:2013	Sicurezza dei macchinari - Dispositivi di interblocco associati alle protezioni - Principi di progettazione e selezione
ISO 13850:2015	Sicurezza dei macchinari - Arresto di emergenza - Principi di progettazione
IEC 62061:2015	Sicurezza dei macchinari - Sicurezza funzionale dei sistemi di controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza
IEC 61508-1:2010	Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili di sicurezza – Requisiti generali
IEC 61508-2:2010	Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza – Requisiti per sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza.
IEC 61508-3:2010	Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili di sicurezza: Requisiti software
IEC 61784-3:2016	Reti di comunicazione industriale - Profili - Parte 3: bus di campo di sicurezza funzionale - Regole generali e definizioni del profilo.
2006/42/EC	Direttiva macchine
2014/30/EU	Direttiva compatibilità elettromagnetica
2014/35/EU	Direttiva bassa tensione

I termini utilizzati nel presente documento possono inoltre essere utilizzati indirettamente, in quanto provenienti da altri standard, quali:

Standard	Descrizione
Serie IEC 60034	Macchine elettriche rotative
Serie IEC 61800	Sistemi di azionamento ad alimentazione elettrica e velocità regolabile
Serie IEC 61158	Comunicazioni dati digitali per misure e controlli – Bus di campo per l'uso con i sistemi di controllo industriali

Infine, l'espressione *area di funzionamento* può essere utilizzata nel contesto di specifiche condizioni di pericolo e in questo caso ha lo stesso significato dei termini *area pericolosa* o *zona di pericolo* espressi nella *Direttiva macchine (2006/42/EC)* e *ISO 12100:2010*.

NOTA: Gli standard indicati in precedenza possono o meno applicarsi ai prodotti specifici citati nella presente documentazione. Per ulteriori informazioni relative ai singoli standard applicabili ai prodotti qui descritti, vedere le tabelle delle caratteristiche per tali codici di prodotti.

Introduzione

Panoramica

Introduzione

EcoStruxure Automation Device Maintenance consente di aggiornare simultaneamente i pacchetti del firmware su più dispositivi. I dispositivi possono essere rilevati automaticamente o essere aggiunti manualmente qualora il rilevamento automatico non fosse supportato o fosse disattivato sul dispositivo.

I metodi supportati per rilevare i dispositivi sono:

- Modbus codice funzione 43 (Read Device Identification)
- DPWS (Device Profile for Web Services)

Funzionalità

EcoStruxure Automation Device Maintenance supporta le seguenti funzionalità:

- Rilevamento automatico dei dispositivi
- Identificazione manuale dei dispositivi
- Funzionalità di sicurezza
- Aggiornamento simultaneo del firmware su più dispositivi
- Gestione indirizzo IP

Dispositivi Schneider Electric supportati

Dispositivi Modicon:

- Modicon M340
- Modicon M580
- Modicon Momentum
- Moduli di I/O Modicon X80

Dispositivi Altivar:

- Famiglie di prodotti Altivar
 - Azionamenti Altivar Process ATV6••
 - Azionamenti Altivar Process ATV9••
 - Azionamenti Altivar Machine ATV340
- Moduli opzionali Altivar:
 - VW3A3720 Ethernet
 - VW3A3721 MultiDrive-Link
 - VW3A3530D ATV dPAC
- Soft starter Altivar:
 - Soft starter Altivar ATS480

Requisiti di sistema

Requisiti hardware

Componente	Requisito minimo
CPU	Intel® Core i3 o versione successiva supportato
RAM	Minimo 4 GB, consigliati 8 GB o più
Spazio libero su disco rigido	500 MB di spazio disponibile sul disco rigido

Requisiti software

- Microsoft Windows® 10 Professional 32 bit/64 bit o versioni successive
- Microsoft Windows Server 2016 standard 64 bit
- Microsoft Windows Server 2019 standard 64 bit

Protocolli di comunicazione

Il tool supporta i seguenti protocolli:

- FTP
- HTTP / HTTPS
- Modbus SL
- Modbus TCP
- OPC UA
- TCP
- UDP
- USB

Risoluzione dello schermo

Per visualizzare il software con la migliore risoluzione dello schermo, usare la risoluzione 1920 x 1080 pixel. È richiesta almeno una risoluzione dello schermo di 1280 x 1024 pixel.

Sicurezza informatica

Il software utilizza le seguenti porte:

- DPWS (tramite la porta 3702)
- FTP (tramite le porte 20, 21)
- HTTP (su porta 80) / HTTPS (su porte 443 e 8080)
- Modbus (su porta 502)
- OPC UA (tramite la porta 4840)

AVVERTIMENTO

POSSIBILE COMPROMISSIONE DELLA DISPONIBILITÀ, DELL'INTEGRITÀ E DELLA CONFIDENZIALITÀ DEL SISTEMA

Utilizzare le migliori prassi per la sicurezza informatica.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

NOTA: Per informazioni dettagliate sulla sicurezza informatica, vedere il capitolo *Sicurezza informatica*, pagina 74.

Installazione

Procedura

Per installare il software si possono scaricare i file di installazione dal sito Web Schneider Electric.

NOTA: Prima di fare doppio clic sul file AutomationDeviceMaintenance.exe, verificare l'integrità del file come descritto nel capitolo *Verifica della firma digitale*, pagina 78.

NOTA: Occorrono i diritti di amministratore per installare il software.

Procedere come segue per installare il software:

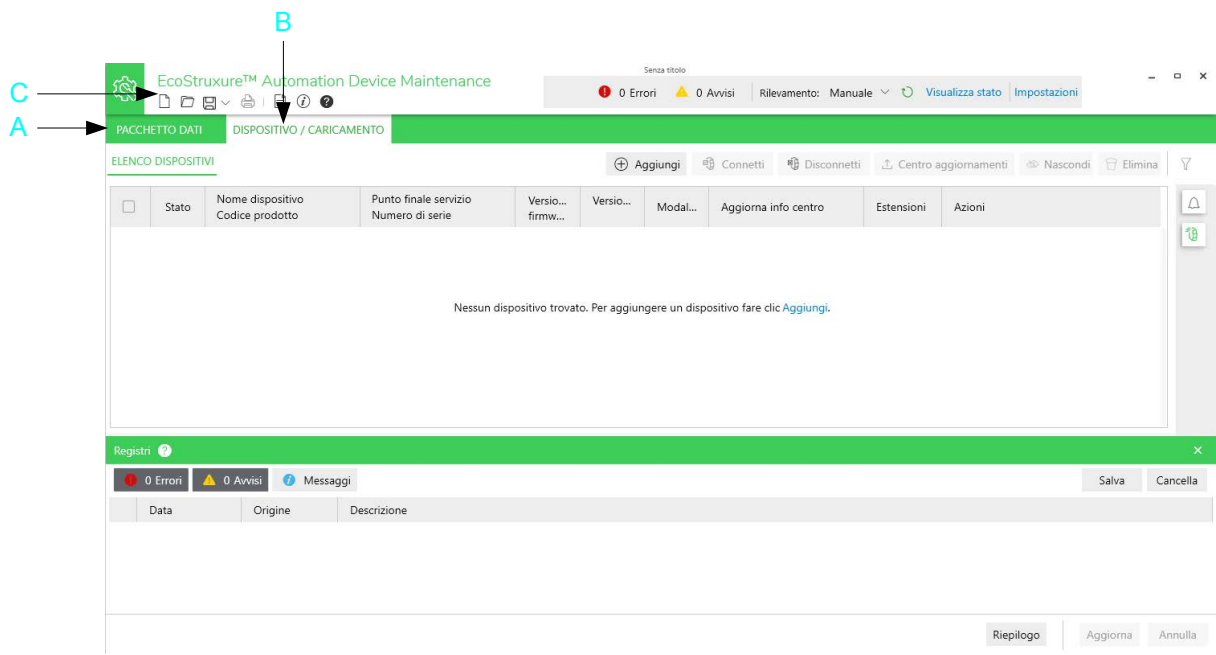
Passo	Azione
1	Utilizzare Esplora risorse di Windows per individuare il percorso dei file di installazione dopo averli scaricati.
2	Fare doppio clic sul file di configurazione EcoStruxure Automation Device Maintenance. Viene visualizzata l'installazione guidata InstallShield Wizard .
3	Seguire le istruzioni della procedura guidata InstallShield Wizard per completare l'installazione.

Guida introduttiva

Schermata di benvenuto

Panoramica











Dopo l'avvio iniziale, EcoStruxure Automation Device Maintenance visualizza la seguente schermata per aggiornare i pacchetti firmware su più dispositivi. Quando si chiude il tool, viene salvato lo stato presente dell'interfaccia utente. EcoStruxure Automation Device Maintenance visualizza quindi la vista presente al momento della chiusura del tool quando viene riavviato.



Legenda	Nome	Funzione
A	Pacchetto dati	Visualizza il contenuto del repository dei pacchetti dati.
B	Dispositivo/Caricamento	Visualizza i dettagli dei dispositivi rilevati o identificati manualmente.
C	Barra degli strumenti	Visualizza l'insieme delle icone per l'esecuzione delle varie funzioni.

Barra degli strumenti

La barra degli strumenti consente di accedere alle funzioni generiche di EcoStruxure Automation Device Maintenance.

Elemento	Nome	Descrizione
	Nuovo progetto	Consente di creare un nuovo progetto EcoStruxure Automation Device Maintenance, pagina 27.
	Apri	Consente di aprire un existing project, pagina 29.
	Salva	Consente di salvare le project settings, pagina 28.
	Stampa	Funzione non disponibile in questa versione.
	Registri	Consente di visualizzare le informazioni di registro.
	Informazioni	Consente di accedere a: <ul style="list-style-type: none"> • Informazioni su EcoStruxure Automation Device Maintenance • Copia dettagli • Accordo di licenza • Informazioni sui componenti • Informazioni di sistema
	Guida	Consente di accedere alla guida in linea.
	Errore	Consente di visualizzare gli errori rilevati , pagina 26.
	Avvertenza	Consente di visualizzare gli allarmi rilevati , pagina 26.
	Rilevamento	Consente di attivare il rilevamento dispositivi quando la modalità di rilevamento dispositivi è impostata su Manuale .
–	Manuale / Automatico	Selezionare la modalità di rilevamento dispositivi Manuale o Automatico dall'elenco. Per ulteriori informazioni, consultare il capitolo <i>Configurazione della modalità di rilevamento dispositivi</i> , pagina 32.
–	Impostazioni	Permette di configurare le impostazioni .

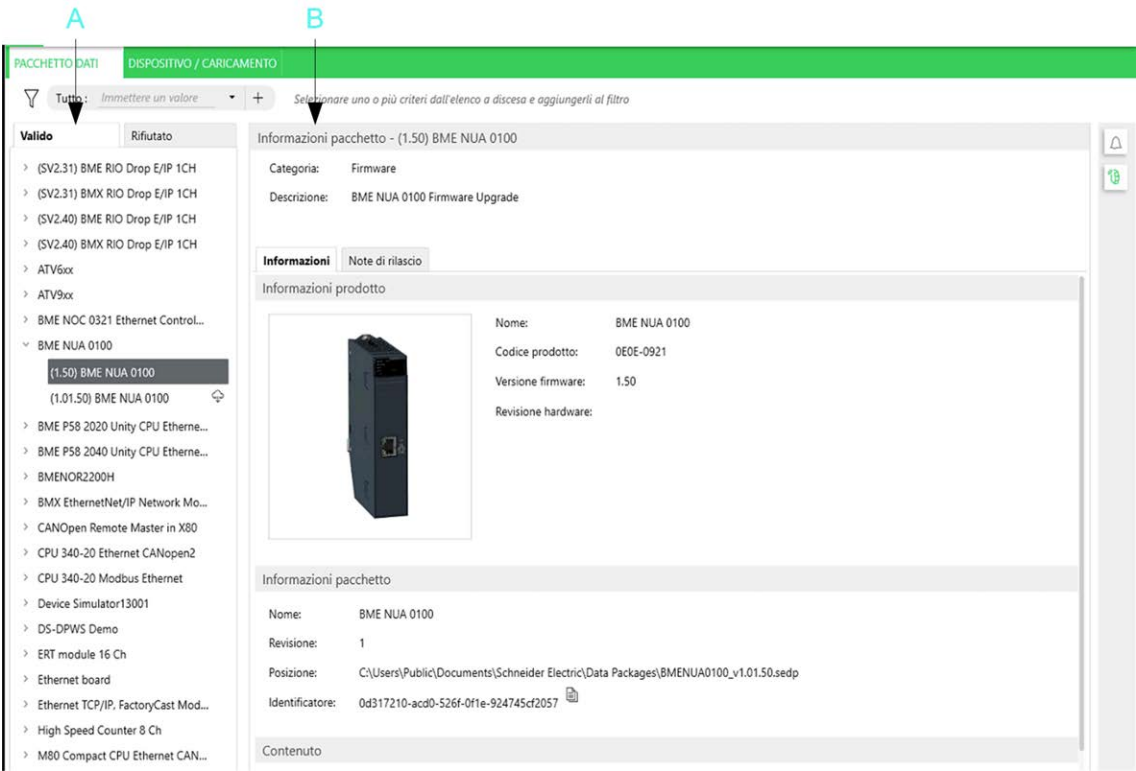
Pulsanti

Pulsante	Descrizione
Riepilogo	Dopo aver eseguito un aggiornamento, fare clic sul pulsante Riepilogo per recuperare le informazioni sui dispositivi aggiornati.
Aggiornamento	Dopo aver configurato le impostazioni per l'aggiornamento del firmware, pagina 69 o l'aggiornamento del file di configurazione sicurezza, pagina 71, fare clic sul pulsante Aggiorna per avviare il processo di aggiornamento come configurato.
Annulla	Il pulsante Annulla consente di annullare un'operazione di aggiornamento.

Interfaccia utente di EcoStruxure Automation Device Maintenance

Pacchetto dati

La funzione **Pacchetto dati** contiene il repository pacchetti e visualizza i pacchetti firmware disponibili nel tool.



Legenda	Nome	Descrizione
A	Elenco PACCHETTO DATI con le schede Valido e Rifiutato	Visualizza l'elenco dei pacchetti firmware disponibili localmente. I pacchetti disponibili nella rete sono visualizzati se è installato l'Add-On richiesto. Per ulteriori informazioni, consultare il capitolo <i>Scheda Pacchetti dati</i> , pagina 51.
B	Informazioni pacchetto	Visualizza descrizione e contenuto del pacchetto dati selezionato con informazioni statiche nella parte superiore con l'indicazione di Categoria e Descrizione e con due schede Informazioni e Note di rilascio nella parte inferiore. Per ulteriori informazioni, consultare il capitolo <i>Scheda Pacchetti dati</i> , pagina 51.

Dispositivo/Caricamento

Panoramica

La scheda **Dispositivo/Caricamento** visualizza i dettagli dei dispositivi noti allo strumento .

NOTA: Le informazioni visualizzate in questa scheda vengono aggiornate automaticamente solo se la modalità di rilevamento è impostata su

Automatica. Fare clic sull'icona  della barra degli strumenti per visualizzare i valori più recenti.

PACCHETTO DATI

DISPOSITIVO / CARICAMENTO

ELENCO DISPOSITIVI

ELENCO DISPOSITIVI NASCOSTI

⊕ Aggiungi

🔌 Connetti

🔌 Disconnetti

📶 Centro aggiornamenti



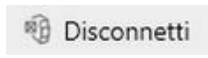
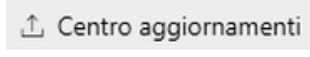

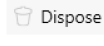


👁️ Nascondi

🗑️ Elimina

🔔










<input type="checkbox"/>	Stato	Nome dispositivo Codice prodotto	Punto finale servizio Numero di serie	Versio... firmw...	Version...	Modal...	Aggiorna info centro	Estensioni	Azioni
<input checked="" type="checkbox"/>	Gruppo predefinito del dispositivo (3)								
<input type="checkbox"/>	●	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B04	-	-	-	-	<div><div>🔔</div><div>🔌</div><div>📶</div><div>📄</div><div>▶</div><div>🔍</div><div>🔒</div><div>⋮</div></div>
<input type="checkbox"/>	●	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94B02	-	-	-	-	<div><div>🔔</div><div>🔌</div><div>📶</div><div>📄</div><div>▶</div><div>🔍</div><div>🔒</div><div>⋮</div></div>
<input checked="" type="checkbox"/>	●	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-	-	-	<div><div>🔔</div><div>🔌</div><div>📶</div><div>📄</div><div>▶</div><div>🔍</div><div>🔒</div><div>⋮</div></div>


Pulsanti della scheda:

Pulsante	Descrizione
	Fare clic sul pulsante Aggiungi per aggiungere un nuovo dispositivo. Per ulteriori informazioni, vedere Aggiungi dispositivo , pagina 23.
	Fare clic sul pulsante Collega per stabilire una connessione con il dispositivo o i dispositivi selezionati.
	Fare clic sul pulsante Scollega per terminare la connessione al dispositivo o ai dispositivi selezionati.
	Fare clic sul pulsante Centro aggiornamenti per aprire la finestra di dialogo Centro aggiornamenti . Consente di configurare le impostazioni per l'esecuzione di un aggiornamento del firmware o di un aggiornamento del file di configurazione sicurezza per il dispositivo o i dispositivi selezionati. Per ulteriori informazioni, vedere Centro aggiornamenti , pagina 68.
	Fare clic sul pulsante Nascondi per nascondere il dispositivo o i dispositivi rilevati. Per ulteriori informazioni, vedere Vista Dispositivo/Caricamento , pagina 55.
	Fare clic sul pulsante Elimina per eliminare il dispositivo o i dispositivi rilevati. Per ulteriori informazioni, vedere Vista Dispositivo/Caricamento , pagina 55.
	Fare clic sul pulsante Area di notifica per visualizzare l'area di notifica sul lato destro della scheda Dispositivo/Caricamento . Per ulteriori informazioni, vedere Visualizzazione/Conferma dei messaggi , pagina 67.
	Fare clic sul pulsante Stato rilevamento dispositivo per visualizzare la vista Stato rilevamento dispositivo sul lato destro della scheda Dispositivo/Caricamento . Per ulteriori informazioni, vedere Monitoraggio dello stato rilevamento dispositivo , pagina 66.

Elementi della tabella:

Elemento	Descrizione
Gruppo	È possibile assegnare i dispositivi visualizzati nell' ELENCO DISPOSITIVI a gruppi diversi, come descritto nel capitolo Raggruppamento di dispositivi nell' ELENCO DISPOSITIVI , pagina 56. Per selezionare tutti i dispositivi appartenenti a un gruppo , selezionare la casella di controllo del gruppo .
Caselle di controllo	Selezionare più caselle di controllo sul lato sinistro per eseguire la stessa operazione su più dispositivi contemporaneamente, ad esempio le operazioni Collega / Scollega o di aggiornamento.


Elemento	Descrizione
Stato	<p>Visualizza lo stato del dispositivo</p> <ul style="list-style-type: none"> Grigio: il dispositivo è scollegato dalla rete. Giallo: il dispositivo è collegato alla rete ma non sono state immesse credenziali valide. Verde: sono state immesse credenziali valide. Blu: lo strumento sta caricando il contenuto nel dispositivo. Rosso: il dispositivo si sta riavviando dopo il download del firmware per completare l'installazione.
Nome dispositivo Riferimento commerciale	<p>Visualizza il nome e il riferimento commerciale (CR) del dispositivo.</p> <p>NOTA: Se al dispositivo è stato assegnato un Nome descrittivo, tale nome definito dall'utente viene visualizzato solo se il protocollo di comunicazione supporta questo parametro. Modbus TCP, ad esempio, non lo supporta.</p>
Punto finale servizio Numero di serie	Visualizza l'indirizzo del punto finale del servizio come URI (Uniform Resource Identifier) e il numero di serie (SN) del dispositivo.
Versione firmware	Visualizza la versione corrente del firmware del dispositivo.
Modo	<p>Disponibile solo dopo l'accesso: indica la modalità del dispositivo: RUN, STOP, BUSY, NOCONF, RESERVED, ENTERED, LOADING, COMPLETED, REQUIRERESTART, ERROR. Il contenuto di questa cella viene aggiornato periodicamente.</p> <p>NOTA: in base al numero di dispositivi a cui si è collegati, questo tipo di monitoraggio può avere un impatto sulla larghezza di banda della rete.</p>
Aggiorna info centro	<p>Visualizza le impostazioni di aggiornamento configurate nella finestra di dialogo Centro aggiornamenti: Firmware selezionato, Configurazione sicurezza selezionata, Aggiornamento firmware riuscito, Aggiornamento firmware annullato, Aggiornamento firmware non riuscito. Per ulteriori informazioni, vedere Centro aggiornamenti, pagina 68.</p>
Estensioni	I dispositivi modulari forniscono un collegamento (Estensioni) che consente di accedere alle singole estensioni del dispositivo. Per ulteriori informazioni, vedere Accesso alle estensioni , pagina 64.
Azioni	Per ogni dispositivo sono disponibili icone che consentono di eseguire diverse operazioni specifiche:
	<p>Fare clic sull'icona Imposta credenziali e immettere le credenziali per la connessione al dispositivo nella finestra di dialogo Imposta credenziali. L'icona nera indica che per il dispositivo non sono memorizzate credenziali. L'icona gialla indica che le credenziali sono state memorizzate ma che non è stato eseguito alcun accesso al dispositivo.</p> <p>In alternativa, è possibile configurare le credenziali globali per il progetto tramite Impostazioni > Progetto > Impostazioni credenziali utente. Per ulteriori informazioni, consultare Gestione delle credenziali utente, pagina 61.</p>
	L'icona Imposta credenziali verde indica che le credenziali per il dispositivo sono state convalidate e che l'accesso è stato eseguito correttamente.
	<p>L'icona Imposta credenziali rossa indica che il tentativo di accesso al dispositivo non è riuscito.</p> <p>Eseguire di nuovo la procedura di accesso e accertarsi di utilizzare le credenziali corrette.</p>
	Fare clic sull'icona Collega / Scollega per stabilire o terminare una connessione al dispositivo.
	<p>Fare clic sull'icona Centro aggiornamenti per aprire la finestra di dialogo Centro aggiornamenti. Consente di configurare le impostazioni per l'esecuzione di un aggiornamento del firmware o di un aggiornamento del file di configurazione sicurezza per il dispositivo. Per ulteriori informazioni, vedere Centro aggiornamenti, pagina 68.</p>
	Fare clic sull'icona Registro dispositivo per visualizzare le informazioni di registro.
	<p>Fare clic sull'icona Avvia dispositivo per avviare il dispositivo.</p> <p>NOTA: Eseguire un test di avviamento prima di utilizzare regolarmente le apparecchiature di automazione e controllo elettrico dopo l'installazione o l'aggiornamento. Per ulteriori informazioni, vedere Avviamento e verifica, pagina 7.</p>
	<p>Visualizza lo stato del certificato.</p> <ul style="list-style-type: none"> Grigio: Certificato attendibile Rosso: Certificato non attendibile <p>Fare clic sull'icona Certificato dispositivo per aprire la finestra di dialogo Informazioni certificato. Per ulteriori informazioni, vedere Gestione dello stato di attendibilità dei certificati nella scheda Dispositivo/Caricamento, pagina 47.</p>
	Indica che il dispositivo è dotato di una scheda di memoria SD. Fare clic su questa icona per scaricare il software direttamente sulla scheda di memoria SD.

