

EcoStruxure Automation Device Maintenance

Firmware Upgrade Tool

Online-Hilfe

EIO0000004046.04
11/2022

Rechtliche Hinweise

Die Marke Schneider Electric sowie alle anderen in diesem Handbuch enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein. Dieses Handbuch und seine Inhalte sind durch geltende Urheberrechtsgesetze geschützt und werden ausschließlich zu Informationszwecken bereitgestellt. Ohne die vorherige schriftliche Genehmigung von Schneider Electric darf kein Teil dieses Handbuchs in irgendeiner Form oder auf irgendeine Weise (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen oder anderweitig) zu irgendeinem Zweck vervielfältigt oder übertragen werden.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Handbuchs oder seiner Inhalte, ausgenommen der nicht exklusiven und persönlichen Lizenz, die Website und ihre Inhalte in ihrer aktuellen Form zurate zu ziehen.

Produkte und Geräte von Schneider Electric dürfen nur von Fachpersonal installiert, betrieben, instand gesetzt und gewartet werden.

Da sich Standards, Spezifikationen und Konstruktionen von Zeit zu Zeit ändern, können die in diesem Handbuch enthaltenen Informationen ohne vorherige Ankündigung geändert werden.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der Verwendung der hierin enthaltenen Informationen entstehen.

Als verantwortungsbewusstes und offenes Unternehmen aktualisieren wir unsere Inhalte, die nicht-inklusive Terminologie enthalten. Bis dieser Vorgang abgeschlossen ist, können unsere Inhalte allerdings nach wie vor standardisierte Branchenbegriffe enthalten, die von unseren Kunden als unangemessen betrachtet werden.

© 2022 – Schneider Electric. Alle Rechte vorbehalten.

Inhaltsverzeichnis

Sicherheitshinweise.....	5
Qualifikation des Personals	5
Sachgerechte Verwendung	6
Bevor Sie beginnen	6
Start und Test.....	7
Betrieb und Einstellungen	8
Sicherheitsanweisungen	8
Über das Handbuch.....	10
Einführung.....	15
Überblick	15
Systemanforderungen	16
Installation	17
Erste Schritte	18
Willkommen-Fenster.....	18
EcoStruxure Automation Device Maintenance -	
Benutzeroberfläche	20
Datenpaket	20
Geräte/Ladevorgang.....	21
Hinzufügen von Geräten	23
Konfiguration der Einstellungen	25
Fenster der Fehler und Warnmeldungen	26
Erstellung eines neuen Projekts von EcoStruxure Automation Device	
Maintenance	27
Speichern eines Projekts.....	28
Öffnen eines Projekts.....	29
Konfiguration des EcoStruxure Automation Device	
Maintenance-Tools	32
Konfiguration des Geräteerkennungsmodus	32
Konfiguration des Modbus TCP-Scanners	34
Konfiguration des DPWS-Scanners	36
Konfiguration der Kommunikationseinstellungen	37
Konfiguration der Speicherorte für Pakete	37
Anzeigen der Protokolldateien	38
Konfigurieren der Sprache.....	40
Zurücksetzen von Anwendungseinstellungen	40
Konfiguration von Sicherheitsfunktionen.....	41
Sicherheitsfunktionen	41
Verwaltung der Zertifikate.....	43
Verwalten der Public Key-Infrastruktur (PKI)	48
Aktivierung der Syslog-Meldungsprotokollierung	49
Datenpaket.....	51
Registerkarte „Datenpaket“	51
Gerät/Laden.....	55
Registerkarte Geräte/Ladevorgang	55
Gruppierung von Geräten in der GERÄTELISTE.....	56
Entfernen eines Geräts	57

Verwaltung der Benutzeranmeldedaten	61
Zugriff auf Erweiterungen	64
Überwachen des Geräteerkennungsstatus	66
Anzeigen/Bestätigen von Meldungen	67
Anzeigen der Protokolle	68
Aktualisierungscenter	69
Aktualisierung der Firmware	70
Aktualisierung der Sicherheitskonfigurationsdatei	72
Cybersicherheit	75
Was ist Cybersicherheit?	75
Richtlinien von Schneider Electric	77
Prüfung der digitalen Signatur	79
Für eine manuelle Deinstallation erforderliche Dateien	80
Von EcoStruxure Automation Device Maintenance verwendete Komponenten.....	81
Glossar	83
Index	86

Sicherheitshinweise

Wichtige Informationen

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.



Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.



Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

GEFAHR

GEFAHR macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge hat**.

WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann**.

VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann**.

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

Bitte beachten

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Qualifikation des Personals

Eine qualifizierte Person hat die folgenden Qualifikationen:

- Fähigkeiten und Kenntnisse hinsichtlich der Konzeption und des Betriebs elektrischer Geräte und deren Installation.
- Kenntnisse und Erfahrung im Bereich industrieller Steuerungsprogrammierung.

- Sie hat eine sicherheitsbezogene Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert.

Das Fachpersonal muss in der Lage sein, potenzielle Gefahrenquellen in Verbindung mit der Parametrierung und Änderung von Parametern sowie allgemein in Verbindung mit mechanischen, elektrischen oder elektronischen Geräten zu erkennen. Alle relevanten Normen, Vorschriften und Regelungen zur industriellen Unfallverhütung müssen dem Fachpersonal bekannt sein und bei der Konzeption und Implementierung des Systems eingehalten werden.

Sachgerechte Verwendung

Bei diesem Produkt handelt es sich um eine Bibliothek, die für eine Verwendung in Verbindung mit Steuerungssystemen und großen Stator-Motorsegmenten ausschließlich zu den in der vorliegenden Dokumentation angegebenen Zwecken gemäß der Anwendung im Industriesektor vorgesehen ist.

Dabei sind stets die geltenden sicherheitsbezogenen Anweisungen, die angegebenen Bedingungen und die technischen Kenndaten zu beachten.

Führen Sie vor der Verwendung des Produkts eine Risikobeurteilung für den geplanten spezifischen Einsatz durch. Ergreifen Sie im Anschluss daran angemessene Sicherheitsmaßnahmen.

Da das Produkt als Teil eines Gesamtsystems verwendet wird, müssen Sie die Personensicherheit durch eine entsprechende Gestaltung des Gesamtsystems (zum Beispiel Maschinengestaltung) gewährleisten.

Andere Verwendungszwecke sind nicht bestimmungsgemäß und können sich als gefährlich erweisen.

Bevor Sie beginnen

Dieses Produkt nicht mit Maschinen ohne effektive Sicherheitseinrichtungen im Arbeitsraum verwenden. Das Fehlen effektiver Sicherheitseinrichtungen im Arbeitsraum einer Maschine kann schwere Verletzungen des Bedienpersonals zur Folge haben.

▲ WARNUNG
UNBEAUF SICHTIGTE GERÄTE <ul style="list-style-type: none"> • Diese Software und zugehörige Automatisierungsgeräte nicht an Maschinen verwenden, die nicht über Sicherheitseinrichtungen im Arbeitsraum verfügen. • Greifen Sie bei laufendem Betrieb nicht in das Gerät. <p>Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.</p>

Dieses Automatisierungsgerät und die zugehörige Software dienen zur Steuerung verschiedener industrieller Prozesse. Der Typ bzw. das Modell des für die jeweilige Anwendung geeigneten Automatisierungsgeräts ist von mehreren Faktoren abhängig, z. B. von der benötigten Steuerungsfunktion, der erforderlichen Schutzklasse, den Produktionsverfahren, außergewöhnlichen Bedingungen, behördlichen Vorschriften usw. Für einige Anwendungen werden möglicherweise mehrere Prozessoren benötigt, z. B. für ein Backup-/Redundanzsystem.

Nur Sie als Benutzer, Maschinenbauer oder -integrator sind mit allen Bedingungen und Faktoren vertraut, die bei der Installation, der Einrichtung, dem Betrieb und der Wartung der Maschine bzw. des Prozesses zum Tragen kommen. Demzufolge sind allein Sie in der Lage, die Automatisierungskomponenten und zugehörigen Sicherheitsvorkehrungen und Verriegelungen zu identifizieren, die

einen ordnungsgemäßen Betrieb gewährleisten. Bei der Auswahl der Automatisierungs- und Steuerungsgeräte sowie der zugehörigen Software für eine bestimmte Anwendung sind die einschlägigen örtlichen und landesspezifischen Richtlinien und Vorschriften zu beachten. Das National Safety Council's Accident Prevention Manual (Handbuch zur Unfallverhütung; in den USA landesweit anerkannt) enthält ebenfalls zahlreiche nützliche Hinweise.