Elemento	Descrizione
	Fare clic sull'icona Opzioni dispositivo aggiuntive per un elenco di comandi disponibili per i dispositivi dopo l'accesso riuscito. Per ulteriori informazioni, vedere <i>Dettagli disponibili dopo l'accesso</i> , pagina 56.
Avanzamento	Visualizza lo stato di avanzamento dell'aggiornamento del firmware.

Aggiungi dispositivo

Panoramica

La finestra di dialogo **Aggiungi dispositivo** si apre facendo clic sul pulsante

 nella scheda **Dispositivo/Caricamento** o facendo clic sul pulsante **Nessun dispositivo trovato. Per aggiungere un dispositivo, fare clic qui** visualizzato quando l'elenco dei dispositivi è vuoto, ad esempio se si crea un nuovo progetto.

La finestra di dialogo "Aggiungi dispositivo" ha un titolo verde con un'icona di chiusura. All'interno, a sinistra, c'è un campo di ricerca "Cerca codice prodotto" con un pulsante "Cerca...". Sotto, un'area di lista "Codice prodotto:*" mostra una lista di codici: 140***, 140*** (modernizzato), 171***, 171*** (modernizzato), ATS***, ATS*** (modernizzato), ATV***, ATV*** (modernizzato). A destra, c'è un menu a tendina "Collegamento:*" con "HTTP/HTTPS" selezionato, un checkbox "Sicuro" con la spunta, e un campo "Indirizzo IP:*" con "172.10.15.25" e un campo per il port "443". In basso a sinistra, una nota spiega che "Modernizzato" significa commercializzato dopo il 2019, con un link al catalogo prodotti Schneider Electric. In basso a destra, ci sono i pulsanti "Aggiungi dispositivo" e "Annulla".

Consente di aggiungere i dispositivi manualmente se non possono essere rilevati automaticamente da EcoStruxure Automation Device Maintenance perché il dispositivo non supporta il rilevamento o la funzionalità di rilevamento dispositivi è disattivata. Per questo scopo, selezionare il riferimento commerciale.

Per impostazione predefinita, l'elenco di **Codici prodotto** contiene solo modelli di codici prodotto (come **BME*****, **BMX***** o **Qualsiasi dispositivo**). In questo caso, sono disponibili due opzioni:

- Selezionare il modello corrispondente al prodotto: ad esempio, per BMEP582020, selezionare **BME***** dall'elenco.

NOTA: per ogni modello che copre la versione obsoleta (ad esempio, **BME*****) e quella recente (ad esempio, **BME*** (modernizzato)**) sono fornite due varianti che differiscono nei protocolli supportati. Quindi, se non si trova il protocollo prescelto nell'elenco **Connessione**, selezionare la seconda opzione fornita per il prodotto.

- Per compilare l'elenco con i codici prodotto dei dispositivi in uso, copiare i pacchetti dati corrispondenti nella cartella configurata come **Repository locale** nella finestra di dialogo **Impostazioni > Impostazioni pacchetto**. Per ulteriori informazioni, vedere il capitolo *Configurazione delle ubicazioni dei pacchetti*, pagina 37. Nella tabella verranno quindi visualizzati codici specifici (ad esempio **BMEP582020** o **BMXNOR0200**).

Componente	Descrizione
Riferimento commerciale	Selezionare il numero di Riferimento commerciale del dispositivo dall'elenco e immettere le informazioni sul dispositivo in base al protocollo selezionato dall'elenco Connessione sul lato destro.
Connessione	Selezionare il protocollo utilizzato per la comunicazione dall'elenco: <ul style="list-style-type: none">• HTTP/HTTPS• MODBUS (SL)• MODBUS (TCP)• OPC UA• FTP• USB I parametri vengono adattati in base al protocollo selezionato.
Sicuro	Questa opzione è disponibile solo per la comunicazione HTTP/HTTPS : Selezionare l'opzione se il dispositivo è collegato tramite connessione sicura (HTTPS).
Indirizzo IP	Immettere l'indirizzo IP del dispositivo da aggiungere e la porta utilizzata per la comunicazione.
ID unità	Questa opzione è disponibile solo per la comunicazione MODBUS (TCP) : Immettere il nodo di identificazione dell'unità per la comunicazione Modbus TCP. Per informazioni più dettagliate sulle specifiche Modbus, vedere Modbus Specifications and Implementation Guides .

NOTA: EcoStruxure Automation Device Maintenance V3.1 e versioni successive supportano l'aggiunta di dispositivi tramite riferimento commerciale. Se si cerca di aprire i file di progetto creati con EcoStruxure Automation Device Maintenance V3.0 e versioni precedenti che contengono dispositivi senza riferimento commerciale, viene richiesto di selezionare un riferimento commerciale per ogni dispositivo sconosciuto.

Vedere inoltre [Apertura del progetto](#), pagina 29.

Configurazione delle impostazioni

Panoramica

La pagina **Impostazioni** consente di configurare le impostazioni generali.

Impostazioni

Globale

Rilevamento

DPWS

Modbus TCP

Comunicazione

Impostazione pacchetto

Sicurezza

Gestione certificato

PKI

Syslog

Registri

Lingua

Raggruppa

Progetto

Reimposta

Rilevamento


Modalità rilevamento: ☒ Manuale ☐ Automatico

Scanner	<input checked="" type="checkbox"/> Abilita scanner	Stato
DPWS	<input checked="" type="checkbox"/>	Non attivo
Modbus TCP	<input checked="" type="checkbox"/>	Non attivo

Ok Annulla Applica

Componenti	Descrizione
Discovery	Selezionare per configurare la modalità di rilevamento. Per ulteriori informazioni, consultare Configurazione della modalità di rilevamento del dispositivo , pagina 32.
DPWS	Selezionare per configurare i dettagli dello scanner DPWS. Per ulteriori informazioni, consultare Configurazione dello scanner DPWS , pagina 36.
Modbus TCP	Selezionare per configurare i dettagli dello scanner Modbus. Per ulteriori informazioni, consultare Configurazione dello scanner Modbus TCP , pagina 34.
Comunicazione	Selezionare per configurare le impostazioni di comunicazione. Per ulteriori informazioni, consultare Configurazione delle impostazioni di comunicazione , pagina 37.
Impostazione pacchetto	Selezionare per configurare le impostazioni dei pacchetti. Per ulteriori informazioni, consultare Configurazione delle ubicazioni dei pacchetti , pagina 37.
Sicurezza	Selezionare l'opzione per attivare la modalità di protezione e per visualizzare le notifiche relative a caratteristiche di sicurezza, ad esempio comunicazioni crittografate con certificati, pacchetti protetti o supporto syslog. Per ulteriori informazioni, consultare Funzionalità di sicurezza , pagina 41.
Gestione certificato	Selezionare questa opzione per registrare il certificato dell'applicazione per EcoStruxure Automation Device Maintenance e gestire lo stato di attendibilità dei certificati digitali dei partner di comunicazione. Per ulteriori informazioni, consultare Gestione dei certificati , pagina 43.
PKI	Selezionare per configurare l'infrastruttura a chiave pubblica (PKI). Per ulteriori informazioni, consultare Gestione dell'infrastruttura a chiave pubblica (PKI) , pagina 48.
Registri	Selezionare per visualizzare i file di registro EcoStruxure Automation Device Maintenance e configurare le impostazioni di registro. Per ulteriori informazioni, consultare Visualizzazione dei file di registro , pagina 38.
Lingua	Selezionare per configurare la lingua desiderata. Per ulteriori informazioni, consultare Configurazione della lingua , pagina 40.
Gruppo	Selezionare per raggruppare i dispositivi visualizzati nell' ELENCO DISPOSITIVI . Per ulteriori informazioni, consultare Raggruppamento di dispositivi nell'ELENCO DISPOSITIVI , pagina 56.
Progetto > Impostazioni credenziale utente	Selezionare per immettere le credenziali globali per i dispositivi del progetto. Per ulteriori informazioni, consultare Gestione delle credenziali utente , pagina 61.

Applicazione delle modifiche

Ogni volta che si modificano le impostazioni in una scheda della pagina **Impostazioni**, questa scheda viene contrassegnata dall'icona di aggiornamento  che indica la presenza di modifiche in questa pagina non ancora applicate.

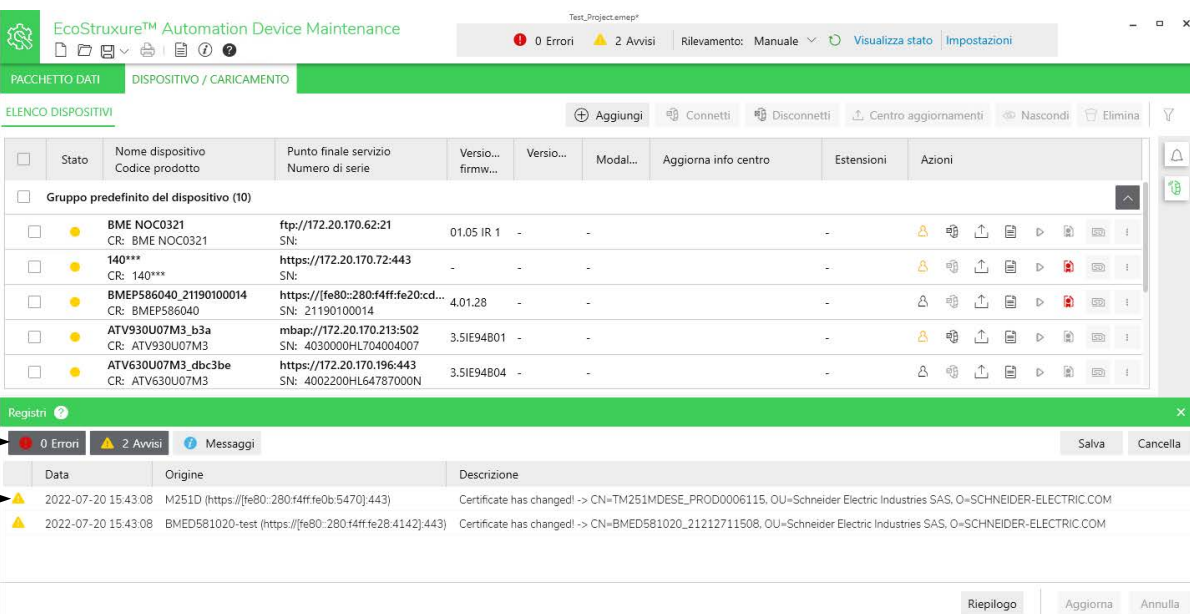
Per applicare le modifiche a questa pagina, fare clic sul pulsante **Applica**.

Per applicare le modifiche apportate in tutte le schede e chiudere la pagina **Impostazioni**, fare clic sul pulsante **OK**.

Finestra degli errori e degli avvisi

Panoramica

I dettagli relativi agli errori rilevati possono essere visualizzati nel tool in una finestra di riepilogo dei registri. Il registro degli errori fornisce informazioni dettagliate su come risolvere l'errore rilevato per il dispositivo selezionato. Se non sono stati risolti gli errori rilevati, non si può passare all'aggiornamento del firmware del dispositivo selezionato.



The screenshot shows the 'Registri' (Logs) window in the EcoStruxure Automation Device Maintenance tool. The window has a title bar with 'Registri' and a close button. Below the title bar, there is a status bar showing '0 Errori' (0 Errors) and '2 Avvisi' (2 Warnings). The main area contains a table with the following columns: Data, Origine, and Descrizione. Two error entries are listed:

Data	Origine	Descrizione
2022-07-20 15:43:08	M251D (https://fe80:280:f4ff:fe0b:5470:443)	Certificate has changed! -> CN=TM251MDESE_PROD0006115, OU=Schneider Electric Industries SAS, O=SCHNEIDER-ELECTRIC.COM
2022-07-20 15:43:08	BMED581020-test (https://fe80:280:f4ff:fe2b:4142:443)	Certificate has changed! -> CN=BMED581020_21212711508, OU=Schneider Electric Industries SAS, O=SCHNEIDER-ELECTRIC.COM

At the bottom of the window, there are buttons for 'Riepilogo' (Summary), 'Aggiorna' (Update), and 'Annulla' (Cancel).

Legenda	Nome	Descrizione
A	Stato errori e avvisi	Visualizza il numero di errori e avvisi rilevati.
B	Registri	Visualizza il numero di errori e avvisi rilevati con una descrizione.

Visualizzazione del registro errori e avvisi

Passo	Azione
1	<p>Fare clic sullo stato Errori o Avvisi nella barra degli strumenti.</p> <p>La finestra Registri visualizza le seguenti informazioni:</p> <ul style="list-style-type: none"> Numero di errori rilevati, avvisi rilevati e informazioni. Descrizione degli errori rilevati.
2	Selezionare l'errore rilevato, l'avvertenza rilevata e/o i messaggi informativi prescelti.


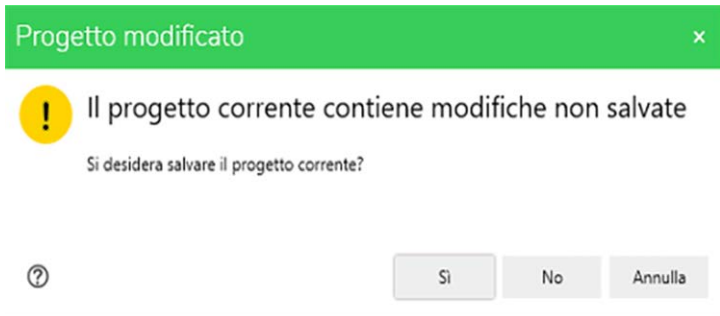
Passo	Azione
3	Fare clic su Salva per salvare l'errore, l'avviso rilevato selezionato e i messaggi informativi.
4	Fare clic su Cancella per rimuovere dal registro tutti i messaggi relativi agli errori e agli avvisi rilevati.

Creazione di un nuovo progetto EcoStruxure Automation Device Maintenance

Procedura

Questa funzionalità permette di creare un nuovo progetto EcoStruxure Automation Device Maintenance.

Per creare un nuovo progetto, seguire la procedura indicata:

Passo	Azione
1	<p>Fare clic sull'icona .</p> <p>Risultato: viene visualizzata la finestra di dialogo Progetto modificato se si apre un progetto modificato e non ancora salvato.</p>
2	<p>Nella finestra di dialogo Progetto modificato, fare clic su Sì per salvare le modifiche al progetto aperto o su No per chiudere il progetto senza salvare.</p>  <p>Risultato: il progetto aperto viene chiuso e si apre un nuovo progetto che mostra la scheda Dispositivo/Caricamento e l'elenco dispositivi vuoto.</p>


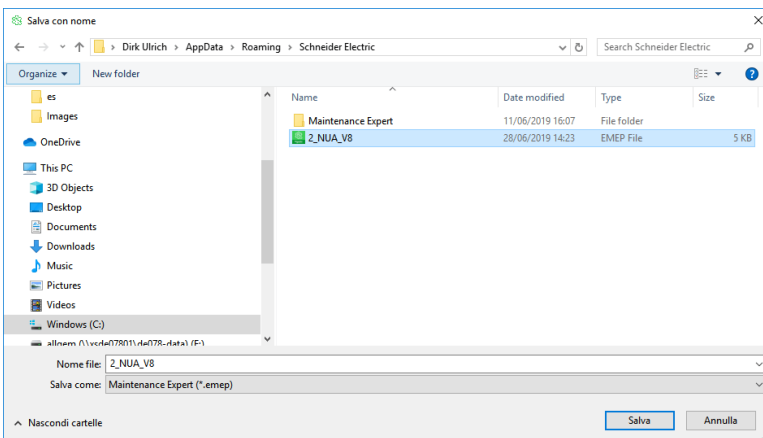

Creando un nuovo progetto, vengono eseguite automaticamente le attività seguenti:

- La modalità di rilevamento è impostata su **Manuale**.
- Le voci del file di registro vengono cancellate.

Salvataggio del progetto

Questa funzionalità consente di salvare una copia del progetto corrente con un nome diverso o in un percorso diverso. Il vantaggio è che i dispositivi non devono essere aggiunti più volte quando si apre il tool EcoStruxure Automation Device Maintenance.


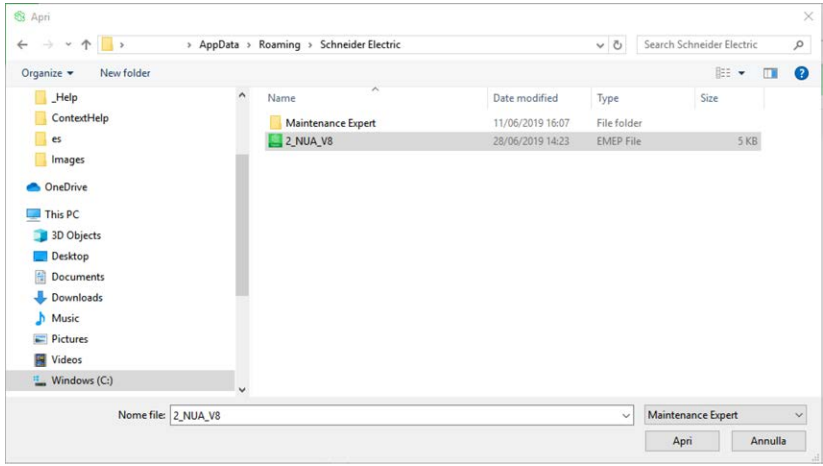
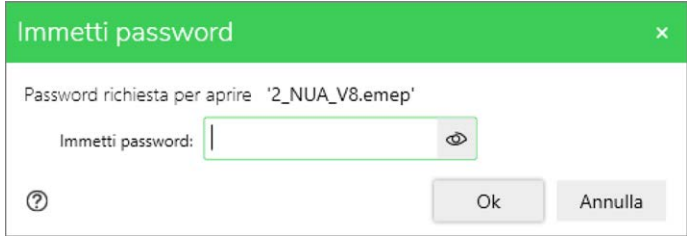
Procedere come segue per salvare le impostazioni del progetto:

Passo	Azione
1	Fare clic sull'icona  .
2	Per salvare le modifiche apportate al progetto corrente, fare clic su Salva . Per salvare una copia del progetto, fare clic su Salva con nome .
3	Selezionare la cartella nella quale si vuole salvare il progetto e immettere il nome file . 
4	Fare clic su Salva e immettere la stessa password in entrambi i campi della finestra di dialogo Imposta password . 
5	Fare clic su OK per continuare.

Apertura del progetto

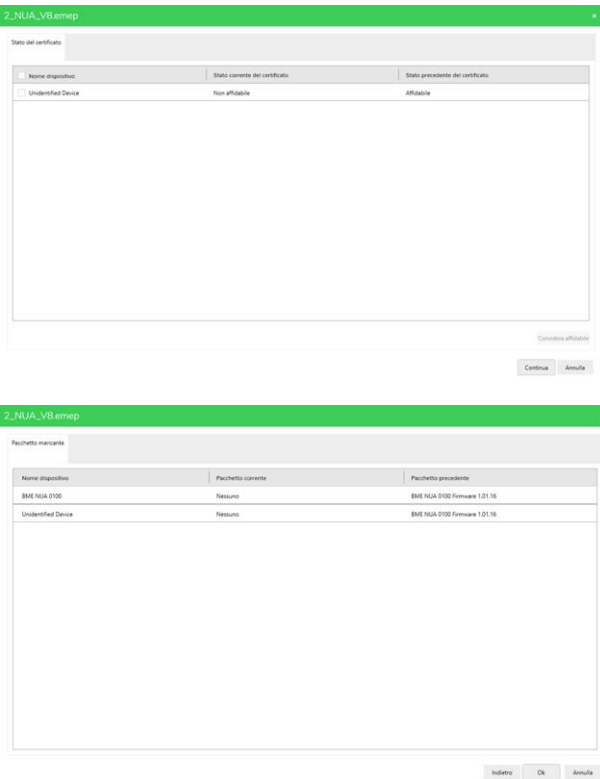
Apertura di un progetto

Per aprire un progetto, procedere come segue:

Passo	Azione
1	<p>Fare clic sull'icona .</p> 
2	<p>Selezionare la cartella e il progetto. Fare clic su Apri e specificare la password.</p> 
3	<p>Fare clic su Ok per aprire il progetto.</p>

Passaggi facoltativi per i file di progetto creati in un altro computer

Se si tenta di aprire un file di progetto creato su un altro computer, opzionalmente il tool indica le differenze di stato di attendibilità del certificato e di disponibilità del pacchetto.