Für einige Anwendungen, z. B. Verpackungsmaschinen, sind zusätzliche Vorrichtungen zum Schutz des Bedienpersonals wie beispielsweise Sicherheitseinrichtungen im Arbeitsraum erforderlich. Diese Vorrichtungen werden benötigt, wenn das Bedienpersonal mit den Händen oder anderen Körperteilen in den Quetschbereich oder andere Gefahrenbereiche gelangen kann und somit einer potenziellen schweren Verletzungsgefahr ausgesetzt ist. Software-Produkte allein können das Bedienpersonal nicht vor Verletzungen schützen. Die Software kann daher nicht als Ersatz für Sicherheitseinrichtungen im Arbeitsraum verwendet werden.

Vor Inbetriebnahme der Anlage sicherstellen, dass alle zum Schutz des Arbeitsraums vorgesehenen mechanischen/elektronischen Sicherheitseinrichtungen und Verriegelungen installiert und funktionsfähig sind. Alle zum Schutz des Arbeitsraums vorgesehenen Sicherheitseinrichtungen und Verriegelungen müssen mit dem zugehörigen Automatisierungsgerät und der Softwareprogrammierung koordiniert werden.

HINWEIS: Die Koordinierung der zum Schutz des Arbeitsraums vorgesehenen mechanischen/elektronischen Sicherheitseinrichtungen und Verriegelungen geht über den Umfang der Funktionsbaustein-Bibliothek, des System-Benutzerhandbuchs oder andere in dieser Dokumentation genannten Implementierungen hinaus.

Start und Test

Vor der Verwendung elektrischer Steuerungs- und Automatisierungsgeräte ist das System zur Überprüfung der einwandfreien Funktionsbereitschaft einem Anlauffest zu unterziehen. Dieser Test muss von qualifiziertem Personal durchgeführt werden. Um einen vollständigen und erfolgreichen Test zu gewährleisten, müssen die entsprechenden Vorkehrungen getroffen und genügend Zeit eingeplant werden.

WARNUNG

GEFAHR BEIM GERÄTEBETRIEB

- Überprüfen Sie, ob alle Installations- und Einrichtungsverfahren vollständig durchgeführt wurden.
- Vor der Durchführung von Funktionstests sämtliche Blöcke oder andere vorübergehende Transportsicherungen von den Anlagekomponenten entfernen.
- Entfernen Sie Werkzeuge, Messgeräte und Verschmutzungen vom Gerät.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Führen Sie alle in der Dokumentation des Geräts empfohlenen Anlauffests durch. Die gesamte Dokumentation zur späteren Verwendung aufbewahren.

Softwaretests müssen sowohl in simulierten als auch in realen Umgebungen stattfinden.

Sicherstellen, dass in dem komplett installierten System keine Kurzschlüsse anliegen und nur solche Erdungen installiert sind, die den örtlichen Vorschriften entsprechen (z. B. gemäß dem National Electrical Code in den USA). Wenn Hochspannungsprüfungen erforderlich sind, beachten Sie die Empfehlungen in der Gerätedokumentation, um eine versehentliche Beschädigung zu verhindern.

Vor dem Einschalten der Anlage:

- Entfernen Sie Werkzeuge, Messgeräte und Verschmutzungen vom Gerät.
- Schließen Sie die Gehäusetür des Geräts.
- Alle temporären Erdungen der eingehenden Stromleitungen entfernen.
- Führen Sie alle vom Hersteller empfohlenen Anlauftests durch.

Betrieb und Einstellungen

Die folgenden Sicherheitshinweise sind der NEMA Standards Publication ICS 7.1-1995 entnommen (die Englische Version ist maßgebend):

- Ungeachtet der bei der Entwicklung und Fabrikation von Anlagen oder bei der Auswahl und Bemessung von Komponenten angewandten Sorgfalt, kann der unsachgemäße Betrieb solcher Anlagen Gefahren mit sich bringen.
- Gelegentlich kann es zu fehlerhaften Einstellungen kommen, die zu einem unbefriedigenden oder unsicheren Betrieb führen. Für Funktionseinstellungen stets die Herstelleranweisungen zu Rate ziehen. Das Personal, das Zugang zu diesen Einstellungen hat, muss mit den Anweisungen des Anlagenherstellers und den mit der elektrischen Anlage verwendeten Maschinen vertraut sein.
- Bediener sollten nur über Zugang zu den Einstellungen verfügen, die tatsächlich für ihre Arbeit erforderlich sind. Der Zugriff auf andere Steuerungsfunktionen sollte eingeschränkt sein, um unbefugte Änderungen der Betriebskenngrößen zu vermeiden.

Sicherheitsanweisungen

Bei der Installation oder der Verwendung dieser Software müssen Sie auf die Sicherheitshinweise achten, die von der Software ausgegeben und in der Dokumentation beschrieben werden. Folgende Sicherheitshinweise gelten für diese Software in ihrer Gesamtheit.

⚠ WARNUNG

GEFAHR EINES UNBEABSICHTIGTEN GERÄTEBETRIEBS

- Die Software darf nicht für kritische Steuerung- oder Schutzapplikationen verwendet werden, wenn die Sicherheit von Personen oder Ausrüstungsgegenständen von der Ausführung der Kontrollaktion abhängig ist.
- Die Software darf nicht für zeitkritische Funktionen verwendet werden. Zwischen dem Start einer Kontrolle und der Ausführung der Aktion kann es zu einer Kommunikationsverzögerung kommen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠️ WARNUNG**GEFAHR UNGENAUER DATENERGEBNISSE**

- Sorgen Sie für eine korrekte Konfiguration der Software, um genaue Berichte und/oder Datenergebnisse zu erhalten.
- Verlassen Sie sich bei der Aktualisierung und Wartung nicht allein auf die von der Software angezeigten Meldungen und Informationen.
- Stützen Sie sich bei der Überprüfung einer korrekten Funktionsweise der Software und der Einhaltung geltender Standards und Anforderungen nicht allein auf die von der Software angezeigten Meldungen und Berichte.
- Berücksichtigen Sie die Auswirkungen unbeabsichtigter Übertragungsverzögerungen oder fehlerhafter Kommunikationslinks.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠️ WARNUNG**POTENTIELLE BEEINTRÄCHTIGUNG DER SYSTEMVERFÜGBARKEIT, INTEGRITÄT UND VERTRAULICHKEIT**

Nutzen Sie Best Practices für die Cybersicherheit.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

HINWEIS: Detaillierte Informationen zur Cybersicherheit finden Sie im Kapitel Cybersicherheit, Seite 75.

Über das Handbuch

Inhalt des Dokuments

In diesem Dokument wird das Tool EcoStruxure Automation Device Maintenance beschrieben. EcoStruxure Automation Device Maintenance kann die Firmware von einem PC auf unterstützte Schneider Electric-Geräte übertragen. Das Tool unterstützt die Erkennung relevanter Geräte im Netzwerk und ermöglicht die manuelle Identifizierung dieser Geräte, wenn die automatische Geräteerkennung nicht möglich ist.

Gültigkeitshinweis

Dieses Dokument wurde für EcoStruxure Automation Device Maintenance Version 3.1 aktualisiert.

Die im vorliegenden Dokument sowie in den Dokumenten im Abschnitt „Weiterführende Dokumentation“ beschriebenen Merkmale sind ebenfalls online verfügbar. Gehen Sie zur Homepage von Schneider Electric, um online auf die Informationen zuzugreifen: www.se.com/ww/en/download/. Für die Dokumentation von EcoStruxure Automation Device Maintenance geben Sie *EcoStruxure Automation Device Maintenance* im Suchtextfeld ein und drücken die **Eingabetaste**.

Die im vorliegenden Dokument beschriebenen Merkmale sollten denjenigen entsprechen, die online angezeigt werden. Im Rahmen unserer Bemühungen um eine ständige Verbesserung werden Inhalte im Laufe der Zeit möglicherweise überarbeitet, um deren Verständlichkeit und Genauigkeit zu verbessern. Sollten Sie einen Unterschied zwischen den Informationen im Dokument und denjenigen online feststellen, nutzen Sie bitte die Online-Informationen als Referenz.