In questo caso, procedere come segue:

Passo	Azione
4	Selezionare i dispositivi che si considerano affidabili e fare clic su Considera affidabile .
5	Fare clic su Continua .
6	Fare clic su OK per aprire il progetto con i pacchetti mancanti o fare clic su Annulla .

Passo opzionale per file di progetto con dispositivi non identificati

Se si cerca di aprire i file di progetto creati con EcoStruxure Automation Device Maintenance V3.0 e versioni precedenti che contengono dispositivi senza codici prodotto, viene visualizzata una finestra di dialogo che chiede di selezionare un riferimento commerciale per ogni dispositivo sconosciuto dall'elenco:

Unidentified_3.0.1.emep

Il progetto contiene dispositivi con un codice prodotto sconosciuto.
Verificare la selezione predefinita di seguito o selezionare un altro codice prodotto dall'elenco a discesa.

Il progetto è stato probabilmente creato con una versione precedente di EcoStruxure Automation Device Maintenance.
L'opzione per aggiungere manualmente dispositivi non identificati non è più supportata in questa versione.

Punto finale servizio	Codice prodotto
COM3/255	ATV***
mbap://145.0.0.1:502	ATV***
mbap://145.0.0.2:502	ATV***

Nota: Modernizzato = commercializzato dopo il 2019.
Per ulteriori informazioni, vedere il [Catalogo prodotti Schneider Electric](#)

Ok Annulla

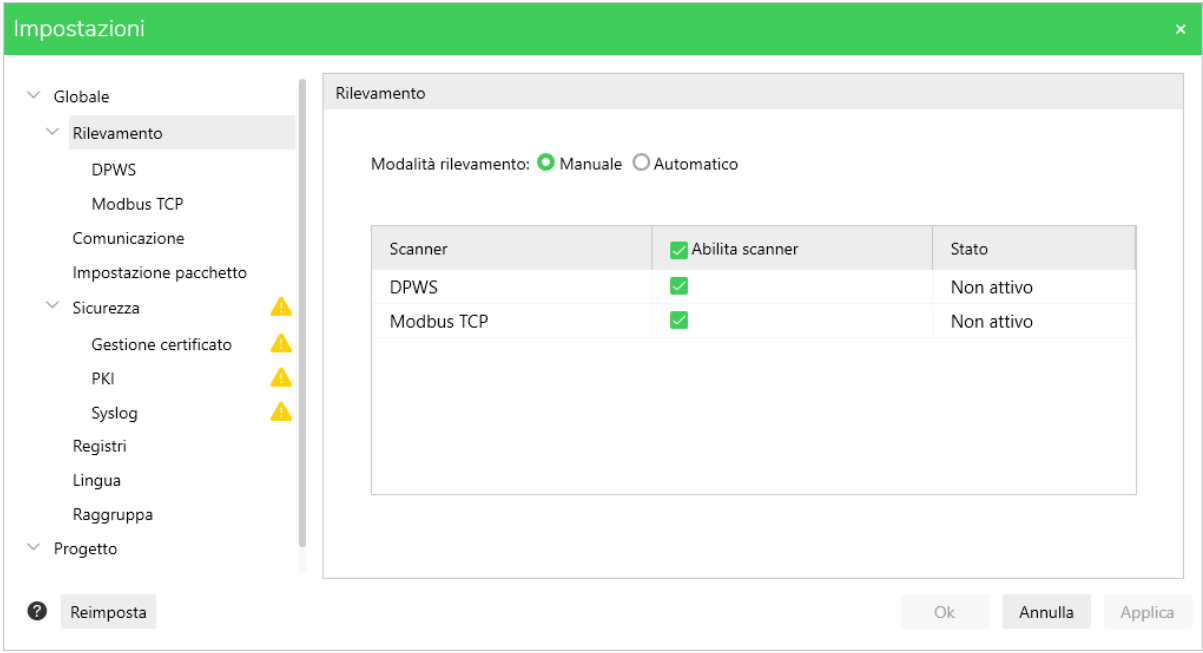
Selezionare i riferimenti commerciali desiderati e fare clic su **Ok** per aprire il progetto.

Configurazione del tool EcoStruxure Automation Device Maintenance

Configurazione della modalità di rilevamento del dispositivo

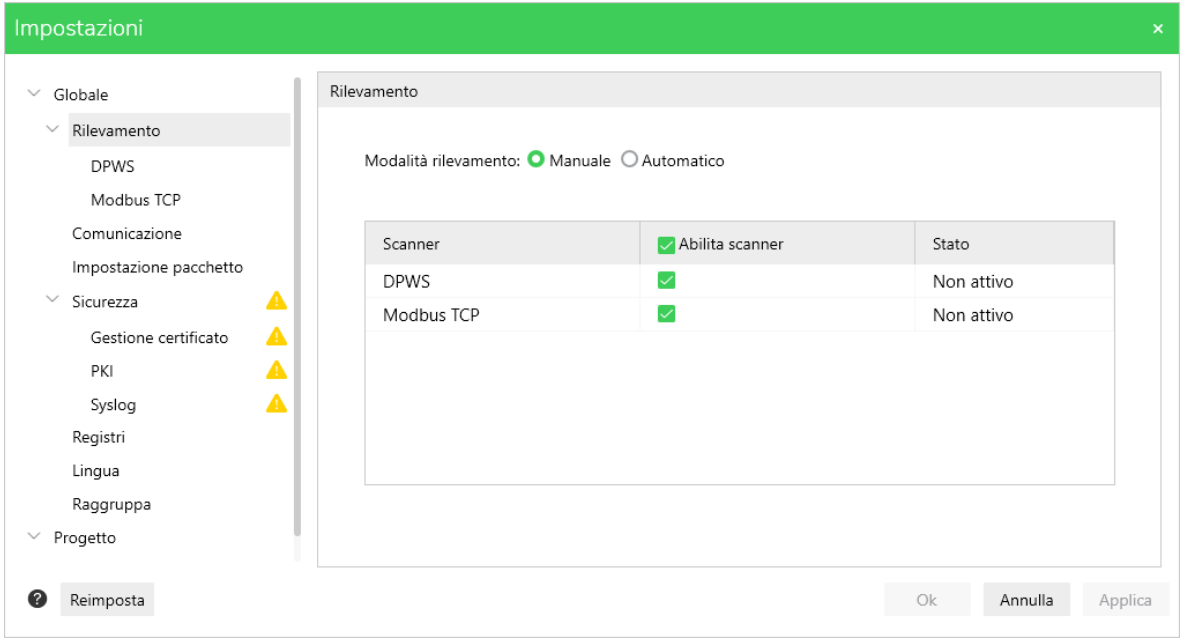
Configurazione della modalità di rilevamento automatico

È possibile selezionare la modalità di rilevamento dispositivi **Automatico** o **Manuale**. Nel rilevamento **Automatico**, il tool invia periodicamente informazioni sulla rete in background e riceve informazioni dai dispositivi che rispondono.

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	<p>Fare clic sull'opzione Rilevamento.</p> 
3	Selezionare la modalità Automatico .
4	Selezionare gli scanner che parteciperanno al rilevamento. Usare questa impostazione per evitare che vengano rilevati dispositivi non voluti.
5	Fare clic su Applica e poi su OK .

Configurazione della modalità di rilevamento manuale

È possibile selezionare la modalità di rilevamento dispositivi **Manuale** per rilevare i dispositivi collegati in rete quando necessario.

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Fare clic sull'opzione Rilevamento . 
3	Selezionare la modalità Manuale .
4	Selezionare gli scanner che parteciperanno al rilevamento. Usare questa impostazione per evitare che vengano rilevati dispositivi non voluti.
5	Fare clic su Applica e poi su OK .

Configurazione dello scanner Modbus TCP

Panoramica

Lo scanner **Modbus TCP** invia richieste codice funzione 43 Modbus a tutti gli indirizzi IP in un intervallo definito da un **indirizzo IP iniziale** e un **indirizzo IP finale**.

È possibile configurare i seguenti parametri **Modbus TCP**:

Elemento	Valore predefinito	Descrizione
Sezione Indirizzo IP :		
Parametro Nome intervallo	–	Nome opzionale dell'intervallo indirizzi.
Parametro Indirizzo IP iniziale	127.0.0.1	Primo indirizzo del campo di scansione degli indirizzi.
Parametro Indirizzo IP finale	127.0.0.1	Ultimo indirizzo del campo di scansione degli indirizzi.
Pulsante Importa	–	Fare clic sul pulsante Importa per importare un file di configurazione disponibile in formato .csv (vedere l'esempio di file di configurazione importato di seguito, pagina 34). NOTA: questo comando consente di sovrascrivere le impostazioni di configurazione presenti. Accertare di eseguire prima il backup delle impostazioni. Risultato: si apre una finestra di dialogo Apri file di Windows che consente di cercare il file csv nella rete. Fare clic su Apri per importare le impostazioni di configurazione dal file. Per applicare le nuove impostazioni, fare clic su Applica o Ok .
Pulsante + Aggiungi	–	Fare clic sul pulsante + Aggiungi per creare un nuovo intervallo di indirizzi. Risultato: viene aggiunta una nuova riga alla tabella con: Nome intervallo = Predefinito Indirizzo IP iniziale = 127.0.0.1 Indirizzo IP finale = 127.0.0.1
Casella di controllo	–	Selezionare/deselezionare una casella di controllo per includere/escludere l'intervallo selezionato per la scansione Modbus.
Pulsante Cestino	–	Fare clic sul pulsante del cestino per rimuovere l'intervallo selezionato, ossia una riga della tabella.
Sezione Impostazioni avanzate :		
Parametro Porta iniziale	502	Prima porta del campo di scansione delle porte.
Parametro Porta finale	502	Ultima porta del campo di scansione delle porte.
Parametro Timeout	4000	Tempo massimo di attesa tra l'invio di un ping al dispositivo e la ricezione della risposta.
Parametro ID unità	255	ID unità Modbus utilizzato per accedere al dispositivo.

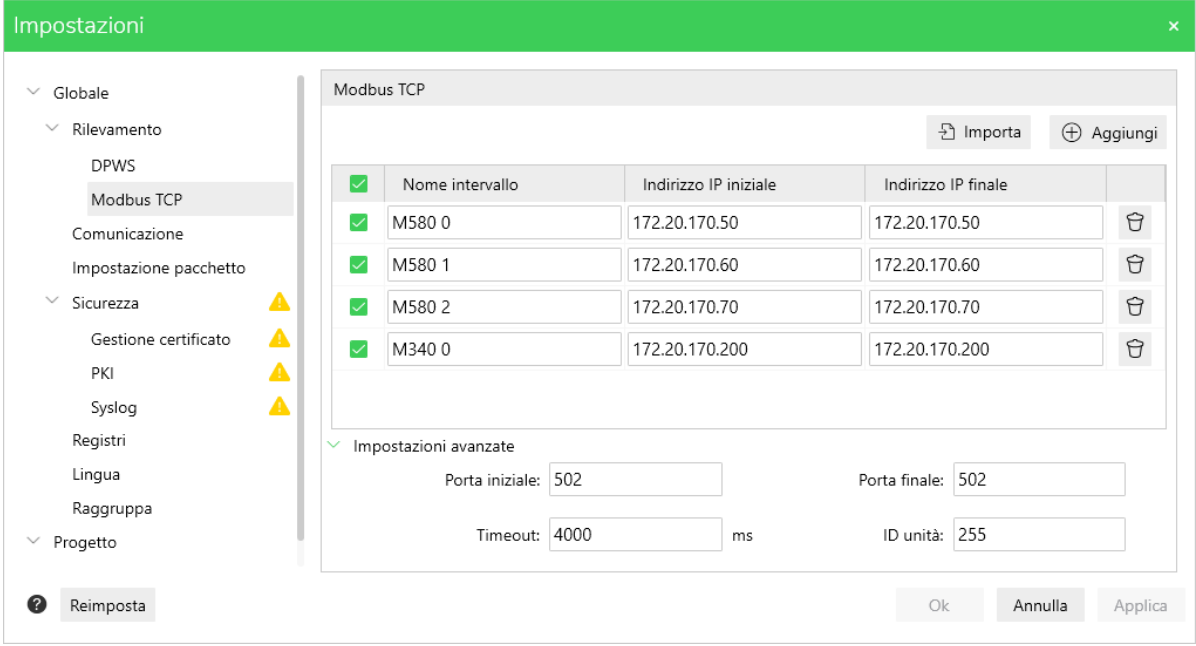
Esempio di file di configurazione di importazione

Il formato del file di configurazione in formato .csv deve essere compatibile con l'esempio seguente:

```
enabled;name;start;end
1;range 1;127.0.0.1;127.0.0.1
1;range 2;127.0.0.2;127.0.0.2
```

Configurazione dello scanner Modbus TCP

Procedere come segue per configurare lo scanner **Modbus TCP**:

Passo	Azione
1	Espandere il menu Rilevamento nella pagina Impostazioni .
2	Selezionare il nodo Modbus TCP .
3	Nella vista Modbus TCP sul lato destro, fare clic sul pulsante Aggiungi per creare un nuovo intervallo di indirizzi.
4	<p>Fare clic sul pulsante Importa per importare un file di configurazione o configurare i parametri seguenti:</p> <ul style="list-style-type: none">• Nome intervallo• Indirizzo IP iniziale• Indirizzo IP finale• Porta iniziale• Porta finale• Timeout• ID unità 
5	Fare clic su Applica per applicare le impostazioni Modbus TCP o su Ok per applicare tutte le modifiche alle impostazioni dell'applicazione e chiudere la finestra di dialogo Impostazioni .

Configurazione dello scanner DPWS

Panoramica

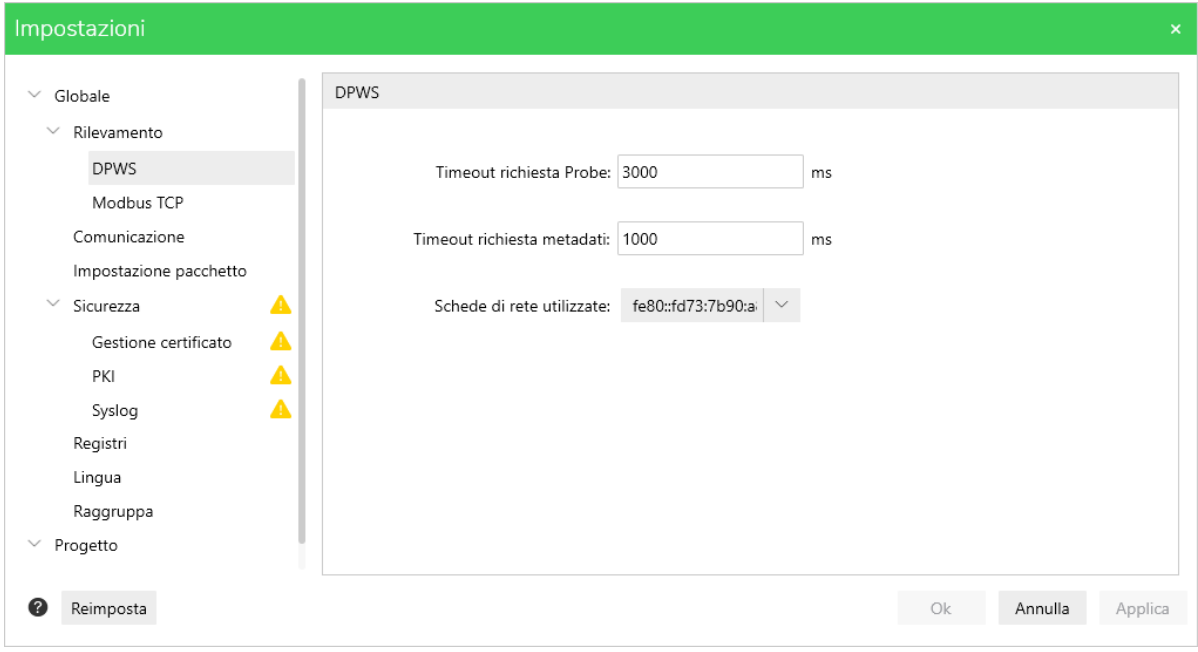
Lo scanner **DPWS** è un'implementazione sul lato client dello standard **DPWS**, che consente di rilevare i dispositivi compatibili con DPWS.

Per informazioni più dettagliate sugli standard DPWS, vedere <http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>.

È possibile configurare i seguenti parametri **DPWS**:

Parametro	Valore predefinito	Descrizione
Timeout richiesta Probe	3000 ms	Tempo massimo di attesa tra l'invio di una richiesta probe e la ricezione della risposta di corrispondenze probe dai dispositivi.
Timeout richiesta metadati	1000 ms	Tempo massimo di attesa tra l'invio di una richiesta di metadati e la ricezione della risposta dai dispositivi.
Schede di rete utilizzate	–	Elenco delle schede di rete da utilizzare per l'invio della richiesta probe DPWS .

Procedere come segue per configurare lo scanner **DPWS**:

Passo	Azione
1	Espandere il menu Rilevamento nella pagina Impostazioni .
2	<p>Selezionare DPWS e immettere i seguenti dettagli:</p> <ul style="list-style-type: none"> • Timeout richiesta Probe • Timeout richiesta metadati • Schede di rete utilizzate 
3	Fare clic su Applica e poi su OK .

Configurazione delle impostazioni di comunicazione

Panoramica

Impostazioni

Globale

Rilevamento

DPWS

Modbus TCP

Comunicazione

Impostazione pacchetto

Sicurezza

Gestione certificato

PKI

Syslog

Registri

Lingua

Raggruppa

Progetto

Comunicazione

Timeout

Timeout: 6000 ms

Interrogazione stato dispositi...

Frequenza (Alta priorità): 3000 ms

Frequenza (Bassa priorità): 10000 ms

Reimposta

Ok

Annulla

Applica

È possibile configurare le seguenti impostazioni di comunicazione per la comunicazione tra EcoStruxure Automation Device Maintenance e i dispositivi:


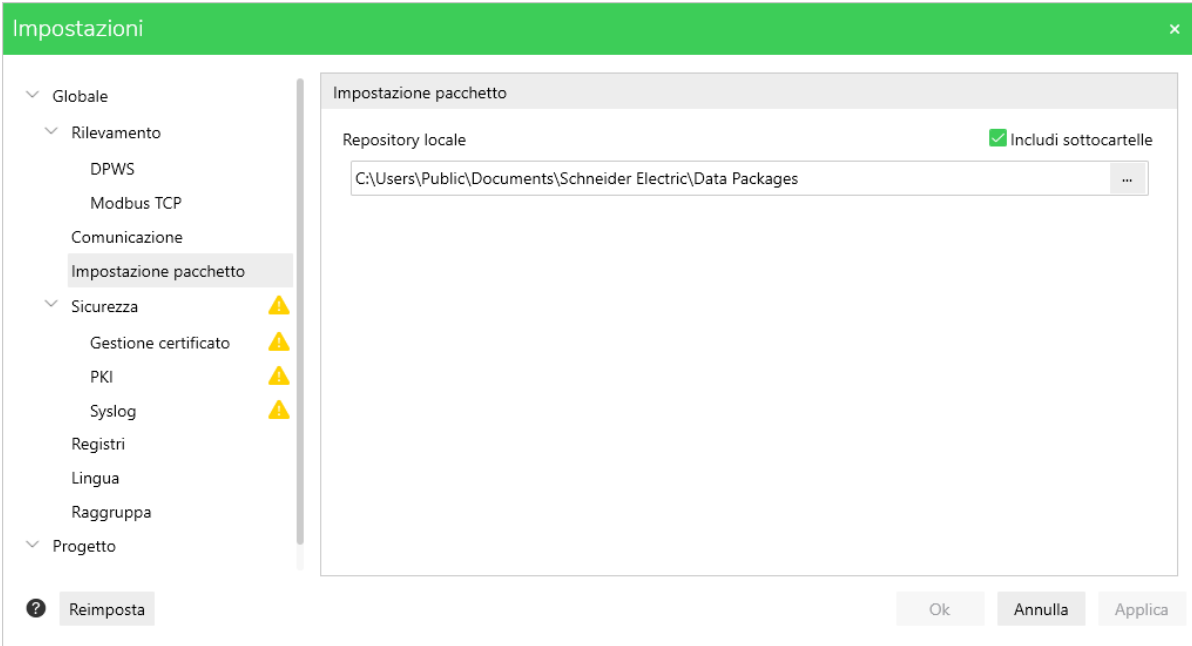
Parametro	Valore predefinito	Descrizione
Sezione Timeout :		
Timeout	6000 ms	Tempo di attesa massimo dopo le richieste / risposte inviate / ricevute da EcoStruxure Automation Device Maintenance (ad esempio, aggiornamenti firmware, impostazione della configurazione IP). Per i timeout che si applicano alle richieste di rilevamento, consultare scanner Modbus TCP, pagina 34 e scanner DPWS, pagina 36.
Sezione Interrogazione stato dispositivo automatica : questi parametri definiscono la frequenza di invio delle richieste di interrogazione ai dispositivi rilevati per mantenere aggiornato lo stato del dispositivo, pagina 21:		
Frequenza (Alta priorità):	3000 ms	L'interrogazione ad alta priorità viene utilizzata quando si eseguono gli aggiornamenti del firmware. Consente di velocizzare il rilevamento del dispositivo dopo il riavvio.
Frequenza (Bassa priorità):	10.000 ms	La bassa priorità con cicli di interrogazione meno frequenti è utilizzata nel funzionamento normale.

Configurazione delle ubicazioni dei pacchetti

È possibile configurare il percorso dei pacchetti dati firmware disponibili nello strumento. Ciò consente di aggiornare le versioni firmware del dispositivo. Inoltre, il riferimento commerciale specifico fornito da ciascun pacchetto dati viene aggiunto all'elenco **Riferimento commerciale** nella finestra di dialogo **Aggiungi dispositivo**, pagina 23.