Weiterführende Dokumentation

Titel der Dokumentation	Referenznummer
Firmware Compatibility Rules, Modicon M580, Modicon Momentum, and Modicon X80 I/O Modules	EIO0000002634 (English)
Modicon-Steuerungsplattform – Cybersicherheit, Referenzhandbuch	EIO0000001999 (English) EIO0000002001 (French) EIO0000002000 (German) EIO0000002003 (Spanish) EIO0000002002 (Italian) EIO0000002004 (Chinese)
Modbus-Spezifikationen und Implementierungshandbuch, Referenzhandbuch	Modbus Application Protocol Specification
Geräteprofile für Internetdienste, Referenzhandbuch	WSDD-DPWS

Titel der Dokumentation	Referenznummer
EcoStruxure™ Control Expert – Betriebsarten	33003101 (English) 33003102 (French) 33003103 (German) 33003104 (Spanish) 33003696 (Italian) 33003697 (Chinese)
EcoStruxure Automation Device Maintenance Altivar, Benutzerhandbuch	JYT50472 (English) JYT50474 (French) JYT50482 (German) JYT50476 (Spanish) JYT50478 (Italian) JYT50483 (Chinese) JYT50484 (Turkish) JYT50485 (Portuguese)

Produktinformationen

⚠️ WARNUNG

STEUERUNGS-AUSFALL

- Bei der Konzeption von Steuerungsstrategien müssen mögliche Störungen auf den Steuerpfaden berücksichtigt werden, und bei bestimmten kritischen Steuerungsfunktionen ist dafür zu sorgen, dass während und nach einem Pfadfehler ein sicherer Zustand erreicht wird. Beispiele kritischer Steuerungsfunktionen sind die Notabschaltung (Not-Aus) und der Nachlauf-Stopp, Stromausfall und Neustart.
- Für kritische Steuerungsfunktionen müssen separate oder redundante Steuerpfade bereitgestellt werden.
- Systemsteuerungspfade können Kommunikationsverbindungen umfassen. Dabei müssen die Auswirkungen unerwarteter Sendeverzögerungen und Verbindungsstörungen berücksichtigt werden.
- Sämtliche Unfallverhütungsvorschriften und lokalen Sicherheitsrichtlinien sind zu beachten.¹
- Jede Implementierung des Geräts muss individuell und sorgfältig auf einwandfreien Betrieb geprüft werden, bevor das Gerät an Ort und Stelle in Betrieb gesetzt wird.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

¹ Weitere Informationen finden Sie in den aktuellen Versionen von NEMA ICS 1.1 „Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control“ sowie von NEMA ICS 7.1, „Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems“ oder den entsprechenden, vor Ort geltenden Vorschriften.

Bevor Sie unter Verwendung der POUs in der Bibliothek eine Lösung (Maschine oder Prozess) für eine spezifische Anwendung bereitstellen, sind relevante Best Practices zu prüfen, anzuwenden und zu vervollständigen. Hierzu gehören u. a. Risikoanalyse, Funktionssicherheit, Komponentenkompatibilität, Prüfung und Systemabnahme, sofern ein Bezug zur Bibliothek gegeben ist.

▲ WARNUNG

UNSACHGEMÄSSE VERWENDUNG DER POUS

- Führen Sie für die betroffene Anwendung und die installierten Geräte eine sicherheitstechnische Analyse durch.
- Vergewissern Sie sich, dass die POUs mit den Geräten in Ihrem System kompatibel sind und den ordnungsgemäßen Betrieb des Systems nicht auf unbeabsichtigte Weise beeinträchtigen.
- Verwenden Sie geeignete Parameter, insbesondere für die Grenzwerte, und kontrollieren Sie Abnutzung und Stoppverhalten der Maschine.
- Stellen Sie sicher, dass die Sensoren und Stellglieder mit den ausgewählten POUs kompatibel sind.
- Bei der Prüfung und Inbetriebnahme sind sämtliche Funktionen in allen Betriebsarten einem gründlichen Test zu unterziehen.
- Stellen Sie in Übereinstimmung mit der durchgeführten sicherheitstechnischen Analyse und allen geltenden Regeln und Vorschriften unabhängige Verfahren für kritische Steuerungsfunktionen bereit (Nothalt, Überschreitung der Grenzbedingungen usw.).

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

▲ WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

- Verwenden Sie mit diesem Gerät nur von Schneider Electric genehmigte Software.
- Aktualisieren Sie Ihr Anwendungsprogramm jedes Mal, wenn Sie die physische Hardwarekonfiguration ändern.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Unvollständige Dateiübertragungen, wie Datendateien, Anwendungsdateien und/oder Firmwaredateien, können ernsthafte Folgen für Ihre Maschine oder Ihre Steuerung haben/ Wenn Sie während der Dateiübertragung den Strom abschalten oder ein Stromausfall oder eine Kommunikationsunterbrechung auftritt, kann Ihre Maschine nicht mehr operativ sein oder Ihre Anwendung kann versuchen, mit beschädigten Dateidaten zu arbeiten. Sollte die Kommunikation unterbrochen werden, dann führen Sie die Übertragung erneut durch. Stellen Sie sicher, dass Sie den Effekt beschädigter Daten in Ihrer Risikoanalyse berücksichtigen.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB, DATENVERLUST ODER DATEIBESCHÄDIGUNG

- Unterbrechen Sie eine laufende Datenübertragung nicht.
- Wenn die Übertragung aus einem beliebigen Grund unterbrochen wird, starten Sie sie erneut.
- Nehmen Sie Ihre Maschine nicht in Betrieb bis die Dateiübertragung erfolgreich abgeschlossen wurde, es sei denn, sie haben die beschädigten Daten in Ihre Risikoanalyse miteinbezogen und entsprechende Schritte eingeleitet, um mögliche ernste Folgen wegen einer nicht erfolgreichen Datenübertragung zu vermeiden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Bei Verwendung dieser Bibliothek zur Maschinensteuerung ist besondere Vorsicht geboten. Sie müssen angemessene Sicherheitsvorkehrungen treffen, um unbeabsichtigte Folgen für den gesteuerten Maschinenbetrieb, Zustandsänderungen, eine Änderung des Datenspeichers oder der Maschinenbetriebsparameter zu vermeiden.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEBETRIEB

- Positionieren Sie Bediengeräte für das Steuerungssystem in nächster Nähe der Maschine bzw. an einem Ort, an dem Sie über eine ungehinderte Sicht auf die Maschine verfügen.
- Schützen Sie die Bedienerbefehle vor unberechtigt Zugriff.
- Wenn die Fernsteuerung ein wichtiger Bestandteil bei der Gestaltung Ihrer Anwendung ist, müssen Sie sicherstellen, dass beim Betrieb ausgehend von einem dezentralen Standort kompetentes und qualifiziertes Wachpersonal vor Ort bereitsteht.
- Konfigurieren und installieren Sie einen Run/Stop-Eingang, sofern verfügbar, oder andere externe Vorrichtungen innerhalb der Anwendung, um eine lokale Kontrolle über den Start und Stopp des Geräts ungeachtet der jeweils gesendeten dezentralen Befehle zu gewährleisten.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Terminologie gemäß den geltenden Normen

Die technischen Begriffe, Terminologien, Symbole und zugehörigen Beschreibungen, die in diesem Handbuch oder auf dem Produkt selbst verwendet werden, werden im Allgemeinen von den Begriffen oder Definitionen internationaler Standards abgeleitet.

Im Bereich der funktionalen Sicherheitssysteme, Antriebe und allgemeinen Automatisierungssysteme betrifft das unter anderem Begriffe wie *Sicherheit*, *Sicherheitsfunktion*, *Sicherer Zustand*, *Fehler*, *Fehlerreset/Zurücksetzen bei Fehler*, *Ausfall*, *Störung*, *Warnung/Warmmeldung*, *Fehlermeldung*, *gefährlich/ gefahrbringend* usw.