Modifica dell'ubicazione del pacchetto

Procedere come segue per modificare il percorso del pacchetto:


Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Impostazioni pacchetto .
3	Selezionare il percorso per modificare la posizione del Repository locale .
4	<p>Fare clic sull'icona  e selezionare la cartella di destinazione per cambiare il percorso.</p> 
5	Fare clic su Applica e poi su OK .

Visualizzazione dei file di registro

È possibile visualizzare i registri memorizzati e analizzarne i dettagli relativi al dispositivo selezionato.

Per visualizzare i registri seguire questa procedura:

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home.
2	Selezionare l'opzione Registri .
3	Impostare la creazione del registro su Attiva/Inattiva .
4	Selezionare il percorso per modificare l'ubicazione del file di registro.

Passo	Azione
5	<p>Fare clic sull'icona  e selezionare la cartella di destinazione per cambiare il percorso.</p> <div><div>Impostazioni</div><div><div><div>Globale</div><div>Rilevamento</div><div>DPWS</div><div>Modbus TCP</div><div>Comunicazione</div><div>Impostazione pacchetto</div><div>Sicurezza</div><div>Gestione certificato</div><div>PKI</div><div>Syslog</div><div>Registri</div><div>Lingua</div><div>Raggruppa</div><div>Progetto</div></div><div><div>Registri</div><div><div>Attivo</div><div>Non attivo</div></div><div>C:\Users\AdminUser\AppData\Local\Temp\AutomationDeviceMaintenance.log</div><div><div>Il file di registro contiene dati sensibili. Eliminare il file di registro dopo l'uso o memorizzarlo in una posizione sicura.</div></div></div><div><div>Reimposta</div><div>Ok</div><div>Annulla</div><div>Applica</div></div></div><p>NOTA: Per ulteriori informazioni sulla notifica di sicurezza informatica, vedere Raccomandazione per una sicurezza informatica ottimizzata, pagina 68.</p></div>
6	Fare clic su Applica e poi su OK .

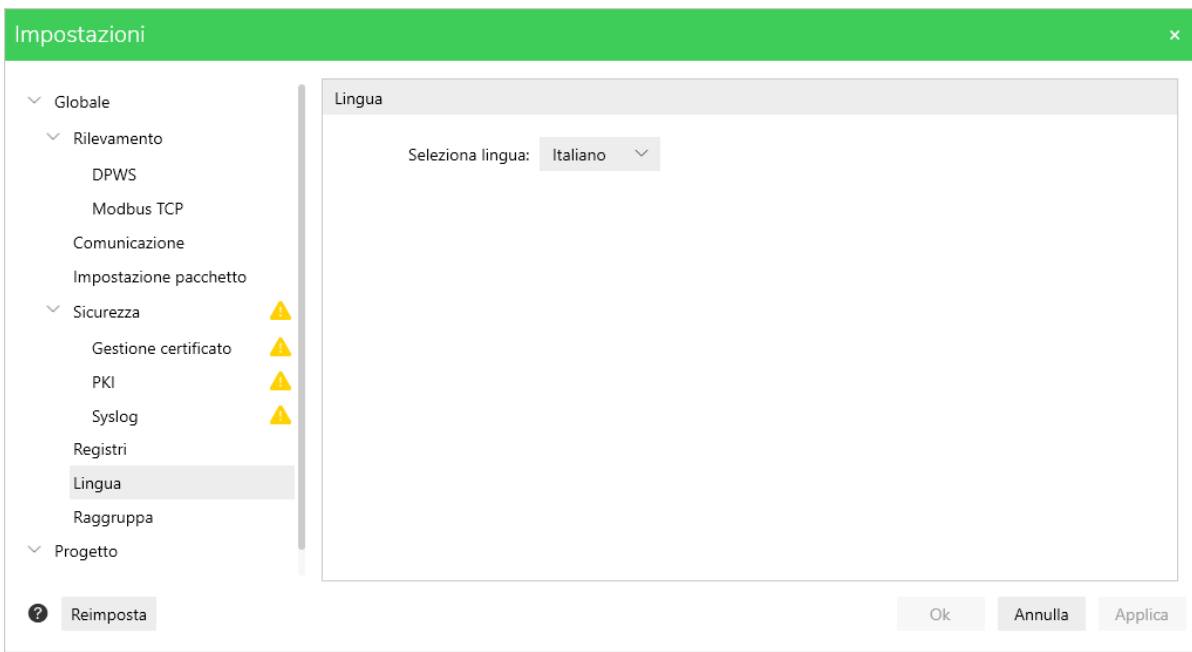
Configurazione della lingua

È possibile impostare la lingua per visualizzare il contenuto del tool EcoStruxure Automation Device Maintenance nella lingua preferita.

Sono supportate le seguenti lingue:

- Inglese
- Tedesco
- Francese
- Spagnolo
- Italiano
- Cinese

Procedere come segue per impostare la lingua:

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Lingua .
3	<p>Fare clic nell'elenco a discesa Seleziona lingua per selezionare la lingua desiderata.</p> 
4	<p>Fare clic su Applica e poi su OK.</p> <p>NOTA: Riavviare EcoStruxure Automation Device Maintenance per applicare le modifiche della lingua.</p>

Ripristino delle impostazioni dell'applicazione

Panoramica

Le finestre di dialogo del menu **Impostazioni** contengono un pulsante **Reimposta** nell'angolo inferiore sinistro.

Fare clic sul pulsante **Reimposta** per ripristinare i valori di tutte le impostazioni dell'applicazione configurate tramite il menu **Impostazioni** ai valori predefiniti.

Configurazione delle funzionalità di sicurezza

Panoramica

Le migliori pratiche e soluzioni per la sicurezza informatica sono in continua evoluzione in funzione delle informazioni disponibili più recenti. Come criteri di progettazione, Schneider Electric incorpora conoscenze e tecniche aggiornate per contribuire a rendere i prodotti più resistenti agli attacchi informatici. L'approccio alla sicurezza fin dalla progettazione si traduce nell'implementazione di meccanismi per mitigare le minacce, ridurre i punti deboli sfruttabili e difendersi da violazioni dei dati e attacchi informatici evitabili.

NOTA:

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* fornito su [Schneider Electric website](#).

A causa del rapido aumento delle macchine e degli impianti di rete, anche le potenziali minacce stanno rapidamente aumentando. Pertanto, considerare attentamente tutte le possibili misure di sicurezza.

Sono necessarie misure di sicurezza per proteggere i dati e i canali di comunicazione da accessi non autorizzati.

NOTA: prima di configurare le funzionalità di protezione, rivolgersi all'amministratore della sicurezza per verificare che le impostazioni di sicurezza siano corrette.

Funzionalità di sicurezza

Panoramica

EcoStruxure Automation Device Maintenance supporta le seguenti funzionalità di sicurezza:

- Comunicazione crittografata mediante certificati digitali in un'infrastruttura a chiave pubblica (PKI).
- Gestione di pacchetti Schneider Electric Data Package Secure (SEDPS) con firma digitale.
- Protocollo di rete Syslog.

Attivazione/disattivazione della modalità di protezione

Se si lavora all'interno di una rete protetta e non si utilizzano funzionalità di sicurezza, è possibile disabilitare le notifiche relative alle funzionalità di sicurezza (ad esempio, i punti esclamativi gialli) tramite l'opzione **Sicurezza** della pagina **Impostazioni**.

The screenshot shows the 'Impostazioni' (Settings) window with a green header. On the left, a sidebar lists various settings categories: Globale, Rilevamento, DPWS, Modbus TCP, Comunicazione, Impostazione pacchetto, Sicurezza (highlighted with a yellow warning icon), Gestione certificato, PKI, Syslog, Registri, Lingua, Raggruppa, and Progetto. The main area displays the 'Sicurezza' (Security) settings. Under 'Modalità protezione:', there are two radio buttons: 'Protezione standard' (selected) and 'Nessuna protezione'. Below these, there is a section 'Importa file di configurazione sicurezza:' with a text input field containing 'Seleziona file', an ellipsis button, and an 'Importa' button. At the bottom of the window, there are buttons for 'Reimposta', 'Ok', 'Annulla', and 'Applica'.

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Sicurezza .
3	Selezionare l'opzione per attivare la modalità di protezione e visualizzare le notifiche relative alle funzionalità di sicurezza.

Importazione di un file di configurazione di sicurezza

EcoStruxure Automation Device Maintenance consente di importare le impostazioni di configurazione di sicurezza configurate globalmente per la rete nell'applicazione EcoStruxure Cybersecurity Admin Expert. Se queste impostazioni sono disponibili come file, importare il file come segue:

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Sicurezza .
3	Nella sezione Importa file di configurazione di sicurezza , fare clic sul pulsante Importa per passare al file di configurazione di protezione.
4	Fare clic su Apri per importare le impostazioni di configurazione di sicurezza dal file.

Per aggiornare il file di configurazione sicurezza, utilizzare il **Centro aggiornamenti** come descritto nel capitolo **Aggiornamento del file di configurazione sicurezza**, pagina 71.

Gestione dei certificati

Panoramica

I certificati digitali sono necessari per garantire la comunicazione protetta tramite i rispettivi protocolli (ad esempio, HTTPS) in un'infrastruttura a chiave pubblica (PKI).

Nel contesto di TLS, è possibile utilizzare i certificati per verificare l'identità dei partner di comunicazione. I certificati vengono scambiati quando si stabilisce una connessione, questa attività viene detta handshake TLS. L'invio del certificato è facoltativo per il client (in questo caso: il certificato dell'applicazione di EcoStruxure Automation Device Maintenance), a meno che il server non richieda il certificato client. Il server, invece, invia sempre il suo certificato. Solo se il risultato della verifica del certificato è positiva, è possibile stabilire una connessione con il partner di comunicazione.

EcoStruxure Automation Device Maintenance supporta le modalità di attendibilità del certificato seguenti:

- Modalità di attendibilità manuale: È possibile considerare attendibili/non attendibili i certificati dei partecipanti alla comunicazione protetta manualmente. Lo stato di attendibilità viene gestito nelle schede **Certificati attendibili** / **Certificati non attendibili** della finestra di dialogo **Gestione certificato**, pagina 46.
- Modalità di attendibilità elenco di autorizzati: È possibile importare un elenco di autorizzati con il file di configurazione di sicurezza, pagina 42. EcoStruxure Automation Device Maintenance considera automaticamente attendibili i certificati contenuti nell'elenco.
- Modalità di attendibilità registrazione / Autorità di certificazione (CA): EcoStruxure Automation Device Maintenance considera attendibili automaticamente i certificati registrati con i certificati CA disponibili nella cartella **Autorità di certificazione radice attendibili** dell'**Archivio certificati** di Windows.

Considerazioni sull'uso dei certificati

Tenere presenti i seguenti aspetti quando si devono usare dei certificati per le comunicazioni sicure.

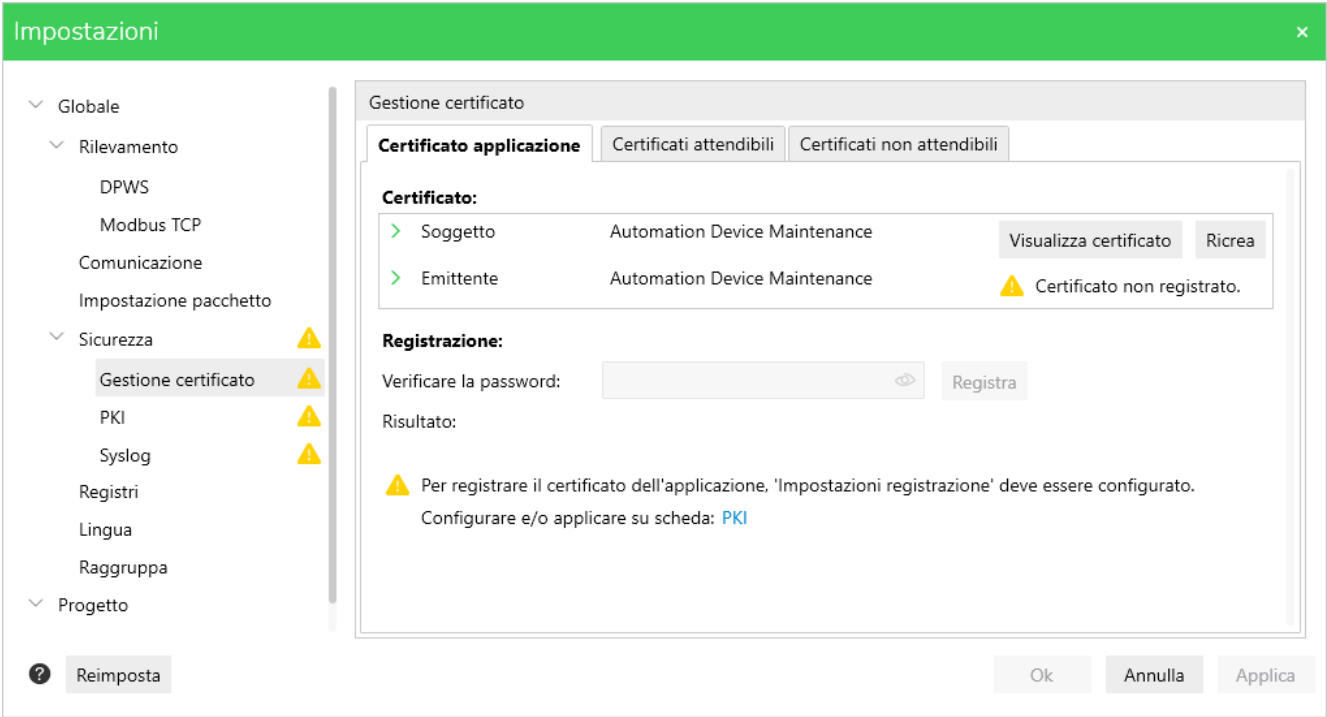
- È richiesta un'attività di amministrazione dei certificati, dato che questi hanno una validità limitata e pertanto devono essere aggiornati a intervalli regolari. Tenere conto di questo fatto per quanto concerne il ciclo di vita della macchina o del controllo.
- Le impostazioni relative a data e ora del PC Windows vengono utilizzate per verificare se il certificato è ancora valido. Verificare le impostazioni a intervalli regolari tramite Windows **Start > Impostazioni > Ora e lingua > Data e ora**.
- Se il PC che esegue EcoStruxure Automation Device Maintenance è sempre offline, è necessario aggiornare manualmente l'**Elenco di revoche di certificati** (CRL) a intervalli regolari. A questo scopo, collegarsi al punto di distribuzione CRL, scaricare il CRL più recente e installarlo sul PC.
Per l'URL corretto del punto di distribuzione CRL, rivolgersi all'amministratore della sicurezza.
- È inoltre possibile dichiarare i certificati come non attendibili in EcoStruxure Automation Device Maintenance, ad esempio, tramite la finestra di dialogo **Gestione certificato**, pagina 46.

Finestra di dialogo Gestione certificato

Dopo l'installazione iniziale, è disponibile un certificato di applicazione autofirmato predefinito per EcoStruxure Automation Device Maintenance.

La finestra di dialogo **Gestione certificato** fornisce le opzioni seguenti per il certificato dell'applicazione:

- Nuova creazione del certificato dell'applicazione autofirmato e assegnazione di singole proprietà (vedere Nuova creazione del certificato dell'applicazione autofirmato, pagina 44).
- Registrazione del certificato dell'applicazione per assegnare una firma digitale a un'Autorità di certificazione (CA) e creare una catena di attendibilità (vedere Registrazione del certificato dell'applicazione, pagina 45).
- Gestione dello stato di attendibilità dei certificati digitali dei partner di comunicazione (vedere Gestione dello stato di attendibilità dei certificati, pagina 46).



Nuova creazione del certificato dell'applicazione autofirmato

Per creare di nuovo il certificato di applicazione predefinito e assegnare le singole proprietà, procedere come segue:

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Sicurezza > Gestione certificato .
3	Nella scheda Certificato applicazione , fare clic sul pulsante Ricrea . Risultato: viene visualizzata la finestra di dialogo Crea certificato .
4	Immettere le proprietà che si desidera assegnare al certificato e fare clic sul pulsante Ok . Risultato: il certificato autofirmato EcoStruxure Automation Device Maintenance viene presentato agli altri partecipanti della comunicazione con le proprietà definite.

Registrazione del certificato dell'applicazione

Per creare una catena di attendibilità, il certificato dell'applicazione EcoStruxure Automation Device Maintenance deve essere registrato e firmato digitalmente da un'Autorità di certificazione (CA).

Per registrare il certificato, configurare innanzitutto le **Impostazioni di registrazione** come fornito dall'opzione **Impostazioni > Sicurezza > PKI**, pagina 48.

Quindi, seguire questa procedura per registrare il certificato dell'applicazione per EcoStruxure Automation Device Maintenance:

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Sicurezza > Gestione certificato .
3	Nella scheda Certificato applicazione , verificare che il certificato dell'applicazione sia ancora autofirmato e non ancora iscritto: <ul style="list-style-type: none"> Nella sezione Certificato, Oggetto ed Emittente visualizzano lo stesso contenuto: Automation Device Maintenance. La notifica Certificato non registrato è visualizzata nella riga Emittente.
4	Immettere la password per la CA nella casella di testo Verificare la password . Questa password viene utilizzata per autorizzare la richiesta di registrazione. Per ulteriori informazioni, rivolgersi all'amministratore della rete industriale.
5	Fare clic su Registra . <p>Risultato: EcoStruxure Automation Device Maintenance invia alla CA una richiesta di firma del certificato dal certificato dell'applicazione insieme alla password di verifica. Se la password non è corretta, viene restituito un messaggio di registrazione non riuscita.</p> <p>NOTA: Questa procedura sostituisce il certificato dell'applicazione autofirmato predefinito con un nuovo certificato firmato. La sostituzione non può essere annullata.</p>
6	Verificare che il processo sia stato completato correttamente: <ul style="list-style-type: none"> Risultato: il messaggio di registrazione riuscita viene visualizzato nella scheda Certificato applicazione. Nella scheda Generale della finestra di dialogo Informazioni certificato, la voce Emittente è stata modificata nel nome della CA, ad esempio <i>INT-DEV-SUB-CA</i> La scheda Percorso di certificazione della finestra di dialogo Informazioni certificato indica la CA radice e le CA subordinate in una struttura gerarchica in base alla configurazione PKI. Il certificato dell'entità finale nella parte inferiore della struttura gerarchica è il certificato di EcoStruxure Automation Device Maintenance con le voci seguenti: <ul style="list-style-type: none"> CN (Common Name) = Automation Device Maintenance O (Organization) = Schneider Electric

Gestione dello stato di attendibilità dei certificati

Le schede **Certificati attendibili** e **Certificati non attendibili** della finestra di dialogo **Gestione certificato** consentono di gestire lo stato di attendibilità dei certificati disponibili in EcoStruxure Automation Device Maintenance.

In entrambe le schede, ogni certificato contiene le informazioni seguenti:

Componente	Descrizione
Oggetto	Fornisce informazioni generali sul certificato: <ul style="list-style-type: none"> • CN = Nome comune • OU = Unità organizzativa
Nome dispositivo	Fornisce il nome del dispositivo così come viene visualizzato nell' ELENCO DISPOSITIVI della scheda Dispositivo/Caricamento . Se il certificato non appartiene a un dispositivo, viene visualizzato n/d .
Punto finale servizio	Le informazioni sul punto finale del servizio sono fornite per i dispositivi utilizzati nella sessione corrente di EcoStruxure Automation Device Maintenance. Se il certificato non appartiene a un dispositivo, viene visualizzato n/d .
Azione	Consente di aprire la finestra di dialogo Informazioni certificato tramite il collegamento Visualizza certificato .
Stato certificati	Indica lo stato del certificato: <ul style="list-style-type: none"> • Attendibile • Non attendibile

Sui certificati è possibile eseguire le azioni seguenti:

- Per non considerare attendibili i certificati, selezionare uno o più certificati nella scheda **Certificati attendibili** e fare clic sul pulsante **Considera non affidabile**.
- Per considerare attendibili i certificati, selezionare uno o più certificati nella scheda **Certificati non attendibili** e fare clic sul pulsante **Attendibile**. Per considerare attendibili temporaneamente i certificati selezionati, selezionare l'opzione **Questa sessione è attendibile**.
- Per rimuovere i certificati, selezionare uno o più certificati nella scheda **Certificati attendibili** o **Certificati non attendibili** e fare clic sul pulsante **Elimina**.


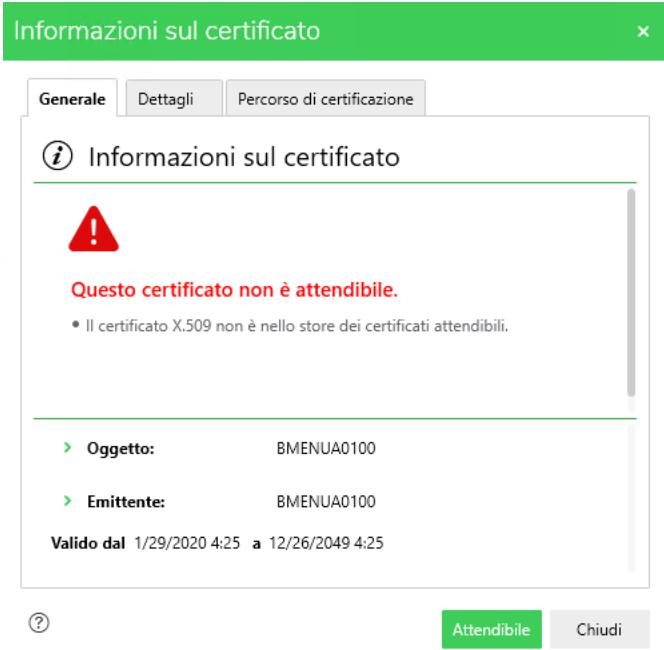
NOTA: i certificati dei dispositivi utilizzati nella sessione corrente EcoStruxure Automation Device Maintenance non possono essere eliminati direttamente. I certificati vengono spostati temporaneamente nell'elenco dei **certificati non attendibili** e rimossi quando si chiude EcoStruxure Automation Device Maintenance.

NOTA: eseguendo questo comando si rimuovono i certificati selezionati dal PC Windows. Verranno inoltre rimossi dall'**Archivio certificati** di Windows.

Gestione dello stato di attendibilità dei certificati nella scheda Dispositivo/Caricamento

È inoltre possibile considerare attendibili/non attendibili i certificati dei dispositivi nella scheda **Dispositivo/Caricamento**.

Per considerare attendibile il certificato del dispositivo nella scheda **Dispositivo/Caricamento**, procedere come segue:

Passo	Azione
1	<p>Fare clic sull'icona Certificato dispositivo  del dispositivo.</p>  <p>NOTA: È possibile indicare temporaneamente come affidabile il certificato del server.</p>
2	Selezionare la casella di controllo Considera temporaneamente affidabile il certificato del dispositivo per la sessione in corso .
3	Fare clic su Considera affidabile il certificato del dispositivo .

Per considerare non attendibile il certificato del dispositivo nella scheda **Dispositivo/Caricamento**, procedere come segue:

Passo	Azione
1	Fare clic sull'icona Certificato dispositivo  del dispositivo.
2	Fare clic su Considera non affidabile il certificato del dispositivo .

Gestione dell'infrastruttura a chiave pubblica (PKI)

Impostazioni per la registrazione del certificato dell'applicazione

Se l'opzione **Sicurezza** è attivata nella finestra di dialogo **Sicurezza** della pagina **Impostazioni**, la finestra di dialogo **PKI** consente di configurare la connessione all'Autorità di certificazione (CA) per la registrazione del certificato di applicazione di EcoStruxure Automation Device Maintenance.

Componente	Descrizione
URL registrazione	Immettere l'URL (Uniform Resource Locator) dell'Autorità di certificazione (CA) che emetterà il certificato.
ID emittente	Immettere l'identificativo dell'emittente dell'autorità di certificazione.
Timeout	Immettere un timeout (in millisecondi) corrispondente alle velocità di trasferimento Internet. Valore predefinito: 10.000 ms
Verifica solo firma	Se questa opzione non è selezionata, il certificato CA deve essere disponibile come certificato attendibile nell' Archivio certificati di Windows. Per verificare solo le firme digitali, selezionare questa opzione.
Pulsante Controlla connessione	Fare clic sul pulsante Controlla connessione per stabilire una connessione al sito Web della CA.
Pulsante Visualizza certificato	Dopo aver stabilito correttamente la connessione alla CA, viene visualizzato il pulsante Visualizza certificato . Fare clic sul pulsante per aprire la finestra di dialogo Informazioni certificato e verificare gli attributi del certificato per assicurarsi di essere connessi alla CA corretta.

Se la connessione al sito Web della CA è stata stabilita correttamente, selezionare l'opzione **Sicurezza > Gestione certificato** e procedere con la registrazione del certificato dell'applicazione.

Attivazione della registrazione dei messaggi Syslog

Panoramica

La finestra di dialogo **Syslog** consente di attivare la funzione syslog e configurare EcoStruxure Automation Device Maintenance come client syslog. EcoStruxure Automation Device Maintenance fornirà quindi un sottoinsieme dei messaggi di registro generati al server syslog corrispondente utilizzando le impostazioni syslog configurate in questa finestra di dialogo.


The screenshot shows the 'Impostazioni' (Settings) window with the 'Syslog' configuration tab selected. The left sidebar lists various settings categories: Globale, Rilevamento, DPWS, Modbus TCP, Comunicazione, Impostazione pacchetto, Sicurezza (with a warning icon), Gestione certificato (with a warning icon), PKI (with a warning icon), Syslog (with a warning icon and highlighted), Registri, Lingua, Raggruppa, and Progetto. The main area of the 'Syslog' tab contains the following configuration options:

- Syslog:** A toggle switch set to 'Disabilita' (Disabled), accompanied by a yellow warning triangle icon.
- Indirizzo server:** A text input field containing '127.0.0.1'.
- Porta:** A text input field containing '6514'.
- Protocollo di rete:** Radio buttons for 'UDP', 'TCP', and 'TLS'. The 'TLS' option is selected.
- Controlla connessione:** A button located below the network protocol options.

At the bottom of the window, there is a 'Reimposta' (Reset) button with a question mark icon, and three buttons on the right: 'Ok', 'Annulla' (Cancel), and 'Applica' (Apply).

Attivazione della registrazione dei messaggi Syslog

Per attivare la funzione syslog e configurare la connessione al server syslog, procedere come indicato di seguito:

Passo	Azione
1	Fare clic sul menu Impostazioni nella parte centrale in alto della pagina Home .
2	Selezionare l'opzione Sicurezza > Syslog .
3	Selezionare l'opzione Attiva per attivare la funzione syslog.
4	Nella casella di testo Indirizzo server , immettere l'indirizzo IP del server syslog.
5	Immettere la porta monitorata dal server per i messaggi syslog provenienti dai client.
6	Selezionare l'opzione Protocollo di rete : <ul style="list-style-type: none"> • UDP (User Datagram Protocol) • TCP (Transmission Control Protocol) • TLS (Transport Layer Security)
7	<p>Per le connessioni TCP o TLS, è possibile opzionalmente fare clic sul pulsante Controlla connessione per verificare la connessione al server syslog</p> <p>Risultati:</p> <p>Per le connessioni TCP: viene visualizzato un messaggio che indica se è stata stabilita una connessione al server.</p> <p>Per le connessioni TLS:</p> <ul style="list-style-type: none"> • Viene visualizzato un messaggio che indica se è stata stabilita una connessione al server. • Un'icona indica se il certificato del server syslog è già dichiarato attendibile. Se il certificato non è attendibile, fare clic sull'icona  per aprire la finestra di dialogo Informazioni certificato che consente di verificare il certificato e dichiararlo attendibile. <p>NOTA: poiché UDP è basato su un modello di comunicazione senza connessione, EcoStruxure Automation Device Maintenance non può fornire una soluzione per verificare la connessione. È necessario verificare manualmente se i messaggi syslog vengono ricevuti sul server specificato.</p>

Pacchetto dati

Scheda Pacchetto dati

Tipi di pacchetti dati supportati

Sono supportati i seguenti tipi di file:

- *.fwp
- *.ldx
- *.sedp
- *.sedps

Pacchetti dati protetti

EcoStruxure Automation Device Maintenance supporta pacchetti di dati *.sedps (Schneider Electric Data Package Secure) con firma digitale: Quando la modalità di protezione è attivata, EcoStruxure Automation Device Maintenance verifica che il pacchetto provenga da un'origine verificata e visualizza le notifiche di sicurezza se la firma non è corretta. Per una descrizione generale dei certificati di movimentazione, vedere il capitolo [Gestione dei certificati](#), pagina 43.

Se la modalità di protezione è attivata, pagina 42, si applica quanto segue:

- I file seguenti del pacchetto sono contrassegnati dall'icona di notifica gialla nell'elenco dei pacchetti della scheda **Pacchetto dati** e il messaggio **Impossibile verificare la catena di attendibilità** viene visualizzato sul lato destro:
 - File di pacchetto senza firma.
 - File di pacchetto autofirmati.
 - File di pacchetto che utilizzano un certificato radice non attendibile.
- Questi pacchetti sono inoltre contrassegnati dall'icona di notifica gialla nella scheda **Dispositivo/Caricamento**.
- Se si tenta di eseguire un processo di aggiornamento del firmware con uno di questi pacchetti di dati, il processo viene sospeso e visualizzato il messaggio **Impossibile verificare la catena di attendibilità del pacchetto selezionato. Il download può danneggiare il dispositivo. Continuare?** nell'area di notifica, pagina 67. Leggere attentamente il messaggio e valutare i rischi. Dopo aver confermato il messaggio, il processo continua.
- Se si tenta di eseguire un processo di aggiornamento del firmware con uno di questi pacchetti di dati, gli errori rilevati vengono visualizzati nella finestra **Registri**, pagina 68.

AVVISO

DISPOSITIVI DANNEGGIATI

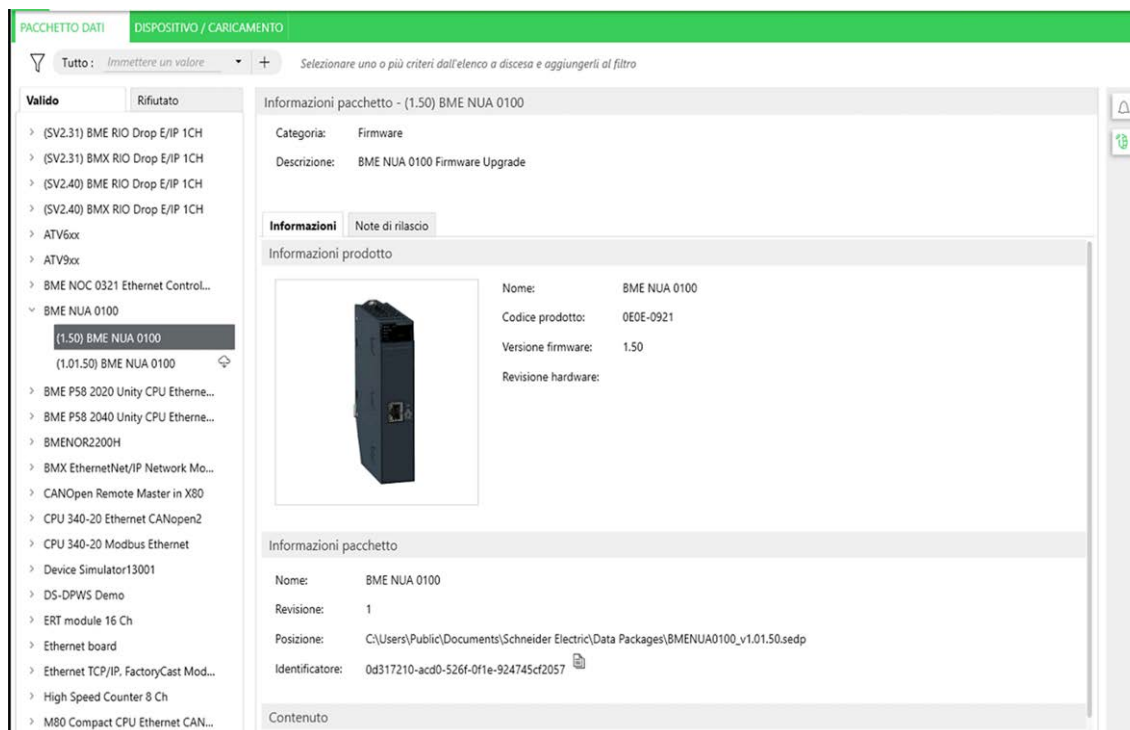
Verificare con attenzione se il pacchetto dati proviene da un'origine attendibile, in quanto il download di un pacchetto dati manomesso può danneggiare il dispositivo.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Panoramica della scheda Pacchetto dati

È possibile visualizzare il contenuto della libreria del pacchetto dati per trovare dettagli sui singoli pacchetti e sul loro contenuto.

Il lato sinistro della scheda visualizza l'elenco dei pacchetti dati disponibili localmente raggruppati per famiglia di dispositivo. Il lato destro della scheda visualizza i dettagli del pacchetto selezionato.



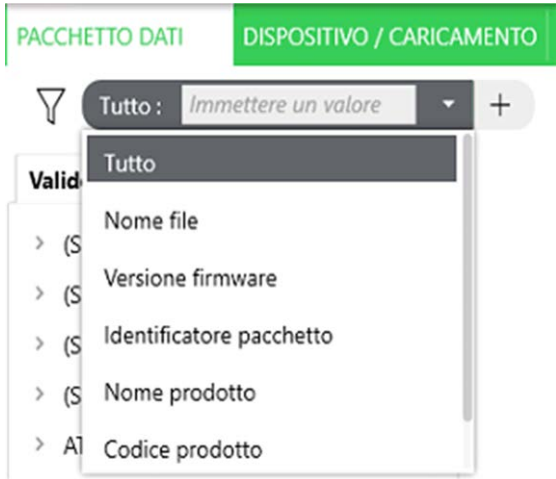
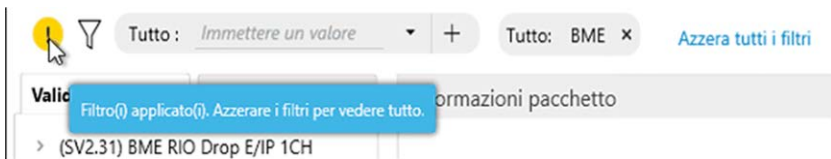
Elenco dei pacchetti dati

L'elenco di pacchetti dati sul lato sinistro consiste di due schede:

- La scheda **Valido** elenca i pacchetti dati disponibili localmente sul PC in uso raggruppati per famiglia di dispositivi.
- La scheda **Rifiutato** elenca i pacchetti dati scaricati sul PC che non è stato possibile elaborare per qualsiasi motivo. Poiché il file del pacchetto dati può essersi danneggiato durante il download, potrebbe essere utile scaricarlo un'altra volta. Se il problema non viene ancora risolto, rivolgersi al rappresentante Schneider Electric per ulteriore assistenza.

Filtraggio dell'elenco pacchetti dati

Per ridurre il numero di pacchetti dati visualizzati nell'elenco, è possibile applicare criteri di ricerca come indicato di seguito:

Passo	Azione
1	<p>Immettere una stringa nel campo di testo Tutti. Per limitare la ricerca su una proprietà di un pacchetto dati specifico, è possibile eventualmente aprire l'elenco e selezionare un criterio di ricerca.</p> 
2	<p>Fare clic sul pulsante Più sul lato destro dell'elenco di ricerca per avviare la ricerca.</p> <p>Risultato: nell'elenco dei pacchetti di dati vengono visualizzate le voci che soddisfano il criterio di ricerca specificato. Un'icona gialla viene visualizzata a sinistra della casella di ricerca per indicare che è applicato un filtro e quindi le voci dell'elenco sono ridotte a questi pacchetti dati che corrispondono al criterio di ricerca.</p> 
3	<p>Ripetere i passaggi 1 e 2 per definire un altro filtro. I filtri sono combinati con la condizione AND.</p> <p>Risultato: nell'elenco dei pacchetti di dati vengono visualizzate le voci che soddisfano entrambi i criteri di ricerca.</p>
4	<p>Per cancellare un singolo filtro, fare clic sul pulsante con la croce del relativo filtro.</p> <p>In alternativa, per rimuovere tutti i filtri definiti, fare clic sul collegamento Azzera tutti i filtri. Viene visualizzato l'elenco completo dei pacchetti dati.</p>

Informazioni pacchetto

Le **Informazioni pacchetto** sul lato destro forniscono informazioni sul pacchetto dati selezionato nell'elenco di pacchetti dati.

La parte superiore fornisce le informazioni seguenti:

- **Categoria**
- **Descrizione**

La scheda **Informazioni** visualizza i seguenti dettagli:

- Sezione **Informazioni prodotto**:
 - Immagine - se disponibile nel pacchetto dati
 - **Nome**
 - **Codice prodotto**
 - **Versione firmware**
 - **Versione hardware**
- Sezione **Informazioni pacchetto**:
 - **Nome**
 - **Revisione**
 - **Posizione**
 - **Identificativo**: Il pulsante **Copia negli Appunti** consente di copiare la stringa di identificazione negli Appunti del PC.
- Sezione **Contenuto**: Fornisce il contenuto del pacchetto dati in un elenco.

La scheda **Note di rilascio** visualizza il contenuto se il pacchetto dati contiene un documento etichettato come `ReleaseNotes`. Se per il pacchetto dati non esiste alcun documento simile, la scheda è vuota.

Dispositivo/Caricamento

Scheda Dispositivo/Caricamento

Panoramica

EcoStruxure Automation Device Maintenance visualizza un determinato insieme di proprietà del dispositivo (come il nome del dispositivo, l'endpoint del servizio, la versione firmware) nella scheda **Dispositivo/Caricamento**.


NOTA: Le informazioni visualizzate in questa scheda vengono aggiornate automaticamente solo se la modalità di rilevamento è impostata su

Automatica. Fare clic sull'icona  della barra degli strumenti per visualizzare i valori più recenti.

PACCHETTO DATI		DISPOSITIVO / CARICAMENTO							
ELENCO DISPOSITIVI		ELENCO DISPOSITIVI NASCOSTI							
		+ Aggiungi Connetti Disconnetti Centro aggiornamenti Nascondi Elimina ▼							
<input type="checkbox"/>	Stato	Nome dispositivo Codice prodotto	Punto finale servizio Numero di serie	Versione... firmw...	Version...	Modal...	Aggiorna info centro	Estensioni	Azioni
<input checked="" type="checkbox"/>		Gruppo predefinito del dispositivo (3)							
<input type="checkbox"/>		ATV630U07M3 dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B04	-	-	-	-	      
<input type="checkbox"/>		ATV630U07M3 a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94B02	-	-	-	-	      
<input checked="" type="checkbox"/>		ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-	-	-	      

Per informazioni sui dettagli visualizzati per i dispositivi, vedere il capitolo Dispositivo/Caricamento, pagina 21.

Dettagli disponibili dopo l'accesso

Dopo aver eseguito correttamente l'accesso a un dispositivo e lo stato del dispositivo è diventato verde, fare clic sul pulsante  per accedere ai comandi seguenti per ogni dispositivo:

Comando	Descrizione
Ottica	Il dispositivo emette un segnale ottico che consente di identificarlo in un rack hardware per i dispositivi che supportano la funzionalità.
Ottica e acustica	Il dispositivo emette un segnale ottico e acustico che consente di identificarlo in un rack hardware per i dispositivi che supportano la funzionalità.
Proprietà	<p>Apri una finestra di dialogo aggiuntiva delle Proprietà che fornisce ulteriori informazioni sul dispositivo in schede diverse:</p> <ul style="list-style-type: none"> La scheda Informazioni sul dispositivo fornisce informazioni generali sul dispositivo: <ul style="list-style-type: none"> Id prodotto Nome prodotto Versione firmware Versione hardware ID hardware Indirizzo MAC La scheda Stato dispositivo fornisce informazioni sullo stato presente del dispositivo. La scheda Configurazione fornisce informazioni sulle impostazioni di configurazione del dispositivo. Se supportato dal dispositivo, le impostazioni di configurazione possono essere modificate in questa scheda. <p>NOTA: le modifiche delle impostazioni di configurazione possono richiedere un riavvio del dispositivo e determinare così l'impostazione del controller nello stato STOP. Gli effetti sono indicati da messaggi visualizzati nell'area di notifica. Leggere attentamente ogni messaggio e confermare dopo aver valutato i rischi. Dopo aver confermato ogni messaggio, il processo continua.</p> <p>Le informazioni sulle Proprietà visualizzate dipendono dal rispettivo dispositivo. Per ulteriori informazioni, vedere la documentazione utente del dispositivo.</p>

Raggruppamento di dispositivi nell'ELENCO DISPOSITIVI

Panoramica

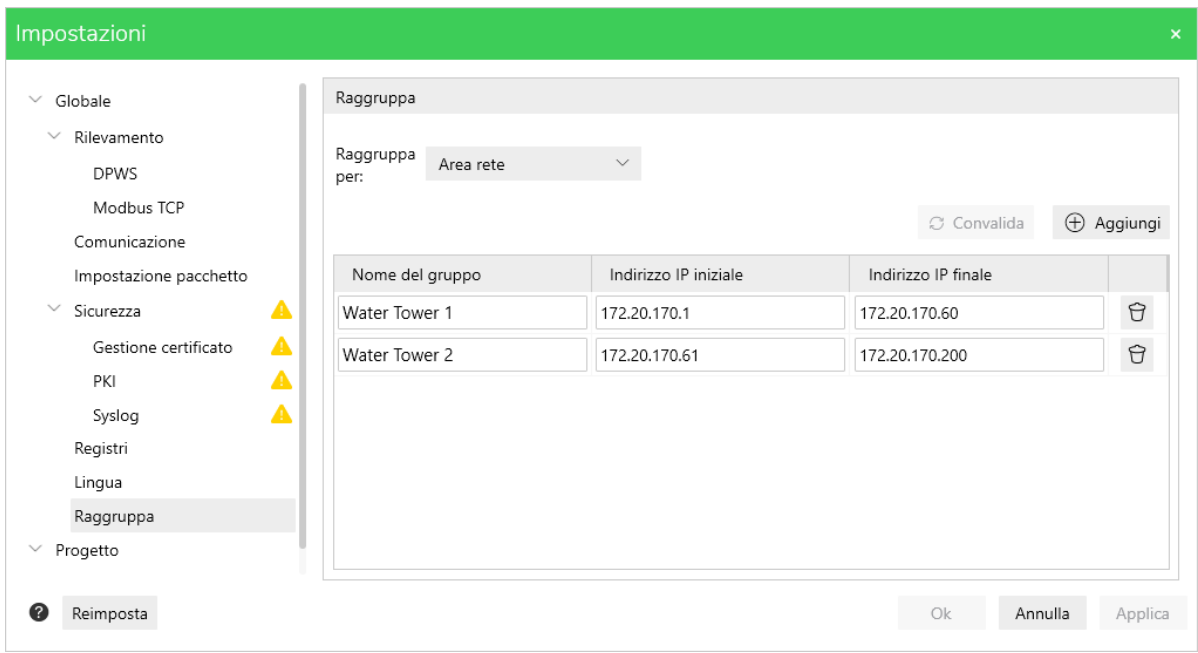
EcoStruxure Automation Device Maintenance consente di strutturare i dispositivi visualizzati nell'**ELENCO DISPOSITIVI** mediante la creazione di gruppi.

EcoStruxure Automation Device Maintenance V3.0 supporta il raggruppamento in base agli indirizzi IP dei dispositivi mediante la definizione di intervalli di indirizzi IP. È possibile aggiungere ulteriori criteri di raggruppamento con versioni successive di EcoStruxure Automation Device Maintenance.