Nachstehend einige der geltenden Standards:

Norm	Beschreibung
IEC 61131-2:2007	Speicherprogrammierbare Steuerungen, Teil 2: Betriebsmittelanforderungen und Prüfungen
ISO 13849-1:2015	Sicherheit von Maschinen: Sicherheitsbezogene Teile von Steuerungen Allgemeine Gestaltungsleitsätze
EN 61496-1:2013	Sicherheit von Maschinen: Berührungslos wirkende Schutzeinrichtungen Teil 1: Allgemeine Anforderungen und Prüfungen
ISO 12100:2010	Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
EN 60204-1:2006	Sicherheit von Maschinen – Elektrische Ausrüstungen von Maschinen – Teil 1: Allgemeine Anforderungen
ISO 14119:2013	Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl
ISO 13850:2015	Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze
IEC 62061:2015	Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und elektronisch programmierbarer Steuerungssysteme
IEC 61508-1:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme: Allgemeine Anforderungen
IEC 61508-2:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme
IEC 61508-3:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme: Anforderungen an Software
IEC 61784-3:2016	Industrielle Kommunikationsnetze - Profile - Teil 3: Funktional sichere Übertragung bei Feldbussen - Allgemeine Regeln und Festlegungen für Profile.
2006/42/EC	Maschinenrichtlinie
2014/30/EU	EMV-Richtlinie (Elektromagnetische Verträglichkeit)
2014/35/EU	Niederspannungsrichtlinie

Darüber hinaus wurden einige der in diesem Dokument verwendeten Begriffe unter Umständen auch anderen Normen entnommen, u. a.:

Norm	Beschreibung
Normenreihe IEC 60034	Rotierende elektrische Geräte
Normenreihe IEC 61800	„Adjustable speed electrical power drive systems“: Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl
Normenreihe IEC 61158	Industrielle Kommunikationsnetze – Feldbus für industrielle Steuerungssysteme

Bei einer Verwendung des Begriffs *Betriebsumgebung/Betriebsbereich* in Verbindung mit der Beschreibung bestimmter Gefahren und Risiken entspricht der Begriff der Definition von *Gefahrenbereich* oder *Gefahrenzone* in der *Maschinenrichtlinie* (2006/42/EC) und der Norm *ISO 12100:2010*.

HINWEIS: Die vorherig erwähnten Standards können auf die spezifischen Produkte in der vorliegenden Dokumentation zutreffen oder nicht. Für weitere Informationen hinsichtlich individueller Standards, die auf hier beschriebene Produkte zutreffen, siehe die Eigenschaftstabellen der hier erwähnten Produkte.

Einführung

Überblick

Einführung

EcoStruxure Automation Device Maintenance ermöglicht Ihnen das Upgrade der Firmwarepakete auf mehreren Geräten gleichzeitig. Die Geräte können automatisch erkannt oder manuell hinzugefügt werden, wenn die automatische Geräteerkennung nicht unterstützt wird oder auf dem Gerät ausgeschaltet wurde.

Im Folgenden sind die unterstützten Geräteerkennungsverfahren aufgeführt:

- Modbus-Funktionscode 43 (Geräteidentifikation lesen)
- DPWS (Device Profile for Web Services)

Funktionen

EcoStruxure Automation Device Maintenance unterstützt die folgenden Funktionen:

- Automatische Geräteerkennung
- Manuelle Geräteidentifikation
- Sicherheitsmerkmale
- Firmwareaktualisierung für mehrere Geräte gleichzeitig
- Verwaltung der IP-Adresse

Unterstützte Geräte von Schneider Electric

Modicon-Geräte:

- Modicon M340
- Modicon M580
- Modicon Momentum
- Modicon X80-E/A-Module

Altivar-Geräte:

- Altivar-Produktfamilien
 - Altivar Process ATV6••-Antriebe
 - Altivar Process ATV9••-Antriebe
 - Altivar Machine ATV340-Antriebe
- Altivar-Optionsmodule:
 - VW3A3720 Ethernet
 - VW3A3721 MultiDrive-Link
 - VW3A3530D ATV dPAC
- Altivar-Sanftanlasser:
 - Altivar-Sanftanlasser ATS480

Systemanforderungen

Hardwareanforderungen

Komponente	Mindestanforderung
CPU	Intel® Core i3 oder aktueller wird unterstützt
RAM	Minimum 4 GB, 8 GB oder mehr empfohlen
Festplattenspeicher	500 MB verfügbarer Festplattenspeicher

Softwareanforderungen

- Microsoft Windows® 10 Professional 32-Bit/64-Bit oder aktueller
- Microsoft Windows Server 2016 Standard 64-Bit
- Microsoft Windows Server 2019 Standard 64-Bit

Kommunikationsprotokolle

Das Tool unterstützt folgende Protokolle:

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

Bildschirmauflösung

Legen Sie die Bildschirmauflösung auf 1920 x 1080 Pixel fest, um von einer optimalen Anzeigequalität zu profitieren. Eine Bildschirmauflösung von mindestens 1280 x 1024 Pixel ist erforderlich.

Cybersicherheit

Die Software nutzt die folgenden Ports:

- DPWS (über Port 3702)
- FTP (über Ports 20, 21)
- HTTP (über Port 80) / HTTPS (über Ports 443 und 8080)
- Modbus (über Port 502)
- OPC UA (über Port 4840)

⚠ WARNUNG

POTENTIELLE BEEINTRÄCHTIGUNG DER SYSTEMVERFÜGBARKEIT, INTEGRITÄT UND VERTRAULICHKEIT

Nutzen Sie Best Practices für die Cybersicherheit.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

HINWEIS: Detaillierte Informationen zur Cybersicherheit finden Sie im Kapitel Cybersicherheit, Seite 75.

Installation

Vorgehensweise

Sie können die Software installieren, indem Sie die Installationsdateien von der Schneider Electric-Website herunterladen.

HINWEIS: Bevor Sie auf die Datei AutomationDeviceMaintenance.exe doppelklicken, überprüfen Sie die Integrität der Datei gemäß der Beschreibung in Kapitel Prüfung der digitalen Signatur, Seite 79.

HINWEIS: Für die Installation der Software müssen Sie über Administratorrechte verfügen.

Gehen Sie zum Installieren der Software vor wie folgt:

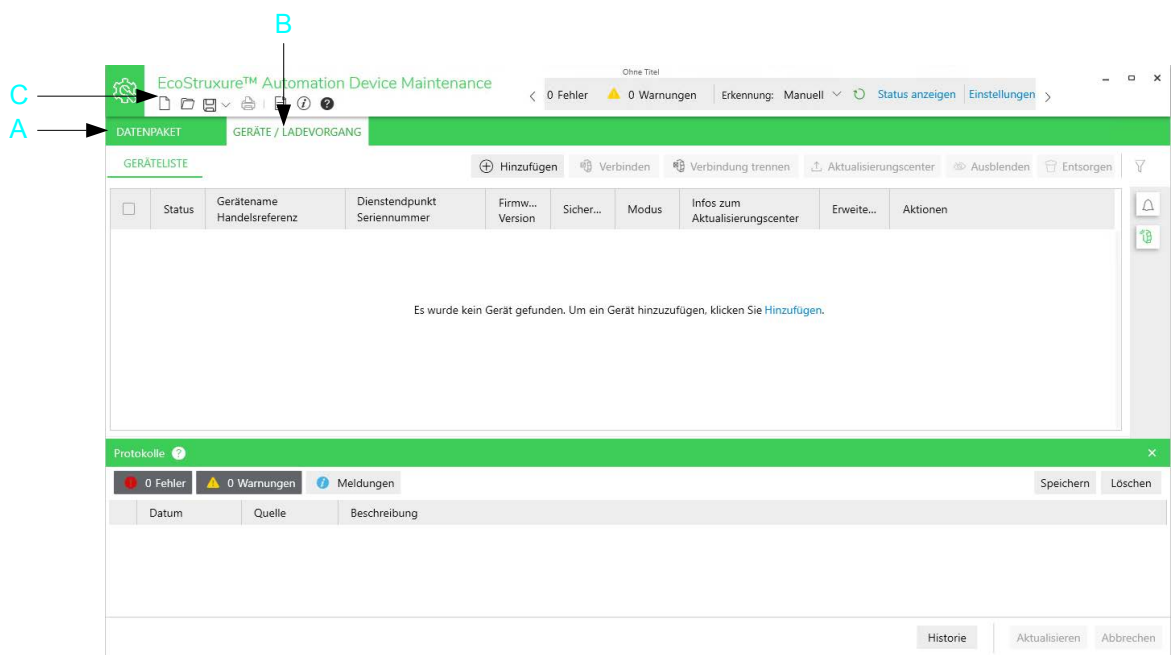
Schritt	Aktion
1	Suchen Sie mit dem Windows Explorer nach den heruntergeladenen Installationsdateien.
2	Doppelklicken Sie auf die Setupdatei von EcoStruxure Automation Device Maintenance. Der InstallShield Wizard wird angezeigt.
3	Folgen Sie den Anweisungen im InstallShield Wizard , um die Installation abzuschließen.

Erste Schritte

Willkommen-Fenster

Überblick











Nach dem ersten Start zeigt EcoStruxure Automation Device Maintenance das folgende Fenster an, um eine Aktualisierung der Firmwarepakete auf mehreren Geräten durchzuführen. Wenn Sie das Tool schließen, wird der aktuelle Zustand der Benutzeroberfläche gespeichert. Beim erneuten Start von EcoStruxure Automation Device Maintenance wird somit die Ansicht angezeigt, die beim letzten Schließen des Tools vorhanden war.



Legende	Name	Funktion
A	Datenpaket	Zeigt den Inhalt des Datenpaket-Repositorys an.
B	Geräte/Ladevorgang	Zeigt die Details der automatisch erkannten oder manuell identifizierten Geräte an.
C	Symbolleiste	Zeigt Symbole für die Ausführung bestimmter Funktionen an.

Symbolleiste

Die Symbolleiste ermöglicht den Zugang zu den Standardfunktionen von EcoStruxure Automation Device Maintenance.

Element	Name	Beschreibung
	Neues Projekt	Ermöglicht Ihnen das Erstellen eines neuen EcoStruxure Automation Device Maintenance-Projekts, Seite 27.
	Öffnen	Ermöglicht Ihnen, ein vorhandenes Projekt (existing project, Seite 29) zu öffnen.
	Speichern	Ermöglicht Ihnen, die Projekteinstellungen (project settings, Seite 28) zu speichern.
	Drucken	Diese Funktion ist in dieser Version nicht verfügbar.
	Protokolle	Ermöglicht Ihnen, die Protokollinformationen anzuzeigen.
	Info über	Zugang zu: <ul style="list-style-type: none"> • Informationen über EcoStruxure Automation Device Maintenance • Versionsangaben • Lizenzvertrag • Komponentenspezifische Informationen • Systeminformationen
	Hilfe	Zugang zur Online-Hilfe.
	Fehler	Ermöglicht Ihnen die erkannten Fehler anzuzeigen , Seite 26.
	Warnung	Ermöglicht Ihnen, die erkannten Warnungen anzuzeigen , Seite 26.
	Erkennung	Ermöglicht die Auslösung der Geräteerkennung, wenn der Modus für die Geräteerkennung auf Manuell festgelegt ist.
–	Manuell/Automatisch	Wählen Sie in der Liste den Geräteerkennungsmodus Manuell oder Automatisch aus. Weitere Informationen finden Sie im Kapitel <i>Konfiguration des Geräteerkennungsmodus</i> , Seite 32.
–	Einstellungen	Konfiguration der Einstellungen .

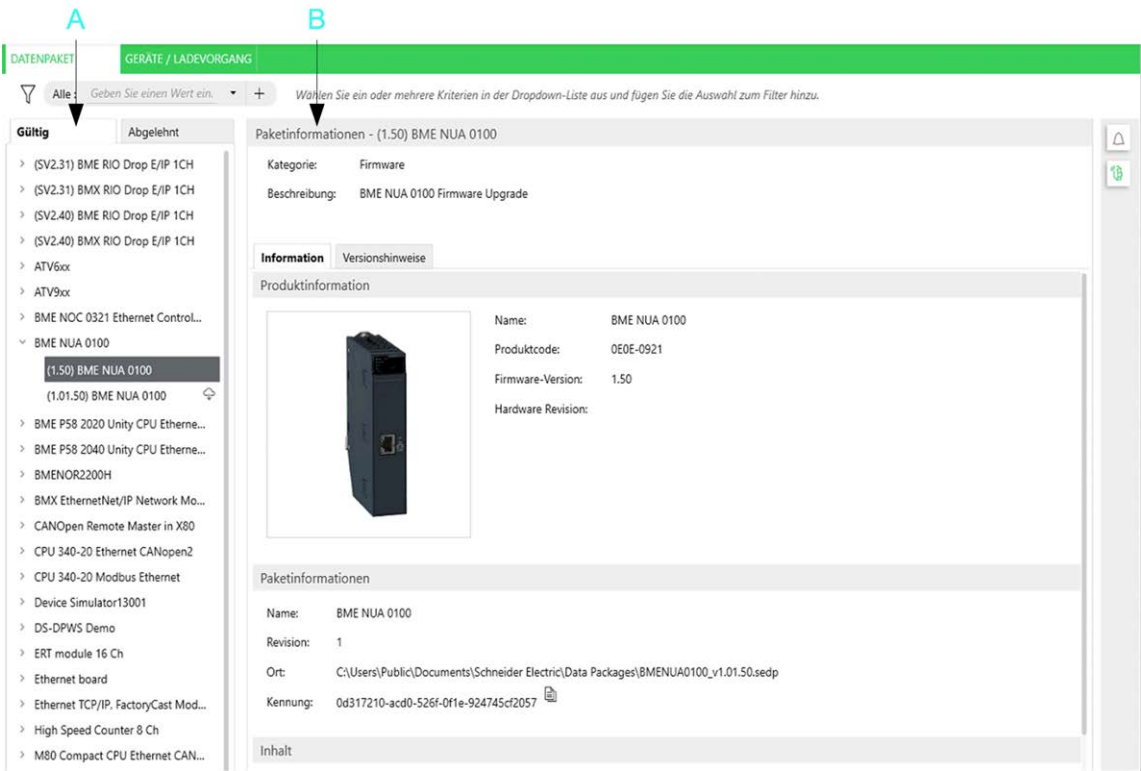
Schaltflächen

Schaltfläche	Beschreibung
Zusammenfassung	Nachdem Sie eine Aktualisierung durchgeführt haben, klicken Sie auf die Schaltfläche Zusammenfassung , um Informationen zu den aktualisierten Geräten abzurufen.
Aktualisieren	Nachdem Sie die Einstellungen für die Aktualisierung der Firmware, Seite 70 oder die Aktualisierung der Sicherheitskonfigurationsdatei, Seite 72 vorgenommen haben, klicken Sie auf die Schaltfläche Aktualisieren , um den Aktualisierungsvorgang wie konfiguriert zu starten.
Abbrechen	Die Schaltfläche Abbrechen ermöglicht Ihnen, einen Aktualisierungsvorgang abzubrechen.

EcoStruxure Automation Device Maintenance - Benutzeroberfläche

Datenpaket

Die Option **Datenpaket** enthält ein Paketrepository und zeigt die Firmware-Pakete an, die im Tool verfügbar sind.




Legende	Name	Beschreibung
A	Liste DATENPAKET mit Registerkarten Gültig und Abgelehnt	Zeigt die Liste der lokal verfügbaren Firmwarepakete an. Im Netzwerk verfügbare Pakete werden angezeigt, wenn das erforderliche Add-On installiert ist. Weitere Informationen finden Sie im Kapitel <i>Registerkarte "Datenpaket"</i> , Seite 51.
B	Paketinformationen	Zeigt die Beschreibung und den Inhalt des ausgewählten Datenpakets mit statischen Informationen im oberen Bereich (Kategorie und Beschreibung) und den beiden Registerkarten Informationen und Release Notes im unteren Bereich an. Weitere Informationen finden Sie im Kapitel <i>Registerkarte "Datenpaket"</i> , Seite 51.

Geräte/Ladevorgang

Überblick

Auf der Registerkarte **Geräte/Ladevorgang** werden die Details der dem Tool bekannten Geräte angezeigt.

HINWEIS: Die auf dieser Registerkarte angezeigten Informationen werden nur automatisch aktualisiert, wenn der Erkennungsmodus auf **Automatisch**

eingestellt ist. Klicken Sie auf das Symbol  in der Symbolleiste, um die neuesten Werte anzuzeigen.