NOTA: questa funzione di raggruppamento è esclusiva degli indirizzi IPv4. Lo standard IPv6 non è supportato da EcoStruxure Automation Device Maintenance V3.0.

Creazione di gruppi

Per raggruppare i dispositivi, procedere come segue:

Passo	Azione
1	Selezionare l'opzione Gruppo nella pagina Impostazioni .
2	Espandere l'elenco Raggruppa per e selezionare l'opzione Area di rete .
3	Fare clic sul pulsante + Aggiungi per creare un nuovo intervallo di indirizzi. Risultato: viene visualizzata una tabella con una riga vuota.
4	Nella cella Nome gruppo , immettere un nome per il gruppo di dispositivi.
5	Nella cella Indirizzo IP iniziale immettere il primo indirizzo IP dell'intervallo di indirizzi per il gruppo di dispositivi.
6	Nella cella Indirizzo IP finale immettere l'ultimo indirizzo IP dell'intervallo di indirizzi per il gruppo di dispositivi.
	
7	Fare clic sul pulsante + Aggiungi per creare un altro gruppo. Oppure Fare clic su Applica per applicare le impostazioni del gruppo . Oppure Fare clic su OK per applicare tutte le modifiche alle impostazioni dell'applicazione e chiudere la finestra di dialogo Impostazioni .

Rimozione di un dispositivo

Panoramica






Si possono rimuovere i dispositivi nascondendoli temporaneamente o eliminandoli definitivamente dalla scheda **Elenco dispositivi** nel menu **Dispositivo/Caricamento**.

Il dispositivo può essere rimosso eseguendo le seguenti azioni:

- Nascondere un dispositivo attivo
- Eliminare un dispositivo attivo
- Eliminare un dispositivo nascosto





Nascondere un dispositivo attivo

Procedere come segue per nascondere un dispositivo attivo:

Passo	Azione
1	Fare clic sulla scheda Dispositivo/Caricamento . I dispositivi attivi rilevati sono elencati nella scheda Elenco dispositivi .
2	In Dispositivo/Caricamento : <ul style="list-style-type: none"> selezionare un singolo dispositivo facendo clic su una cella nella riga del dispositivo. OPPURE Selezionare più dispositivi selezionando le caselle di controllo sul lato sinistro di ogni riga o selezionando l'intero Gruppo.
3	Per i dispositivi selezionati sono attivate le seguenti icone: <ul style="list-style-type: none">  Hide  Dispose
4	Fare clic sull'icona  Hide. Viene visualizzato il messaggio Nascondi dispositivo . <div> <div>Nascondi dispositivo</div> <div>  Si è certi di voler spostare tutti i dispositivi selezionati nell'ELENCO DISPOSITIVI NASCOSTI? I dispositivi nascosti si possono riattivare dall'ELENCO DISPOSITIVI NASCOSTI. </div> <div>  <div> <div>Si</div> <div>No</div> </div> </div> </div>
5	Fare clic su Si per continuare. Il dispositivo selezionato viene spostato nella scheda Elenco dispositivi nascosti . NOTA: È possibile riattivare i dispositivi nascosti da Elenco dispositivi nascosti .







Mostrare un dispositivo nascosto

Procedere come segue per mostrare un dispositivo nascosto:

Passo	Azione
1	Fare clic sulla scheda Dispositivo/Caricamento . I dispositivi nascosti sono elencati nella scheda Elenco dispositivi nascosti .
2	<ul style="list-style-type: none">• selezionare un singolo dispositivo facendo clic su una cella nella riga del dispositivo. OPPURE• Selezionare più dispositivi selezionando le caselle di controllo sul lato sinistro di ogni riga o selezionando l'intero Gruppo.
3	Per i dispositivi selezionati sono attivate le seguenti icone: <ul style="list-style-type: none">•  Unhide•  Dispose
4	 Unhide Fare clic sull'icona  . Il dispositivo selezionato viene spostato nella scheda Elenco dispositivi .







Eliminare un dispositivo attivo

Procedere come segue per eliminare un dispositivo attivo:

Passo	Azione
1	Fare clic sulla scheda Dispositivo/Caricamento . I dispositivi attivi rilevati sono elencati nella scheda Elenco dispositivi .
2	<ul style="list-style-type: none"> selezionare un singolo dispositivo facendo clic su una cella nella riga del dispositivo. OPPURE Selezionare più dispositivi selezionando le caselle di controllo sul lato sinistro di ogni riga o selezionando l'intero Gruppo.
3	Per i dispositivi selezionati sono attivate le seguenti icone: <div>  Hide </div> <ul style="list-style-type: none"> <div>  Dispose </div> <ul style="list-style-type: none">
4	<div>  Dispose </div> <p>Fare clic sull'icona .</p> <p>Viene visualizzato il messaggio Elimina dispositivo.</p> <div> <div>Elimina dispositivo</div> <div>×</div> </div> <div>  Si è certi di voler rimuovere definitivamente i dispositivi selezionati? </div> <p>L'eliminazione di un dispositivo è irreversibile. Un dispositivo eliminato può essere nuovamente rilevato se si seleziona il rilevamento automatico e il dispositivo è ancora accessibile in rete.</p> <div>  <div> <div>Si</div> <div>No</div> </div> </div>
5	Fare clic su Si per continuare. NOTA: Scegliendo Si , il dispositivo viene eliminato in modo definitivo dal tool; se in seguito lo si vuole reinserire, sarà necessario rilevarlo o aggiungerlo manualmente.

Eliminare un dispositivo nascosto

Procedere come segue per eliminare un dispositivo nascosto:

Passo	Azione
1	Fare clic sulla scheda Dispositivo/Caricamento . I dispositivi nascosti sono elencati nella scheda Elenco dispositivi nascosti .
2	<ul style="list-style-type: none"> selezionare un singolo dispositivo facendo clic su una cella nella riga del dispositivo. OPPURE Selezionare più dispositivi selezionando le caselle di controllo sul lato sinistro di ogni riga o selezionando l'intero Gruppo.
3	Per i dispositivi selezionati sono attivate le seguenti icone: <div>  Unhide </div> <ul style="list-style-type: none"> • <div>  Dispose </div> •
4	<div>  Unhide </div> <p>Fare clic sull'icona  .</p> <p>Viene visualizzato il messaggio Elimina dispositivo.</p> <div> <div>Elimina dispositivo</div> <div>×</div> </div> <div>  Si è certi di voler rimuovere definitivamente i dispositivi selezionati? </div> <p>L'eliminazione di un dispositivo è irreversibile. Un dispositivo eliminato può essere nuovamente rilevato se si seleziona il rilevamento automatico e il dispositivo è ancora accessibile in rete.</p> <div>  <div> <div>Si</div> <div>No</div> </div> </div>
5	Fare clic su Si per continuare. NOTA: Scegliendo Si , il dispositivo viene eliminato in modo permanente dal tool e non può essere recuperato.

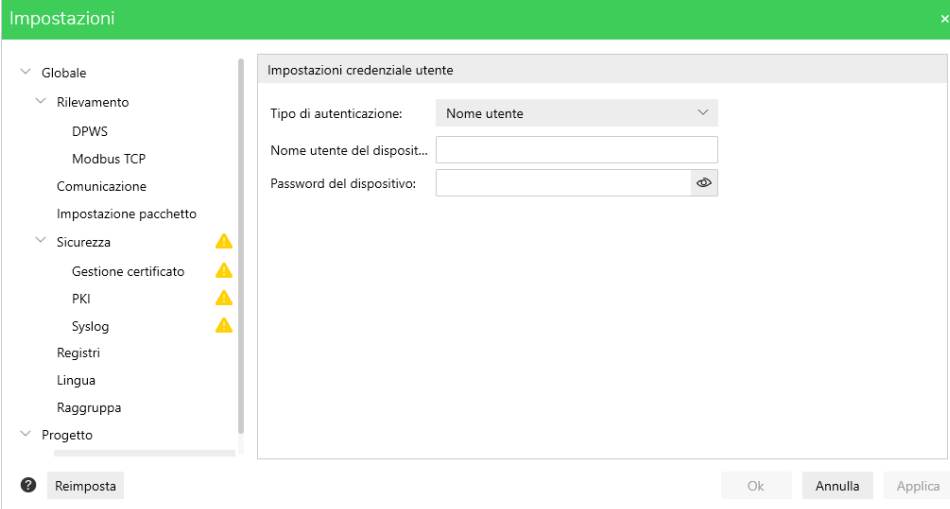
Gestione delle credenziali utente

Panoramica

EcoStruxure Automation Device Maintenance consente di immettere le credenziali per l'accesso autorizzato ai dispositivi a livello globale per il progetto e singolarmente per ogni dispositivo.

Gestione globale delle credenziali utente


Per gestire le credenziali utente a livello globale per il progetto, andare alla pagina **Impostazioni** e selezionare l'opzione **Progetto > Impostazioni credenziali utente**.

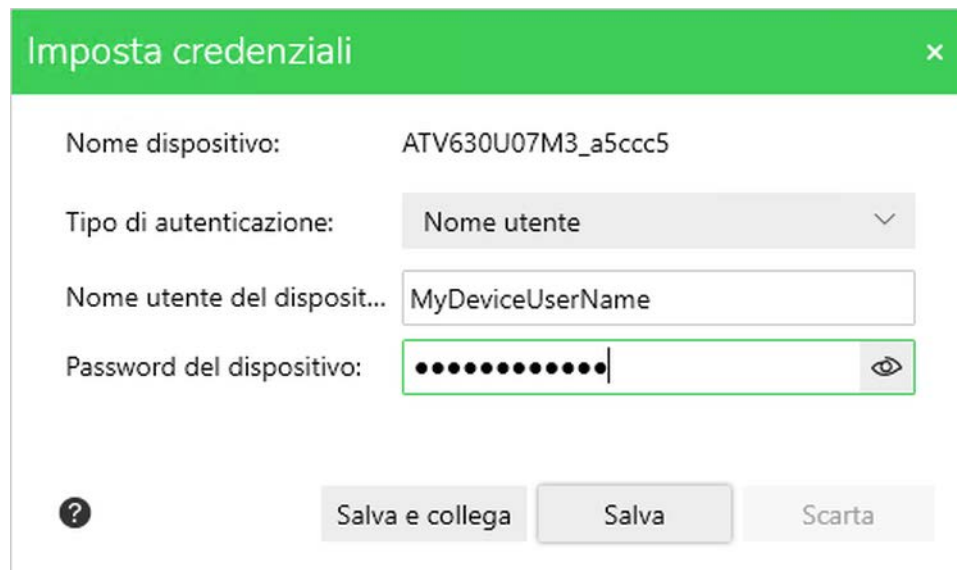


Selezionare **Tipo di autenticazione > Nome utente** o **Tipo di autenticazione > Personalizzato** e immettere le credenziali come richiesto. Fare clic su **OK** per salvare le credenziali. Di conseguenza, l'icona **Imposta credenziali** dei dispositivi applicabili nella pagina **Dispositivo/Caricamento** è impostata su giallo ed è



possibile fare clic sull'icona **Connetti**  o sul pulsante **Connetti**  per l'accesso senza immettere nuovamente le credenziali.

Gestione delle credenziali utente per dispositivo

Per gestire le credenziali utente di ogni singolo dispositivo, aprire la pagina **Dispositivo/Caricamento** e fare clic sull'icona **Imposta credenziali**  nella riga dispositivo della tabella:



È possibile fare clic su **Salva e connetti** per salvare le credenziali e stabilire una connessione con il dispositivo. Dopo l'accesso, l'icona **Imposta credenziali** diventa verde. In alternativa, è possibile fare clic su **Salva** per salvare le credenziali per questo dispositivo per un accesso successivo. In questo caso, l'icona **Imposta credenziali** diventa gialla ed è possibile fare clic sull'icona

Connetti  o sul pulsante  **Connetti** per l'accesso senza immettere nuovamente le credenziali.

Parametri credenziali utente

I parametri visualizzati sono specifici del dispositivo e richiedono le credenziali necessarie per accedere al dispositivo specifico. Per ulteriori informazioni, vedere la documentazione utente del dispositivo.

Per accedere ai controller Modicon M340, Modicon M580 o Momentum, sono necessarie tre password. Per informazioni dettagliate sulla password di protezione dell'applicazione, la password di archiviazione dati e la password di protezione del firmware, consultare i capitoli corrispondenti in *EcoStruxure Control Expert Operating Modes* or the legacy *Unity Pro Operating Modes* manual. I collegamenti per scaricare le traduzioni di questo manuale sono forniti nell'elenco dei Documenti correlati in questa guida online, pagina 10.

Accesso alle estensioni

Panoramica

Un dispositivo modulare nell'**ELENCO DISPOSITIVI** della scheda **Dispositivo/Caricamento** fornisce un collegamento che consente di accedere alle singole estensioni del dispositivo.

Esempio di un dispositivo modulare:

PACCHETTO DATI		DISPOSITIVO / CARICAMENTO							
ELENCO DISPOSITIVI		ELENCO DISPOSITIVI NASCOSTI							
<div>⊕ Aggiungi</div> <div>🔌 Connetti</div> <div>🔌 Disconnetti</div> <div>🔄 Centro aggiornamenti</div> <div>🔍 Nascondi</div> <div>🗑 Elimina</div>									
<input checked="" type="checkbox"/>	Stato	Nome dispositivo Codice prodotto	Punto finale servizio Codice di serie	Versione... firmware...	Versione...	Modal...	Aggiorna info centro	Estensioni	Azioni
Gruppo predefinito del dispositivo (2)									
<input checked="" type="checkbox"/>	<div><div></div><div></div></div>	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64767000N	3.5IE94804	-	-	-	-	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
<input checked="" type="checkbox"/>	<div><div></div><div></div></div>	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44716401Y	2.6IE94813	-	STOP	-	Estensioni	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>

Se supportato dal dispositivo, il collegamento **Estensioni** ([Estensioni](#)) apre una nuova scheda **Estensioni** e fornisce i dispositivi modulari raggruppati per **estensione**.


PACCHETTO DATI		DISPOSITIVO / CARICAMENTO		ESTENSIONI		
ATV630EIP						
ATV630EIP		mbap://172.20.170.209:502		Versione firmware: 2.6IE94813		
CR: ATV630U07M3		SN: 4004000HL44716401Y		  Centro aggiornamenti		
0						
Stato	Nome dispositivo Codice prodotto	Punto finale servizio Numero di serie	Versione firmware	Aggiorna info centro		Azioni
<input type="checkbox"/>	 Ethernet/IP ModbusTCP module CR: VW3A3721	1 SN:	1.8IE13802			 

Entrambe le schede forniscono accesso alla finestra di dialogo **Centro aggiornamenti** (tramite l'icona **Centro aggiornamenti** o il pulsante **Centro aggiornamenti** **Centro aggiornamenti**) che consente di selezionare il pacchetto dati del firmware tramite il pulsante **Firmware**.

Per i dispositivi che non possono caricare le estensioni a richiesta facendo clic sul collegamento **Estensioni**, seguire il processo descritto nella sezione successiva per accedere alle singole estensioni.


Accesso manuale alle estensioni

Per i dispositivi che non possono caricare le estensioni a richiesta facendo clic sul collegamento **Estensioni**, procedere come indicato di seguito:

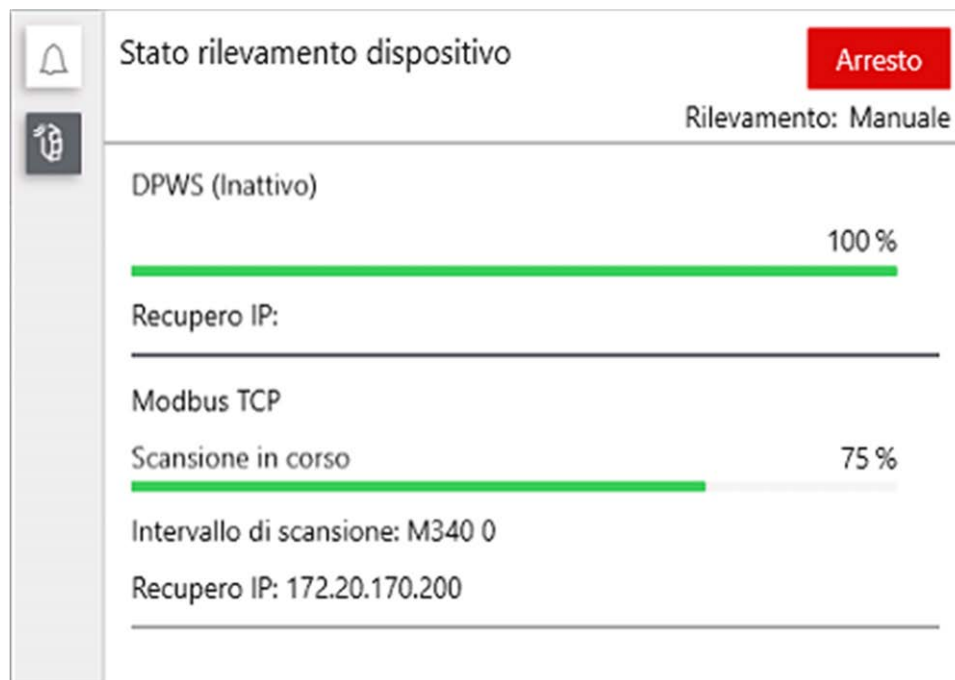
Passo	Azione
1	Fare clic sul collegamento Estensioni del dispositivo modulare. Risultato: viene visualizzata la scheda Estensioni . Se il dispositivo non è in grado di caricare le estensioni a richiesta facendo clic sul collegamento Estensioni , è disponibile un pulsante Aggiungi .
2	Fare clic sul pulsante Aggiungi o sul collegamento Nessun modulo trovato . Per aggiungere un modulo, fare clic qui. Risultato: viene visualizzata la finestra di dialogo Aggiungi modulo .
3	Nella finestra di dialogo Aggiungi modulo , configurare i parametri per accedere alle estensioni del dispositivo: <ul style="list-style-type: none"> Numero Rack Numero Slot
4	Fare clic sul pulsante OK per avviare la scansione di rilevamento. Dopo il corretto rilevamento delle estensioni, viene visualizzata la scheda Estensioni . 
5	Chiudere la scheda Estensioni .

Monitoraggio dello stato di rilevamento del dispositivo

Panoramica

Mentre è in esecuzione il processo di rilevamento dei dispositivi, è possibile recuperare lo stato su tale processo facendo clic sul pulsante  nella scheda **Dispositivo/Caricamento**.

Sul lato destro si apre la vista **Stato rilevamento dispositivo**:



Sono visualizzate le informazioni seguenti:

- Le informazioni sull'avanzamento sono fornite singolarmente per ogni scanner.
- Se sono configurati più intervalli per uno scanner, le informazioni sull'avanzamento sono fornite singolarmente per ciascun intervallo (ad esempio, per lo scanner Modbus TCP, pagina 34).

Il pulsante **Start/Stop** consente di avviare un rilevamento dispositivo manuale o di arrestare un processo di rilevamento dispositivo direttamente da questa vista.

Visualizzazione/Conferma messaggi

Panoramica

Alcuni dei processi eseguiti da EcoStruxure Automation Device Maintenance richiedono l'interazione dell'utente. Qualora sia richiesta conferma, il processo, ad esempio l'aggiornamento del firmware, viene interrotto e viene visualizzato un messaggio nell'area di notifica. Leggere attentamente ogni messaggio e confermare dopo aver valutato i rischi. Dopo aver confermato ogni messaggio, il processo continua.

Per aprire l'area di notifica, fare clic sul pulsante  nella scheda **Dispositivo/Caricamento**.

PACCHETTO DATI
DISPOSITIVO / CARICAMENTO

ELENCO DISPOSITIVI

+ Aggiungi
Connetti
Disconnetti
Centro aggiornamenti
Nascondi
Elimina

Stato	Nome dispositivo Codice prodotto	Punto finale servizio Numero di serie	Versio... firmw...	Version...	Modal...	Aggiorna info centro
Gruppo predefinito del dispositivo (10)						
<input checked="" type="checkbox"/>	BME N0C0321 CR: BME N0C0321	ftp://172.20.170.62:21 SN:	01.06 IR 2	Conferma richiesta	Firmware selezionato	
<input type="checkbox"/>	140*** CR: 140***	https://172.20.170.72:443 SN:	-	-	-	
<input type="checkbox"/>	BMEP586040 CR: BMEP586040	https://[fe80::280:f4ff:fe20:cde0]:443 SN: 21190100014	4.01.28	-	-	
<input type="checkbox"/>	ATV930U07M3_b3a CR: ATV930U07M3	mbap://172.20.170.213:502 SN: 4030000HL704004007	3.5IE94B01	-	-	
<input type="checkbox"/>	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B04	-	-	
<input type="checkbox"/>	BMED581020-test CR: BMED581020	https://[fe80::280:f4ff:fe28:4142]:443 SN: 21212711508	22.0.22152	-	-	
<input type="checkbox"/>	BME P58 2020 CR: BME P58 2020	ftp://172.20.170.60:21 SN:	02.90 IR 5	-	-	
<input type="checkbox"/>	M251D CR: TM251MDESE	https://[fe80::280:f4ff:fe0b:5470]:443 SN: PROD0006115	22.0.2215...	-	-	
<input type="checkbox"/>	ATV630U07M3 CR: ATV630U07M3	mbap://[fe80::280:f4ff:fec2:3639%1... SN: 18c23639	3.5IE94B02	-	-	
<input type="checkbox"/>	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94B02	-	-	

Area di notifica

Suggerimento per la sicurezza

BME N0C0321
ftp://172.20.170.62:21

Prima di trasferire i dati al PLC, assicurarsi di avere eseguito il collegamento al dispositivo corretto verificando l'indirizzo PLC e l'indirizzo MAC visualizzati nella scheda Firmware. Il trasferimento dati a un'apparecchiatura sbagliata può comportare interazioni a rischio con il processo.

Continuare il trasferimento dati?