DATENPAKET

GERÄTE / LADEVORGANG

GERÄTELISTE

Hinzufügen

Verbinden

Verbindung trennen

Aktualisierungscenter

Ausblenden

Entsorgen









<input checked="" type="checkbox"/>	Status	Gerätename Handelsreferenz	Dienstendpunkt Seriennummer	Firmw... Version	Sicherhei...	Modus	Infos zum Aktualisierungscenter	Erweiterungen	Aktionen
<input checked="" type="checkbox"/>	Gerätestandardgruppe (8)								
<input checked="" type="checkbox"/>	<div><div></div><div></div></div>	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-		Erweiterungen	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div></div></div>	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"/>	<div><div></div><div></div></div>	ATV930_Spare CR: ATV930D11M3	mbap://172.20.170.208:502 SN: 402110088536202002	3.5IE94B04	-	-		-	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>



Schaltflächen der Registerkarte:

Schaltfläche	Beschreibung
Add	Klicken Sie auf die Schaltfläche Hinzufügen , um ein neues Gerät hinzuzufügen. Für weitere Informationen siehe Hinzufügen von Geräten , Seite 23.
Verbinden	Klicken Sie auf die Schaltfläche Verbinden , um eine Verbindung zu den ausgewählten Geräten herzustellen.
Verbindung trennen	Klicken Sie auf die Schaltfläche Trennen , um die Verbindung zu den ausgewählten Geräten zu beenden.
Aktualisierungscenter	Klicken Sie auf die Schaltfläche Aktualisierungscenter , um das Dialogfeld Aktualisierungscenter zu öffnen. In diesem Dialogfeld können Sie Einstellungen für die Durchführung einer Firmwareaktualisierung oder einer Aktualisierung der Sicherheitskonfigurationsdatei für das bzw. die ausgewählten Geräte konfigurieren. Für weitere Informationen siehe Aktualisierungscenter , Seite 69.
Hide	Klicken Sie auf die Schaltfläche Ausblenden , um die erkannten Geräte auszublenden. Weitere Informationen finden Sie unter Ansicht „Geräte/Ladevorgang“ , Seite 55.
Dispose	Klicken Sie auf die Schaltfläche Entsorgen , um die erkannten Geräte zu entfernen. Weitere Informationen finden Sie unter Ansicht „Geräte/Ladevorgang“ , Seite 55.
	Klicken Sie auf die Schaltfläche Benachrichtigungsbereich , um den Benachrichtigungsbereich auf der rechten Seite der Registerkarte Geräte/Ladevorgang anzuzeigen. Weitere Informationen finden Sie unter Anzeigen/Bestätigen von Meldungen , Seite 67.
	Klicken Sie auf die Schaltfläche Geräteerkennungstatus , um die Ansicht Geräteerkennungstatus auf der rechten Seite der Registerkarte Geräte/Ladevorgang anzuzeigen. Weitere Informationen finden Sie unter Überwachung des Geräteerkennungstatus , Seite 66.

Elemente der Tabelle:

Element	Beschreibung
Gruppe	Sie können die in der GERÄTELISTE angezeigten Geräte verschiedenen Gruppen zuweisen, wie im Kapitel Gruppierung von Geräten in der GERÄTELISTE , Seite 56 beschrieben. Um alle Geräte auszuwählen, die zu einer Gruppe gehören, aktivieren Sie das Kontrollkästchen der Gruppe .
Kontrollkästchen	Aktivieren Sie mehrere Kontrollkästchen auf der linken Seite, um denselben Vorgang für mehrere Geräte gleichzeitig durchzuführen, z. B. Verbinden/Trennen oder eine Aktualisierung.

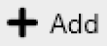
Element	Beschreibung
Status	<p>Zeigt den Gerätestatus an.</p> <ul style="list-style-type: none"> Grau: Das Gerät ist nicht mit dem Netzwerk verbunden. Gelb: Das Gerät ist mit dem Netzwerk verbunden, es wurden jedoch keine gültigen Anmeldeinformationen eingegeben. Grün: Es wurden gültige Anmeldeinformationen eingegeben. Blau: Das Tool lädt Inhalt in das Gerät. Rot: Das Gerät wird nach dem Herunterladen der Firmware neu gestartet, um die Installation abzuschließen.
Gerätename Handelsreferenz	<p>Zeigt den Namen und die Handelsreferenz (CR: Commercial Reference) des Geräts an.</p> <p>HINWEIS: Wenn Sie Ihrem Gerät einen Friendly Name zugewiesen haben, wird dieser benutzerdefinierte Name nur angezeigt, wenn das Kommunikationsprotokoll diesen Parameter unterstützt. Beispielsweise wird es von Modbus TCP nicht unterstützt.</p>
Dienstendpunkt Seriennummer	<p>Zeigt die Adresse des Dienstendpunkts als URI (Uniform Resource Identifier) sowie die Seriennummer (SN) des Geräts an.</p>
Firmwareversion	<p>Zeigt die aktuelle Firmwareversion des Geräts an.</p>
Modus	<p>Nur nach der Anmeldung verfügbar: Gibt den Modus des Geräts an: RUN, STOP, BUSY, NOCONF, RESERVED, ENTERED, LOADING, COMPLETED, REQUIRERESTART, FEHLER. Der Inhalt dieser Zelle wird regelmäßig aktualisiert.</p> <p>HINWEIS: Abhängig von der Anzahl der Geräte, mit denen Sie verbunden sind, kann diese Modusüberwachung Auswirkungen auf die Netzwerkbandbreite haben.</p>
Infos zum Aktualisierungszentrum	<p>Zeigt die Aktualisierungseinstellungen an, die im Dialogfeld Aktualisierungszentrum konfiguriert wurden: Firmware ausgewählt, Sicherheitskonfiguration ausgewählt, Firmwareaktualisierung erfolgreich, Firmwareaktualisierung abgebrochen, Firmwareaktualisierung gescheitert. Für weitere Informationen siehe Aktualisierungszentrum, Seite 69.</p>
Erweiterungen	<p>Modulare Geräte stellen einen Link (Erweiterungen) zur Verfügung, über den Sie auf die einzelnen Erweiterungen des Geräts zugreifen können. Für weitere Informationen siehe Zugriff auf Erweiterungen, Seite 64.</p>
Aktionen	<p>Für jedes Gerät sind Symbole verfügbar, um verschiedene gerätespezifische Vorgänge auszuführen:</p>
	<p>Klicken Sie auf das Symbol Anmeldedaten festlegen und geben Sie die Anmeldeinformationen für die Verbindung mit dem Gerät im Dialogfeld Anmeldedaten festlegen ein. Das schwarze Symbol zeigt an, dass keine Anmeldedaten für das Gerät gespeichert sind. Das gelbe Symbol zeigt an, dass die Anmeldedaten gespeichert wurden, aber keine Anmeldung beim Gerät durchgeführt wurde.</p> <p>Alternativ können Sie globale Anmeldedaten für das Projekt über Einstellungen > Projekt > Einstellungen für die Benutzeranmeldedaten konfigurieren. Weitere Informationen finden Sie unter Verwaltung der Benutzeranmeldedaten, Seite 61.</p>
	<p>Das grüne Symbol Anmeldedaten festlegen gibt an, dass die Anmeldedaten für das Gerät überprüft wurden und die Anmeldung erfolgreich durchgeführt wurde.</p>
	<p>Das rote Symbol Anmeldedaten festlegen zeigt an, dass der Versuch, sich beim Gerät anzumelden, nicht erfolgreich war.</p> <p>Führen Sie das Anmeldeverfahren erneut durch und geben Sie unbedingt die richtigen Anmeldedaten an.</p>
	<p>Klicken Sie auf das Symbol Verbinden / Trennen, um eine Verbindung zum Gerät herzustellen oder die Verbindung zu trennen.</p>
	<p>Klicken Sie auf das Symbol Aktualisierungszentrum, um das Dialogfeld Aktualisierungszentrum zu öffnen. In diesem Dialogfeld können Sie Einstellungen für die Durchführung einer Firmwareaktualisierung oder einer Aktualisierung der Sicherheitskonfigurationsdatei für das Gerät konfigurieren. Für weitere Informationen siehe Aktualisierungszentrum, Seite 69.</p>
	<p>Klicken Sie auf das Symbol Geräteprotokoll, um die Protokollinformationen anzuzeigen.</p>
	<p>Klicken Sie auf das Symbol Gerät starten, um das Gerät zu starten.</p> <p>HINWEIS: Führen Sie zuerst einen Anlauftest durch, bevor Sie elektrische Steuerungs- und Automatisierungsgeräte für einen regulären Betrieb nach der Installation bzw. einer Aktualisierung verwenden. Für weitere Informationen siehe Start und Test, Seite 7.</p>
	<p>Zeigt den Zertifikatsstatus an.</p> <ul style="list-style-type: none"> Grau: Vertrauenswürdiges Zertifikat Rot: Nicht vertrauenswürdiges Zertifikat <p>Klicken Sie auf das Symbol Gerätezertifikat, um das Dialogfeld Zertifikatinformationen zu öffnen. Für weitere Informationen siehe Verwalten des Vertrauensstatus von Zertifikaten auf der Registerkarte Geräte/Ladevorgang, Seite 47.</p>

Element	Beschreibung
	Gibt an, dass das Gerät mit einer SD-Speicherkarte ausgestattet ist. Klicken Sie auf dieses Symbol, um Software direkt auf die SD-Speicherkarte herunterzuladen.
	Klicken Sie auf das Symbol Zusätzliche Geräteoptionen , um eine Liste der Befehle anzuzeigen, die für Geräte nach erfolgreicher Anmeldung verfügbar sind. Weitere Informationen finden Sie unter <i>Verfügbare Details nach der Anmeldung</i> , Seite 56.
Fortschritt	Zeigt den Fortschritt der Aktualisierung an.

Hinzufügen von Geräten

Überblick

Das Dialogfeld **Gerät** hinzufügen wird geöffnet, indem Sie auf die Schaltfläche

 auf der Registerkarte **Gerät/Laden** oder auf **Kein Gerät gefunden** **Zum Hinzufügen eines Moduls hier klicken** klicken. Dieser Link wird angezeigt, wenn die Geräteliste leer ist, z. B. wenn Sie ein neues Projekt erstellen.

Gerät hinzufügen

Bestellreferenz suchen

Suchen...

Verbindung:*

HTTP/HTTPS

Handelsreferenz:*

140***

140*** (Modernisiert)

171***

171*** (Modernisiert)

ATS***

ATS*** (Modernisiert)

ATV***

ATV*** (Modernisiert)

☒ Sichere Verbindung

IP-Adresse:*

172.10.15.25

x

:

443

Hinweis: Modernisiert = Markteinführung nach 2019

Weitere Informationen hierzu finden Sie im [Produktkatalog von Schneider Electric](#).

Gerät hinzufügen

Abbrechen

In diesem Dialogfeld können Sie Geräte manuell hinzufügen, wenn diese nicht automatisch von EcoStruxure Automation Device Maintenance erkannt werden können, weil das Gerät die Erkennung nicht unterstützt oder die Funktion zur Geräteerkennung ausgeschaltet ist. Wählen Sie dazu die Handelsreferenz aus.

Standardmäßig enthält die Liste der **Handelsreferenzen** nur Vorlagen für Handelsreferenzen (z. B. **BME*****, **BMX***** oder **Jedes Gerät**). In diesem Fall haben Sie zwei Möglichkeiten:

- Wählen Sie die Vorlage aus, die Ihrem Produkt entspricht: Wählen Sie für BMEP582020 beispielsweise **BME***** in der Liste aus.

HINWEIS: Für jede Vorlage werden zwei Varianten bereitgestellt, die die Vorgängerversion (z. B. **BME*****) und die aktuelle Version (z. B. **BME*** (modernisiert)**) abdecken. Sie unterscheiden sich in den unterstützten Protokollen. Wenn Sie das von Ihnen gewünschte Protokoll also nicht in der Liste **Verbindung** finden, wählen Sie die zweite Option aus, die für Ihr Produkt verfügbar ist.

- Um die Liste mit den Handelsreferenzen der verwendeten Geräte zu füllen, kopieren Sie die entsprechenden Datenpakete in den Ordner, den Sie als **Lokales Repository** im Dialogfeld **Einstellungen > Paketeinstellungen** konfiguriert haben. Weitere Informationen finden Sie im Kapitel *Konfiguration der Speicherorte für Pakete*, Seite 37. In der Tabelle werden dann spezifische Referenzen angezeigt (z. B. **BMEP582020** oder **BMXNOR0200**).

Komponente	Beschreibung
Handelsreferenz	Wählen Sie die Handelsreferenz Ihres Geräts in der Liste aus und geben Sie die Geräteinformationen gemäß dem in der Liste Verbindung rechts ausgewählten Protokoll ein.
Verbindung	Wählen Sie das für die Kommunikation verwendete Protokoll in der Liste aus: <ul style="list-style-type: none"> HTTP/HTTPS MODBUS (SL) MODBUS (TCP) OPC UA FTP USB Je nach ausgewähltem Protokoll werden die Parameter angepasst.
Sicher	Diese Option ist nur für die Kommunikation über HTTP/HTTPS verfügbar: Wählen Sie die Option aus, wenn das Gerät über eine gesicherte Verbindung (HTTPS) angeschlossen ist.
IP-Adresse	Geben Sie die IP-Adresse des hinzuzufügenden Geräts und den Port ein, der für die Kommunikation verwendet wird.
Einheits-ID	Diese Option ist nur für die Kommunikation über MODBUS (TCP) verfügbar: Geben Sie den Identifikationsknoten der Einheit für die Modbus TCP-Kommunikation ein. Weitere Informationen zu Modbus-Spezifikationen finden Sie hier: Modbus Specifications and Implementation Guides .

HINWEIS: EcoStruxure Automation Device Maintenance V3.1 und höher unterstützt das Hinzufügen von Geräten über die Handelsreferenz. Wenn Sie versuchen, Projektdateien zu öffnen, die mit EcoStruxure Automation Device Maintenance V3.0 und früheren Versionen erstellt wurden, die Geräte ohne Handelsreferenz enthalten, werden Sie zur Auswahl einer Handelsreferenz für jedes unbekannte Gerät aufgefordert.

Siehe auch *Öffnen eines Projekts*, Seite 29.

Konfiguration der Einstellungen

Überblick

Auf der Seite **Einstellungen** können Sie die Einstellungen für den Normalbetrieb konfigurieren.

Einstellungen

Global

Erkennung

DPWS

Modbus TCP

Kommunikation

Paketeinstellungen

Sicherheit

Zertifikatmanagement

PKI

Syslog

Protokolle

Sprache

Gruppe

Projekt

Erkennung

Erkennungsmodus: ☒ Manuell ☐ Automatisch

Scanner	<input checked="" type="checkbox"/> Scanner aktivieren	Status
DPWS	<input checked="" type="checkbox"/>	Inaktiv
Modbus TCP	<input checked="" type="checkbox"/>	Inaktiv

Zurücksetzen

OK

Abbrechen


Übernehmen

Komponenten	Beschreibung
Erkennung	Option zum Konfigurieren des Erkennungsmodus. Weitere Informationen finden Sie unter Konfiguration des Geräteerkennungsmodus, Seite 32.
DPWS	Option zum Konfigurieren des DPWS-Scanners. Weitere Informationen finden Sie unter Konfiguration des DPWS-Scanners, Seite 36.
Modbus TCP	Option zum Konfigurieren des Modbus-Scanners. Weitere Informationen finden Sie unter Konfiguration des Modbus TCP-Scanners, Seite 34.
Kommunikation	Option zum Konfigurieren der Kommunikationseinstellungen. Weitere Informationen finden Sie unter Konfiguration der Kommunikationseinstellungen, Seite 37.
Paketeinstellung	Option zum Konfigurieren der Paketeinstellungen. Weitere Informationen finden Sie unter Konfiguration der Speicherorte für Pakete, Seite 37.
Sicherheit	Wählen Sie die Option aus, um den Schutzmodus zu aktivieren und Benachrichtigungen zu den Sicherheitsfunktionen anzuzeigen, wie z. B. verschlüsselte Kommunikation über Zertifikate, gesicherte Pakete oder syslog-Support. Weitere Informationen finden Sie unter Sicherheitsfunktionen, Seite 41.
Zertifikatmanagement	Wählen Sie die Option aus, um das Anwendungszertifikat für EcoStruxure Automation Device Maintenance zu registrieren und den Vertrauensstatus der digitalen Zertifikate der Kommunikationspartner zu verwalten. Weitere Informationen finden Sie unter Verwaltung der Zertifikate, Seite 43.
PKI	Wählen Sie diese Option aus, um die Public-Key-Infrastruktur (PKI) zu konfigurieren. Weitere Informationen finden Sie unter Verwalten der Public Key-Infrastruktur (PKI), Seite 48.
Protokolle	Wählen Sie diese Option aus, um die Protokolldateien von EcoStruxure Automation Device Maintenance anzuzeigen und die Protokolleinstellungen zu konfigurieren. Weitere Informationen finden Sie unter Anzeigen der Protokolldateien, Seite 38.
Sprache	Option zum Konfigurieren der gewünschten Sprache. Weitere Informationen finden Sie unter Konfigurieren der Sprache, Seite 40.

Komponenten	Beschreibung
Gruppe	Wählen Sie diese Option aus, um Geräte zu gruppieren, die in der GERÄTELISTE angezeigt werden. Weitere Informationen finden Sie unter Gruppierung von Geräten in der GERÄTELISTE, Seite 56.
Projekt > Einstellungen für die Benutzeranmeldedaten	Wählen Sie diese Option aus, um globale Anmeldedaten für die Projektgeräte einzugeben. Weitere Informationen finden Sie unter Verwaltung der Benutzeranmeldedaten, Seite 61.