Conferma
Rifiuta

Riepilogo
Aggiorna
Annulla

Nell'area di notifica possono essere visualizzati due diversi tipi di messaggi:

- Messaggi di conferma: selezionare il messaggio selezionando la casella di controllo e fare clic su **Conferma** per confermare il messaggio e riprendere l'esecuzione del processo, oppure fare clic su **Rifiuta** per interrompere il processo.
- Messaggi di notifica: selezionare il messaggio selezionando la casella di controllo e fare clic su **OK** per confermare il messaggio e riprendere l'esecuzione del processo.

L'opzione **Non mostrare notifiche** consente di disattivare la visualizzazione dei messaggi di notifica. Se questa opzione è selezionata, i processi vengono eseguiti automaticamente senza interruzioni delle interazioni dell'utente, considerando confermati i messaggi.

NOTA: attivare questa opzione solo se si lavora in modalità manutenzione e l'operatore ha verificato lo stato di sicurezza dell'ambiente della macchina o del processo.

Visualizzazione dei registri


È possibile visualizzare i registri memorizzati e analizzarli per i dettagli relativi al dispositivo selezionato.

Le informazioni del registro possono essere visualizzate nelle sezioni seguenti:

- Per ogni dispositivo nella pagina **Dispositivo/Caricamento**
- Per l'intero progetto nella finestra **Registri**

NOTA: Nella finestra **Registri**, gli errori rilevati, gli avvisi rilevati e i messaggi informativi sono visualizzati in una singola finestra.

Per visualizzare i registri esclusivi del dispositivo selezionato, procedere come segue:

Pas- so	Azione
1	Accedere alla pagina Dispositivo/Caricamento .
2	Fare clic sull'icona Registro dispositivo  di un dispositivo. Risultato: si apre una piccola vista Informazioni di registro direttamente nella tabella sotto la riga del dispositivo. Utilizzare la barra di scorrimento sul lato destro per visualizzare tutte le voci del registro, se necessario.

Per nascondere le **Informazioni di registro** per un dispositivo, fare di nuovo clic sull'icona **Registro dispositivo** .

Raccomandazione per una sicurezza informatica ottimizzata

Il file di registro in genere contiene dati riservati, quali



- indirizzi dispositivo
- nomi dispositivo
- dettagli della topologia di rete
- dettagli della configurazione di rete

Questo file è memorizzato sul disco rigido del PC. Eliminare il file di registro se non è più necessario o salvarlo in un'ubicazione sicura, in modo che non sia accessibile senza autorizzazione.

Centro aggiornamenti

Panoramica

La finestra di dialogo **Centro aggiornamenti** consente di configurare le impostazioni per l'esecuzione di un aggiornamento del firmware o di un aggiornamento del file di configurazione sicurezza. Queste impostazioni di configurazione possono essere applicate a un singolo dispositivo o a dispositivi diversi simultaneamente.

- Per eseguire aggiornamenti su un singolo dispositivo, fare clic sull'icona **Centro aggiornamenti**  nella riga dispositivo della tabella nella scheda **Dispositivo/Caricamento**.
- Per eseguire aggiornamenti simultanei per dispositivi diversi del progetto, selezionare i dispositivi nella scheda **Dispositivo/Caricamento** e fare clic sul pulsante **Centro aggiornamenti**  **Centro aggiornamenti** dalla barra dei pulsanti.

Finestra di dialogo Centro aggiornamenti

Entrambe le operazioni aprono la finestra di dialogo **Centro aggiornamenti** che consente di selezionare:

- **Firmware:** per configurare le impostazioni per l'aggiornamento del firmware del dispositivo o dei dispositivi selezionati. Per ulteriori informazioni, vedere *Aggiornamento del firmware*, pagina 69.
- **Sicurezza:** per configurare le impostazioni per l'aggiornamento del file di configurazione della sicurezza del dispositivo o dei dispositivi selezionati. Per ulteriori informazioni, vedere *Aggiornamento del file di configurazione sicurezza*, pagina 71.
- **Reset:** per ripristinare le impostazioni di aggiornamento per il dispositivo o i dispositivi selezionati.

Per confermare le impostazioni e chiudere la finestra di dialogo **Centro aggiornamenti**, fare clic sul pulsante **Salva**. Di conseguenza, la configurazione effettuata è indicata nelle celle **Aggiorna info centro** del dispositivo o dei dispositivi nella scheda **Dispositivo/Caricamento**, pagina 21.

Per eseguire il processo di aggiornamento come configurato, fare clic sul pulsante **Aggiorna**.

Aggiornamento del firmware

Panoramica

EcoStruxure Automation Device Maintenance consente di aggiornare il firmware dei dispositivi visualizzati nella scheda **Dispositivo/Caricamento**.



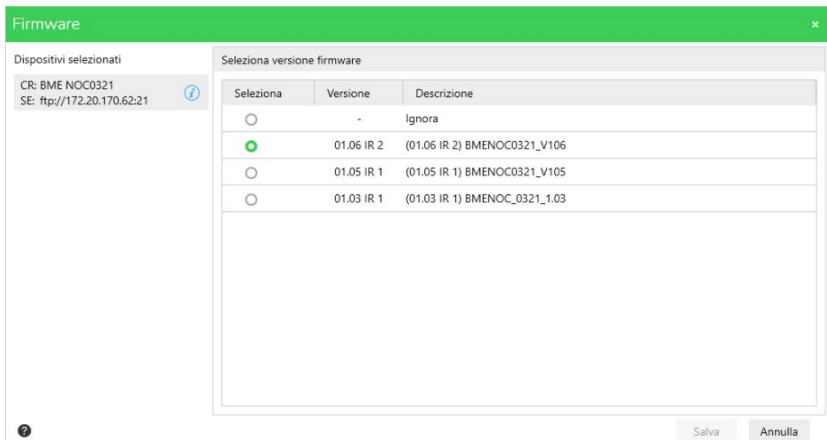
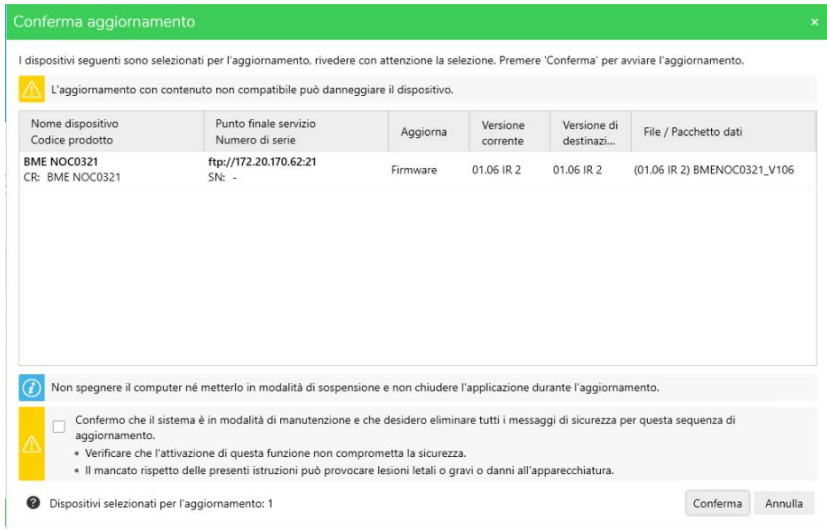
Per aggiornare il firmware dei dispositivi modulari, è possibile accedere alle singole estensioni come descritto nel capitolo *Accesso alle estensioni*, pagina 64.

È possibile selezionare pacchetti dati per più estensioni e/o moduli del rack. EcoStruxure Automation Device Maintenance aggiorna contemporaneamente il firmware di tali dispositivi.

NOTA: Se si esegue un aggiornamento simultaneo per il controller e i moduli, assicurarsi di non riavviare il controller mentre l'aggiornamento dei moduli è ancora in esecuzione. Vedere di seguito un importante messaggio di pericolo.

Aggiornamento del firmware

Per aggiornare il firmware, procedere come segue:

Passo	Azione
1	Accedere alla pagina Dispositivo/Caricamento .
2a	Per eseguire aggiornamenti su un singolo dispositivo, fare clic sull'icona Centro aggiornamenti  nella riga del dispositivo.
2b	Per eseguire contemporaneamente aggiornamenti per diversi dispositivi del progetto, selezionare le caselle di controllo dei dispositivi o selezionare la casella di controllo dell'intero Gruppo e fare clic sul pulsante Centro aggiornamenti  Centro aggiornamenti nella barra dei pulsanti.
3	Nella finestra di dialogo Centro aggiornamenti fare clic sul pulsante Firmware .
4	Nella finestra di dialogo Firmware , selezionare il pacchetto di dati del firmware per ogni dispositivo. 
5	Fare clic su Salva per salvare la configurazione dell'aggiornamento firmware e chiudere la finestra di dialogo Firmware . Risultato: la cella o le celle Aggiorna info centro del dispositivo o dei dispositivi nella scheda Dispositivo/Caricamento , pagina 21 visualizza(no) il testo Firmware selezionato .
6	Fare clic sul pulsante Aggiorna nella scheda Dispositivo/Caricamento per avviare il processo di aggiornamento. Risultato: viene visualizzata la finestra di dialogo Conferma aggiornamento . 
7	Nella finestra di dialogo Conferma aggiornamento , rivedere attentamente l'elenco dei dispositivi selezionati per l'aggiornamento e verificare le impostazioni effettuate.

Passo	Azione
8	Fare clic sul pulsante Conferma per avviare il processo di aggiornamento. Risultato: viene avviato il processo di aggiornamento del firmware. Qualora fosse richiesta l'interazione dell'utente, il processo viene interrotto e nell'area di notifica, pagina 67 viene visualizzato un messaggio. Leggere attentamente ogni messaggio e confermare dopo aver valutato i rischi. Dopo aver confermato ogni messaggio, il processo continua.
9	Una volta completato il processo del firmware, fare clic sul pulsante di Riepilogo , pagina 19 nella parte inferiore di EcoStruxure Automation Device Maintenance per visualizzare la finestra di dialogo di Riepilogo aggiornamento . Fornisce informazioni sullo stato dell'aggiornamento per ogni dispositivo che indica la versione precedente e quella di destinazione, nonché il pacchetto dati/file.

AVVISO

DISPOSITIVI DANNEGGIATI

Non spegnere il PC o chiudere l'applicazione e assicurarsi che il PC non entri in modalità di sospensione mentre è in esecuzione il processo di aggiornamento del firmware poiché l'interruzione del processo può danneggiare il dispositivo.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Se si desidera, è possibile selezionare la casella di controllo **Confermo che il sistema è in modalità manutenzione e che desidero eliminare tutti i messaggi di sicurezza per questa sequenza di aggiornamento..** In questo modo si evita la sospensione del processo.

NOTA: attivare questa opzione solo se si lavora in modalità manutenzione e l'operatore ha verificato lo stato di sicurezza dell'ambiente della macchina o del processo.

Dopo aver completato il processo del firmware, per i controller è possibile fare clic sull'icona **Avvia dispositivo** nella scheda **Dispositivo/Caricamento**, pagina 21 per avviare il dispositivo.

NOTA: Eseguire un test di avviamento prima di utilizzare regolarmente le apparecchiature di automazione e controllo elettrico dopo l'installazione o l'aggiornamento. Per ulteriori informazioni, vedere **Avviamento e verifica**, pagina 7.

Aggiornamento del file di configurazione sicurezza



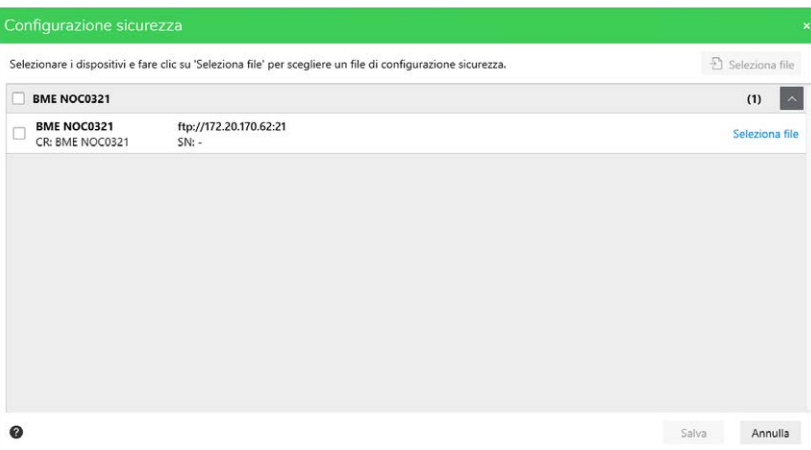
Panoramica

EcoStruxure Automation Device Maintenance consente di aggiornare il file di configurazione sicurezza contenente le impostazioni di configurazione di sicurezza configurate globalmente per la rete nell'applicazione EcoStruxure Cybersecurity Admin Expert.

NOTA: Il nuovo file di configurazione sicurezza può assegnare nuove credenziali al dispositivo o ai dispositivi. Per gli accessi futuri, saranno richieste le nuove credenziali.

Aggiornamento del file di configurazione sicurezza

Per aggiornare il file di configurazione sicurezza, procedere come segue:

Passo	Azione
1	Accedere alla pagina Dispositivo/Caricamento .
2a	Per eseguire aggiornamenti su un singolo dispositivo, fare clic sull'icona Centro aggiornamenti  nella riga del dispositivo.
2b	Per eseguire contemporaneamente aggiornamenti per diversi dispositivi del progetto, selezionare le caselle di controllo dei dispositivi o selezionare la casella di controllo dell'intero Gruppo e fare clic sul pulsante Centro aggiornamenti  Centro aggiornamenti nella barra dei pulsanti.
3	Nella finestra di dialogo del Centro aggiornamenti , fare clic sul pulsante Sicurezza .
4	<p>Nella finestra di dialogo Configurazione sicurezza, selezionare un singolo dispositivo e fare clic sul collegamento Seleziona file per questo dispositivo o selezionare più dispositivi e fare clic sul pulsante Seleziona file nella parte superiore della finestra di dialogo.</p>  <p>Risultato: viene visualizzata una finestra di dialogo di apertura file di Windows che consente di cercare il file di configurazione sicurezza nella rete.</p>
5	<p>Selezionare il file di configurazione sicurezza e fare clic sul pulsante Apri.</p> <p>Risultato: la finestra di dialogo Configurazione sicurezza visualizza i dispositivi con i file selezionati.</p>
6	<p>Fare clic sul pulsante Salva per salvare la configurazione e chiudere la finestra di dialogo Configurazione sicurezza.</p> <p>Risultato: la cella o le celle Aggiorna info centro del dispositivo o dei dispositivi nella scheda Dispositivo/Caricamento, pagina 21 visualizza(no) il testo Configurazione sicurezza selezionata.</p>
7	<p>Fare clic sul pulsante Aggiorna nella scheda Dispositivo/Caricamento per avviare il processo di aggiornamento.</p> <p>Risultato: viene visualizzata la finestra di dialogo Conferma aggiornamento.</p>
8	Nella finestra di dialogo Conferma aggiornamento , rivedere attentamente l'elenco dei dispositivi selezionati per l'aggiornamento e verificare le impostazioni effettuate.
9	<p>Fare clic sul pulsante Conferma per avviare il processo di aggiornamento.</p> <p>Risultato: viene avviato il processo di aggiornamento. Qualora fosse richiesta l'interazione dell'utente, il processo viene interrotto e nell'area di notifica, pagina 67 viene visualizzato un messaggio. Leggere attentamente ogni messaggio e confermare dopo aver valutato i rischi. Dopo aver confermato ogni messaggio, il processo continua.</p>

AVVISO

DISPOSITIVI DANNEGGIATI

Non spegnere il PC o chiudere l'applicazione e assicurarsi che il PC non entri in modalità di sospensione mentre è in esecuzione il processo di aggiornamento del firmware poiché l'interruzione del processo può danneggiare il dispositivo.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Se si desidera, è possibile selezionare la casella di controllo **Confermo che il sistema è in modalità manutenzione e che desidero eliminare tutti i messaggi di sicurezza per questa sequenza di aggiornamento..** In questo modo si evita la sospensione del processo.

NOTA: attivare questa opzione solo se si lavora in modalità manutenzione e l'operatore ha verificato lo stato di sicurezza dell'ambiente della macchina o del processo.

Sicurezza informatica

Introduzione

La Cybersecurity è un ramo dell'amministrazione di rete che si occupa degli attacchi indirizzati a o provenienti da computer e da reti informatiche dai quali possono derivare interruzioni accidentali o intenzionali del servizio. L'obiettivo della cybersecurity è quello di contribuire ad aumentare i livelli di protezione delle informazioni e delle risorse fisiche da furti, danneggiamento, uso improprio o altri pregiudizi, mantenendole al contempo accessibili agli utenti che le devono utilizzare.

Non esiste un unico approccio per affrontare il problema della sicurezza informatica. Schneider Electric raccomanda di adottare un approccio del tipo Defense-in-Depth. Tale approccio, concepito dalla National Security Agency (NSA), suddivide la rete in più livelli distinti per funzioni di sicurezza, apparecchiature e processi. I componenti di base di questo approccio sono:

- valutazione dei rischi
- un piano di sicurezza elaborato sulla base dei risultati della valutazione dei rischi
- una campagna di formazione multifase
- separazione fisica delle reti industriali dalle reti aziendali, con la creazione di una zona demilitarizzata (DMZ) e con l'uso di firewall e instradamento per delimitare altre zone di sicurezza
- controllo degli accessi al sistema
- riduzione delle vulnerabilità dei dispositivi ("hardening")
- monitoraggio e manutenzione delle reti

Questo capitolo definisce gli elementi che consentono di configurare un sistema meno sensibile agli attacchi informatici. Per informazioni dettagliate sull'approccio di difesa in profondità, fare riferimento alla *nota tecnica del sistema: Come... Ridurre la vulnerabilità agli attacchi informatici* sul sito [Schneider Electric website](#).

Definizione della sicurezza informatica

Panoramica

Le cyberminacce, o minacce informatiche, sono azioni deliberate o eventi avversi che possono interrompere il normale funzionamento di computer e reti informatiche. Tali azioni possono essere avviate all'interno di una struttura fisica o provenire da una posizione esterna. Le esigenze di sicurezza per l'ambiente di controllo includono:

- limiti fisici e logici separati
- più siti e ampie distanze geografiche
- conseguenze negative dell'implementazione della sicurezza sulla disponibilità dei processi
- maggiore esposizione a worm e virus che migrano dai sistemi aziendali ai sistemi di controllo quando le comunicazioni di controllo aziendale diventano più aperte
- maggiore esposizione a software dannoso proveniente da dispositivi USB, laptop di fornitori e tecnici dell'assistenza e rete aziendale
- impatto diretto dei sistemi di controllo su apparecchiature fisiche e meccaniche

Origine dei cyberattacchi

Implementare un piano di sicurezza informatica che tenga conto delle diverse possibili origini dei cyberattacchi e degli eventi avversi, inclusi:

Origine	Descrizione
interna	<ul style="list-style-type: none">• comportamento inappropriato di dipendenti o fornitori• dipendente o fornitore scontento
esterno opportunistico (indiretto)	<ul style="list-style-type: none">• script kiddie*• hacker "ricreativi"• scrittori di virus
esterno deliberato (diretto)	<ul style="list-style-type: none">• gruppi criminali• attivisti• terroristi• agenzie di stati esteri
accidentale	
* termine dello slang usato per descrivere gli hacker che utilizzano script dannosi scritti da altri senza comprendere esattamente il funzionamento dello script o il suo potenziale impatto su un sistema	

Un cyberattacco deliberatamente lanciato su un sistema di controllo può essere motivato dall'intento di causare una serie di conseguenze dannose, inclusi:

- interruzione del processo di produzione con il blocco o il ritardo del flusso di informazioni
- danno, disattivazione o spegnimento di apparecchiature per influire negativamente sulla produzione o sull'ambiente
- modifica o disattivazione di sistemi di sicurezza per causare intenzionalmente un danno

Metodi di accesso degli autori degli attacchi

L'autore di un cyberattacco aggira le difese adottate per ottenere accesso alla rete del sistema di controllo. I punti di accesso comuni includono:

- accesso remoto ai dispositivi di un'unità terminale remota (RTU)
- punti di accesso del fornitore (come i punti di accesso dell'assistenza tecnica)
- prodotti di rete con controllo IT
- rete privata virtuale aziendale (VPN)
- collegamenti a database
- firewall configurati in modo non corretto
- utility "peer"

Certificazioni di cybersecurity

Schneider Electric ha sviluppato delle linee guida per la sicurezza informatica sulla base delle seguenti raccomandazioni:

- Achilles
- ISA Secure

Per domande, notizie o segnalazione di problemi di vulnerabilità

Per inviare una domanda sulla sicurezza informatica, ricevere le ultime notizie da Schneider Electric o segnalare problemi di vulnerabilità, visitare il nostro [website](#).

Linee guida Schneider Electric

Introduzione

Il sistema del PC può eseguire una serie di applicazioni per aumentare la sicurezza dell'ambiente di controllo. Il sistema è dotato di impostazioni predefinite che richiedono la riconfigurazione per l'allineamento alle raccomandazioni sull'hardening dei dispositivi Schneider Electric dell'approccio di difesa in profondità (Defense-in-Depth, DiD).

Le seguenti linee guida descrivono le procedure in un sistema operativo Windows. Sono fornite solo a titolo esemplificativo. Ogni sistema operativo e applicazione può avere requisiti o procedure diverse.

Rafforzamento delle workstation di ingegnerizzazione

Gli utenti possono scegliere tra vari sistemi PC commerciali per costruire le workstation di progettazione necessarie. Le tecniche fondamentali di rafforzamento includono:

- Gestione di password significative.
- Gestione degli account utenti.
- Metodi di privilegi limitati applicati alle applicazioni e agli account utenti.
- Rimozione o disattivazione di servizi non necessari.
- Rimozione dei privilegi di gestione remota.
- Gestione dei patch sistematica.

Disabilitazione delle schede di interfaccia di rete non utilizzate

Verificare che le schede dell'interfaccia di rete non richieste dall'applicazione siano disattivate. Ad esempio, se il sistema è dotato di 2 schede e l'applicazione ne utilizza solo una, verificare che l'altra scheda di rete (connessione alla rete locale, LAN 2) sia disattivata.

Per disattivare una scheda di rete in Windows:

Passo	Azione
1	Selezionare Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione > Modifica impostazioni scheda .
2	Fare clic con il pulsante destro del mouse sulla connessione non utilizzata. Selezionare Disabilita .

Configurazione della connessione alla rete locale

Diverse impostazioni di rete Windows forniscono un miglioramento della sicurezza in linea con l'approccio di difesa in profondità (DiD) raccomandato da Schneider Electric.

Nei sistemi Windows, accedere a queste impostazioni selezionando **Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione > Modifica impostazioni scheda > Connessione alla rete locale (x)**.

Questo elenco è un esempio delle modifiche alla configurazione che possono essere apportate nel sistema dalla schermata **Proprietà connessione alla rete locale (LAN)**:

- Disattivare tutti gli stack IPv6 sulle rispettive schede di rete (questo esempio di sistema non richiede l'intervallo di indirizzi IPv6 e la disattivazione degli stack IPv6 limita la vulnerabilità a potenziali rischi di sicurezza IPv6).
- Disabilitare **Condivisione di file e stampanti per rete Microsoft**.

Le raccomandazioni di Schneider Electric per una difesa in profondità includono anche quanto segue:

- Definire solo indirizzi IPv4, maschere di sottorete e gateway statici.
- Non utilizzare DHCP o DNS nella sala di controllo.

Gestione di Windows Firewall

Le raccomandazioni dell'approccio di difesa in profondità (Defense-in-Depth, DiD) di Schneider Electric comprendono l'abilitazione di Windows host firewall su tutti i PC dei sistemi. Abilita i firewall per qualsiasi profilo pubblico o privato indicato.

È consigliabile che gli utenti definiscano le regole dei firewall che rifiutano le connessioni dirette o provenienti da qualunque host esterno sconosciuto/non affidabile.

Disabilitazione di Remote Desktop Protocol

Le raccomandazioni relative all'approccio di difesa in profondità di Schneider Electric includono la disabilitazione del protocollo RDP (Remote Desktop Protocol) a meno che l'applicazione non richieda RDP.

Per disabilitare il protocollo per i sistemi Windows 10, procedere come segue:

Passo	Azione
1	Fare clic con il pulsante destro del mouse sul pulsante Start di Windows ed eseguire il comando Sistema .
2	Dal menu Impostazioni , eseguire il comando Desktop remoto .
3	Nella vista Desktop remoto , disattivare Attiva desktop remoto (commutare su Disattivato).

Per altri sistemi operativi Windows, eseguire procedure equivalenti.

Aggiornamento dei criteri di sicurezza

Aggiornare i criteri di sicurezza sui PC del sistema da `gpupdate` in una finestra di comando. Per maggiori informazioni, vedere la documentazione di Microsoft su `gpupdate`.

Disabilitazione di LANMAN e NTLM

Il protocollo Microsoft LAN Manager (LANMAN o LM) e il suo successore NT LAN Manager (NTLM) presentano delle vulnerabilità che ne sconsigliano l'utilizzo nelle applicazioni di controllo.

La seguente procedura illustra come disabilitare LM e NTLM in un sistema Windows:

Passo	Azione
1	In una finestra di comando, eseguire <code>secpol.msc</code> per aprire la finestra Criteri di sicurezza locali .
2	Aprire Impostazioni di protezione > Criteri locali > Opzioni di sicurezza .
3	Selezionare Invia solo risposta NTLMv2. Rifiuta LM e NTLM nel campo Sicurezza di rete: livello di autenticazione di LAN Manager .
4	Selezionare la casella di controllo Sicurezza di rete: non memorizzare il valore hash di LAN Manager al prossimo cambio di password .
5	In una finestra di comando, immettere <code>gpupdate</code> per confermare il criterio di sicurezza modificato.

Gestione degli aggiornamenti

Prima della distribuzione, aggiornare tutti i sistemi operativi del PC utilizzando le utility nella pagina Web **Windows Update** di Microsoft. Per accedere a questo strumento in Windows, selezionare **Start > Tutti i programmi > Windows Update**.

Verifica della firma digitale

Verifica dell'integrità di EcoStruxure Automation Device Maintenance dopo il download

Dopo aver scaricato il file eseguibile EcoStruxure Automation Device Maintenance dal sito Web Schneider Electric, verificare l'integrità del file eseguendo la procedura indicata:

Passo	Azione
1	Fare clic con il pulsante destro del mouse sul file <code>AutomationDeviceMaintenance.exe</code> ed eseguire il comando Proprietà dal menu contestuale.
2	Nella finestra di dialogo AutomationDeviceMaintenance.exe Properties , selezionare la scheda Firme digitali .
3	Dall' elenco firme , selezionare la voce Schneider Electric USA, INC. e fare clic sul pulsante Dettagli per visualizzare Dettagli firma digitale .
4	Nella finestra di dialogo Dettagli firma digitale , verificare che siano visualizzate le informazioni La firma digitale è valida .

È ora possibile fare doppio clic sul file .exe per avviare EcoStruxure Automation Device Maintenance.

Verifica dei componenti durante l'avvio

Quando EcoStruxure Automation Device Maintenance è avviato, ciascuna DLL (Dynamic Link Library) caricata viene analizzata per verificare se sia attendibile o

meno. Si tratta di una funzionalità di sicurezza integrata contro gli attacchi informatici e per aumentare il livello di attendibilità.

Operazioni da eseguire se vengono rilevati componenti non attendibili

Se vengono rilevati componenti non attendibili, l'avvio di EcoStruxure Automation Device Maintenance viene interrotto e visualizzato un messaggio che indica che è stata rilevata un'eccezione.

In questo caso, sono disponibili le opzioni seguenti:

- Reinstallare EcoStruxure Automation Device Maintenance.
- Nel caso si sospetti che il problema sia stato causato da un attacco informatico, consultare il [Schneider Electric Cybersecurity services portal](#) per ulteriori consigli o assistenza.

Per trovare il componente che provoca il problema, è possibile utilizzare un tool di debug, ad esempio WinDbg: Avviare il tool di debug, avviare EcoStruxure Automation Device Maintenance e osservare il contenuto del file di registro per le voci che indicano che non è possibile determinare la validità della firma del codice di una DLL.

File che richiedono la disinstallazione manuale

Panoramica

Quando si disinstalla EcoStruxure Automation Device Maintenance dal PC, i file di programma vengono rimossi automaticamente, ma vi sono alcuni file specifici dell'utente che occorre gestire individualmente per evitare problemi di sicurezza informatica.

File di impostazioni EcoStruxure Automation Device Maintenance

Il file di impostazioni EcoStruxure Automation Device Maintenance *AutomationDeviceMaintenanceSettings.emes* viene creato da EcoStruxure Automation Device Maintenance per memorizzare la configurazione eseguita nella finestra di dialogo **Impostazioni** (ad esempio, intervalli di scansione Modbus TCP o impostazioni di rilevamento). Non viene rimosso dal PC con la disinstallazione di EcoStruxure Automation Device Maintenance ma deve essere rimosso manualmente.

Rimuoverlo dalla cartella *%APPDATA%\Schneider Electric\Automation Device Maintenance* utilizzando Esplora risorse di Windows o altri strumenti del file system.

Certificati

Il certificato di EcoStruxure Automation Device Maintenance e i **Certificati attendibili** e **Certificati non attendibili** gestiti nella finestra di dialogo **Impostazioni** in **Sicurezza > Gestione certificato** (vedere anche **Finestra di dialogo Gestione certificato**, pagina 44) vengono rimossi dal PC Windows con la disinstallazione di EcoStruxure Automation Device Maintenance. Vengono anche rimossi dall'Archivio certificati di Windows.

Pacchetti di dati

I pacchetti di dati, pagina 20 salvati localmente non vengono rimossi dal PC con la disinstallazione di EcoStruxure Automation Device Maintenance. Per impostazione predefinita, i pacchetti di dati vengono memorizzati nella cartella %PUBLIC%\Public Documents\Schneider Electric\Data Packages. È possibile configurare il percorso individuale nella finestra di dialogo **Impostazioni > Impostazioni pacchetto**, pagina 37.

Rimuovere manualmente la cartella predefinita o configurata utilizzando Esplora risorse di Windows o altri strumenti del file system.

File di progetto di EcoStruxure Automation Device Maintenance

I file di progetto di EcoStruxure Automation Device Maintenance non vengono rimossi dal PC con la disinstallazione di EcoStruxure Automation Device Maintenance. Cercare i file con estensione *.emep e rimuoverli manualmente o memorizzarli per un successivo utilizzo in un'ubicazione sicura dove non sia possibile l'accesso non autorizzato.

File di registro

I file di registro salvati localmente nel percorso specificato nella finestra di dialogo **Impostazioni > Registri**, pagina 38 non vengono rimossi dal PC con la disinstallazione di EcoStruxure Automation Device Maintenance. Rimuovere manualmente la cartella utilizzando Esplora risorse di Windows o altri strumenti del file system, oppure memorizzare i file di registro per un successivo utilizzo in un'ubicazione sicura in cui non sia possibile l'accesso non autorizzato.



Componenti utilizzati da EcoStruxure Automation Device Maintenance

Panoramica

EcoStruxure Automation Device Maintenance fornisce una panoramica dei componenti e delle versioni attuali. Se viene rilevata un'eccezione, questo elenco di componenti e versioni consente di individuare il componente che potrebbe essere la causa.

Recupero di un elenco di componenti

Per recuperare un elenco dei componenti caricati da EcoStruxure Automation Device Maintenance, procedere come segue:

Passo	Azione																																	
1	<p>Fare clic sul pulsante Informazioni  sulla barra degli strumenti.</p> <p>Risultato: viene visualizzata la finestra di dialogo Informazioni.</p>																																	
2	<p>Fare clic sul collegamento Informazioni componente.</p> <p>Risultato: viene visualizzata la finestra di dialogo Informazioni componente.</p> <div><div>Informazioni su</div><div><div>Informazioni componente</div><table><thead><tr><th>Nome componente</th><th>Versione</th><th>Descrizione</th></tr></thead><tbody><tr><td>AutomationDeviceMaintenance</td><td>3.0.154.0</td><td>General</td></tr><tr><td>BrandIdentity</td><td>4.19.0.2175</td><td>General</td></tr><tr><td>ServiceCommon</td><td>3.1.3.0</td><td>General</td></tr><tr><td>log4net</td><td>2.0.11.0</td><td>General</td></tr><tr><td>PackageCommon</td><td>3.0.4.0</td><td>General</td></tr><tr><td>Org.Schneider.FWChecker</td><td>2.5.2.0</td><td>General</td></tr><tr><td>Org.Schneider.Crypto</td><td>2.5.2.0</td><td>General</td></tr><tr><td>Asn1Parser</td><td>2.5.2.0</td><td>General</td></tr><tr><td>SE.CS.PKI.Common</td><td>1.0.6.0</td><td>General</td></tr><tr><td>PackageDescriptionLibrary</td><td>3.1.1.0</td><td>General</td></tr></tbody></table><div>Torna a Informazioni su Copia dettagli</div><div><div>Life Is On</div><div></div></div><div>OK</div></div></div>	Nome componente	Versione	Descrizione	AutomationDeviceMaintenance	3.0.154.0	General	BrandIdentity	4.19.0.2175	General	ServiceCommon	3.1.3.0	General	log4net	2.0.11.0	General	PackageCommon	3.0.4.0	General	Org.Schneider.FWChecker	2.5.2.0	General	Org.Schneider.Crypto	2.5.2.0	General	Asn1Parser	2.5.2.0	General	SE.CS.PKI.Common	1.0.6.0	General	PackageDescriptionLibrary	3.1.1.0	General
Nome componente	Versione	Descrizione																																
AutomationDeviceMaintenance	3.0.154.0	General																																
BrandIdentity	4.19.0.2175	General																																
ServiceCommon	3.1.3.0	General																																
log4net	2.0.11.0	General																																
PackageCommon	3.0.4.0	General																																
Org.Schneider.FWChecker	2.5.2.0	General																																
Org.Schneider.Crypto	2.5.2.0	General																																
Asn1Parser	2.5.2.0	General																																
SE.CS.PKI.Common	1.0.6.0	General																																
PackageDescriptionLibrary	3.1.1.0	General																																
3	<p>Fare clic sul collegamento Copia dettagli per copiare l'elenco dei componenti e delle versioni negli Appunti.</p> <p>È ora possibile incollare il contenuto in un file *.txt che consente di eseguire operazioni di ricerca per componenti specifici e versioni corrispondenti.</p>																																	

Glossario

C

Certificato del dispositivo:

Un certificato a chiave pubblica X.509 utilizzato dal tool e dal dispositivo per stabilire un canale di comunicazione sicuro (ad esempio: HTTPs).

D

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DPWS:

Device Profile for Web Services, uno standard per il rilevamento e la descrizione di dispositivi che supportano i servizi web.

F

Famiglia di dispositivi:

Un gruppo di dispositivi di tipo simile; ogni famiglia di dispositivi è identificata da un ID prodotto.

H

HTTP:

Hypertext Transfer Protocol

HTTPs:

Hypertext Transfer Protocol Secure, noto anche come HTTP over TLS.

I

ICS: Industrial Control and Systems (Sistemi e controllo industriale)

ID prodotto:

Identificativo del prodotto; identifica la famiglia di dispositivi alla quale appartiene un dispositivo.

IEC:

L'*IEC (International Electrotechnical Commission)* è un'organizzazione internazionale non governativa senza scopo di lucro che redige e pubblica gli standard internazionali relativi a tutte le tecnologie elettriche, elettroniche e correlate.

Indirizzo IP:

Indirizzo di un dispositivo secondo gli standard di protocollo IP. Può essere nel formato di indirizzo IPv4 o IPv6.

IP:

Internet Protocol (protocollo Internet)

ISO: Organizzazione internazionale per la standardizzazione

N

NEMA:

(*National Electrical Manufacturers Association*) è l'ente preposto alla pubblicazione degli standard relativi alle caratteristiche di cabinet elettrici di diverse classi. Gli standard NEMA si riferiscono alla resistenza contro la corrosione, alla capacità di protezione contro la pioggia e in caso di immersione, ecc. Per gli stati la cui legislazione aderisce alle normative IEC, lo standard IEC 60529 classifica il grado di tenuta dei cabinet.

O

OPC UA:

OPC Unified Architecture: OPC UA è uno standard di interoperabilità per lo scambio sicuro e affidabile dei dati nello spazio di automazione industriale. È un protocollo di comunicazione indipendente dalla piattaforma che utilizza il modello server/client. La connessione tra client e server si basa comunemente sul protocollo del livello di trasporto affidabile (TCP, Transmission Control Protocol).

Per ulteriori informazioni su OPC e in particolare OPC UA, vedere la pagina Web ufficiale di OPC Foundation su <https://opcfoundation.org>.

P

Pacchetto dati, pacchetto firmware:

Un pacchetto dati è un file utilizzato per lo scambio di contenuti tra i tool e i dispositivi. Può essere in formato SEDP. Un pacchetto dati contiene uno o più pacchetti firmware, ma può anche contenere la configurazione, applicazioni PLC, ecc.

PLC:

(*Programmable Logic Controller*) Un computer industriale utilizzato per l'automazione dei processi di produzione, industriali e altri processi elettromeccanici. I PLCs differiscono dai computer comuni poiché includono numerosi array di ingressi e uscite e rispondono a specifiche più rigorose, in particolare per quanto riguarda gli urti, le vibrazioni, la temperatura e le interferenze elettriche.

POU:

(*Program Organization Unit, unità di organizzazione dei programmi*) Una dichiarazione di variabili nel codice sorgente e il set di istruzioni corrispondente. Le POUs semplificano il riutilizzo modulare di programmi software, funzioni e blocchi funzione. Una volta dichiarate, le POUs sono reciprocamente disponibili.

R

Rilevamento dispositivi:

Rilevamento automatico di dispositivi e servizi che i dispositivi offrono in una rete informatica.

S

SEDP:

Schneider Electric Data Package, formato file standardizzato per lo scambio di contenuti tra i tool software e i dispositivi.

T

TCP:

Transmission Control Protocol (protocollo di trasmissione)

TLS:

Transport Layer Security (sicurezza a livello di trasporto)

U

UDP: User Datagram Protocol

URL:

Uniform Resource Locator (localizzatore uniforme di risorse)

Indice

A		
accesso alle estensioni	64	
aggiornamento del file di configurazione sicurezza	71	
aggiornamento firmware	69	
aggiungi dispositivo	23	
allarme		
salva, cancella	26	
Applica , pulsante	26	
applicazione modifiche	26	
AutomationDeviceMaintenanceSettings.emes, file	79	
Autorità di certificazione	43	
B		
Barra degli strumenti		
informazioni, assistenza, rilevamento	19	
C		
CA	43	
capacità	25, 61, 69	
Centro aggiornamenti	68	
certificati	43	
certificato		
convalida, attendibile, non attendibile, rimuovi	43	
Certificato applicazione	43	
certificato attendibile	43	
certificato dispositivo		
attendibile, non attendibile	21	
certificato non attendibile	43	
componenti e versioni	80	
configurazione		
comunicazione, impostazioni	37	
lingua, modifica	40	
Modbus TCP	34	
rilevamento	32	
rilevamento, Modbus, impostazione pacchetto,		
lingua, certificato	25	
scanner DPWS	36	
ubicazioni pacchetto	37	
configurazione, importazione file	34	
copia dell'identificativo	54	
csv, file per l'importazione	34	
csv, importazione file	34	
D		
dati		
firmware, configurazione	52	
disinstallazione	79	
dispositivi modulari	64	
dispositivi supportati	15	
dispositivo		
aggiornamento, opzioni di configurazione,		
credenziali	61	
dispositivo/caricamento		
nome dispositivo, stato, pacchetto dati	21	
Dispositivo/Caricamento , scheda	55	
DLL non attendibile	78	
E		
eccezione	78	
elimina certificato	43	
errore		
errore, avviso	19	
salva, cancella	26	
estensioni	64	
Estensioni , scheda	64	
F		
file di progetto con dispositivi non identificati	31	
file di progetto da un altro computer	30	
file pacchetto protetti sedps	51	
finestra di dialogo Accesso al dispositivo	61	
Finestra di dialogo Conferma aggiornamento	69	
finestra di dialogo di accesso	61	
Finestra di dialogo Firmware	69	
Finestra di dialogo Progetto modificato	27	
Finestra di dialogo Riepilogo aggiornamento	69	
firmware		
aggiornamento, dispositivo/caricamento, pacchetto		
dati	69	
versione, informazioni di aggiornamento,		
avanzamento	21	
frequenza di interrogazione	37	
funzionalità di sicurezza	41	
fwp, file pacchetto	51	
G		
Gestione certificato	43	
H		
hardware		
CPU, RAM, HDD	16	
HTTP / HTTPS, comunicazione	23	
I		
icona di aggiornamento	26	
identificativo		
copia	54	
Importa file di configurazione di sicurezza	41	
importazione di un file di configurazione	34	
informazioni		
pacchetto, prodotto	52	
salva, cancella	26	
informazioni sui componenti	80	
Infrastruttura a chiave pubblica (PKI)	48	
installazione		
procedura, installazione guidata, installazione,		
contratto di licenza	17	
interrogazione, frequenza	37	
L		
Idx, file pacchetto	51	
login per l'aggiornamento del firmware	69	
M		
messaggi di conferma	67	
messaggi di notifica	67	
Modbus TCP		
ID unità, timeout ping, porta	34	
Modbus TCP, comunicazione	23	

modifiche nella pagina Impostazioni	26	sicurezza informatica (cybersecurity)	74
moduli rack	64	certificazioni	74
monitoraggio dello stato di rilevamento del dispositivo	66	connessione alla rete locale	77
		firewall	77
N		Introduzione	74
non attendibile, DLL	78	LANMAN/NTLM	78
notifica, area	67	linee guida	76
nuovo progetto	27	remote desktop	77
		schede di interfaccia di rete	76
O		sicurezza, file di configurazione	41, 71
Ok, pulsante	26	software	
Opzione Gruppo	56	funzionalità, pacchetti firmware supportati	15
		Stato rilevamento dispositivo	66
P		syslog	49
Pacchetti dati rifiutati	52		
Pacchetti dati validi	52	T	
pacchetto dati	51	TCP	49
nome pacchetto, informazioni pacchetto	20	timeout	
pacchetto firmware		comunicazione, impostazioni	37
informazioni pacchetto, nome pacchetto	18	TLS	49
password	61, 69		
PKI	48	U	
progetto		ubicazione pacchetto	
apri, salva	19	aggiungere	38
aprire	29	UDP	49
nuovo	27		
salvare	28	V	
protocolli di comunicazione	16	vista	21
Pulsante Copia negli Appunti	54		
R			
raggruppamento dispositivi	56		
registrare certificato applicazione	43		
registri			
vista	68		
Repository locale	37		
requisiti di sistema			
hardware, software, protocolli di comunicazione, risoluzione dello schermo, sicurezza informatica	16		
rilevamento			
automatico, manuale	32		
manuale, automatico	25		
rilevamento dispositivi			
Modbus, DPWS (device profile for web services)	15		
rimozione file	79		
rimuovi certificato	43		
Ripristino impostazioni applicazione	40		
S			
scanner DPWS			
richiesta probe, richiesta metadati, schede di rete	36		
Scheda di memoria SD	21		
schermata di benvenuto			
pacchetto dati, dispositivo/caricamento, barra degli strumenti	18		
sedp, file pacchetto	51		
sedps, file pacchetto	51		

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 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.

© 2022 Schneider Electric. Tutti i diritti sono riservati.

EIO0000004049.04