Anwenden von Änderungen

Wenn Sie die Einstellungen auf einer Registerkarte der Seite **Einstellungen**

ändern, wird diese Registerkarte durch das Symbol „Aktualisieren“  gekennzeichnet, das angibt, dass auf dieser Seite Änderungen vorgenommen wurden, die jedoch noch nicht angewendet wurden.

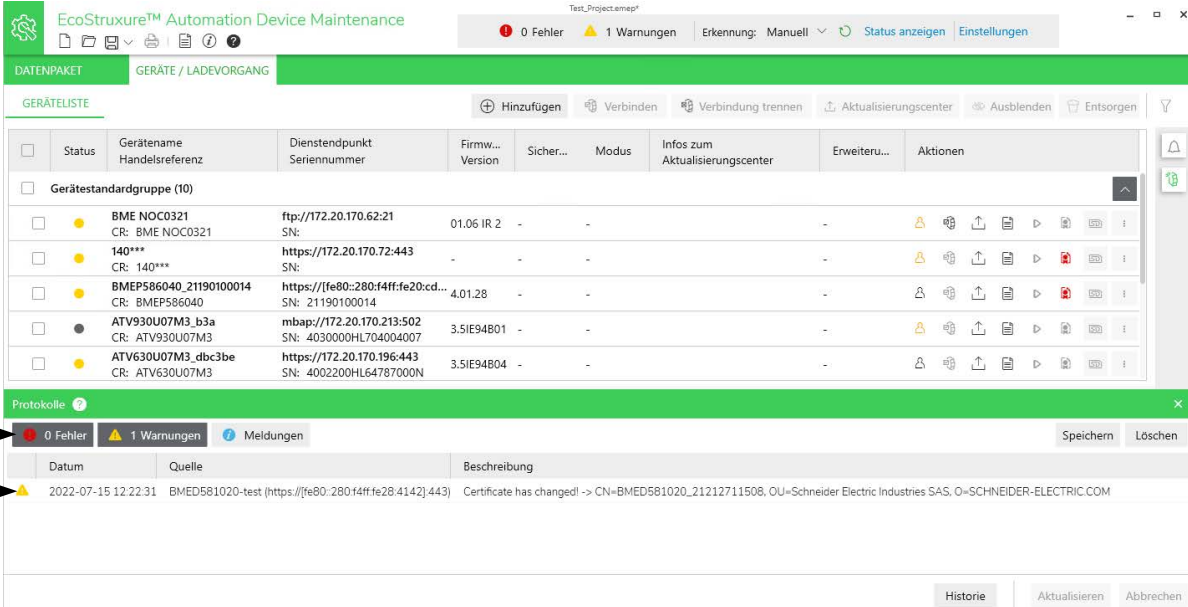
Um die Änderungen auf dieser Seite anzuwenden, klicken Sie auf die Schaltfläche **Anwenden**.

Um die auf allen Registerkarten vorgenommenen Änderungen zu übernehmen und die Seite **Einstellungen** zu schließen, klicken Sie auf die Schaltfläche **OK**.

Fenster der Fehler und Warnmeldungen

Überblick

Sie können die Einzelheiten zu den vom Tool erkannten Fehlern in einem Protokollfenster anzeigen. Das Fehlerprotokoll enthält Einzelheiten zum Korrigieren der Fehler, die auf dem jeweils ausgewählten Gerät erkannt wurden. Sie können erst nach dem Beheben der erkannten Fehler mit der Aktualisierung der Firmware auf dem ausgewählten Gerät fortfahren.



The screenshot displays the 'EcoStruxure™ Automation Device Maintenance' application window. The top bar shows '0 Fehler' (0 errors) and '1 Warnungen' (1 warning). The main area is divided into two sections: 'GERÄTELISTE' (Device List) and 'Protokolle' (Logs).

GERÄTELISTE: A table listing devices with columns for Status, Geräte-Handelsreferenz, Dienstendpunkt, Seriennummer, Firmw... Version, Sicher..., Modus, Infos zum Aktualisierungscenter, Erweiteru..., and Aktionen. The table shows five devices, including BME NOC0321, 140***, BMEP586040, and two ATV630U07M3 units.

Protokolle: A window showing a log of events. It includes a header with '0 Fehler', '1 Warnungen', and 'Meldungen'. The log table has columns for Datum, Quelle, and Beschreibung. A single entry is visible: '2022-07-15 12:22:31 BMEP581020-test (https://fe80::28014ff:fe28:4142):443) Certificate has changed! -> CN=BMEP581020_21212711508, OU=Schneider Electric Industries SAS, O=SCHNEIDER-ELECTRIC.COM'.

Annotations A and B point to the error/warning status indicators and the log window header, respectively.

Legende	Name	Beschreibung
A	Fehler- und Warnstatus	Zeigt die Anzahl der erkannten Fehler und Warnungen an.
B	Protokolle	Zeigt die Anzahl der erkannten Fehler und Warnungen mit einer Beschreibung an.

Anzeigen des Protokolls mit Fehlern und Warnungen



Schritt	Aktion
1	Klicken Sie in der Symbolleiste auf den Status für Fehler oder Warnungen . Im Fenster Protokolle werden folgende Informationen angezeigt: <ul style="list-style-type: none">Anzahl der erkannten Fehler, Warnungen und InformationenBeschreibung der erkannten Fehler
2	Wählen Sie den Fehler, die Warnmeldung und/oder die Informationsmeldung Ihrer Wahl aus.
3	Klicken Sie auf Speichern , um die ausgewählten Meldungen zu erkannten Fehler und Warnungen sowie die Informationsmeldungen zu speichern.
4	Klicken Sie auf Löschen , um alle Meldungen zu erkannten Fehlern und Warnungen aus dem Protokoll zu löschen.

Erstellung eines neuen Projekts von EcoStruxure Automation Device Maintenance

Vorgehensweise

Mit dieser Funktion können Sie ein neues Projekt von EcoStruxure Automation Device Maintenance erstellen.

Gehen Sie zum Erstellen eines Projekts wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf das Symbol  Ergebnis: Das Dialogfeld Projekt geändert wird angezeigt, wenn ein Projekt geöffnet ist, das geändert und noch nicht gespeichert wurde.
2	Klicken Sie im Dialogfeld Projekt geändert auf Ja , um die Änderungen an dem geöffneten Projekt zu speichern, oder auf Nein , um das Projekt zu schließen, ohne es zu speichern.  Ergebnis: Das geöffnete Projekt wird geschlossen und ein neues Projekt wird geöffnet, das die Registerkarte Geräte/Ladevorgang anzeigt, wobei die Geräteliste leer ist.


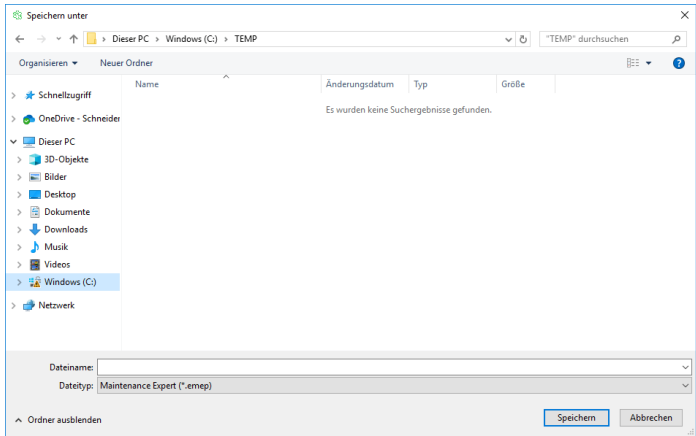

Wenn ein neues Projekt erstellt wird, werden die folgenden Aufgaben automatisch ausgeführt:

- Der Erkennungsmodus wird auf **Manuell** festgelegt.
- Die Einträge in der Protokolldatei werden gelöscht.

Speichern eines Projekts

Diese Funktion ermöglicht Ihnen das Speichern einer Kopie des aktuellen Projekts unter einem anderen Namen oder an einem anderen Speicherort. Der Vorteil ist, dass die Geräte bei jedem Öffnen des Tools EcoStruxure Automation Device Maintenance nicht erneut hinzugefügt werden müssen.


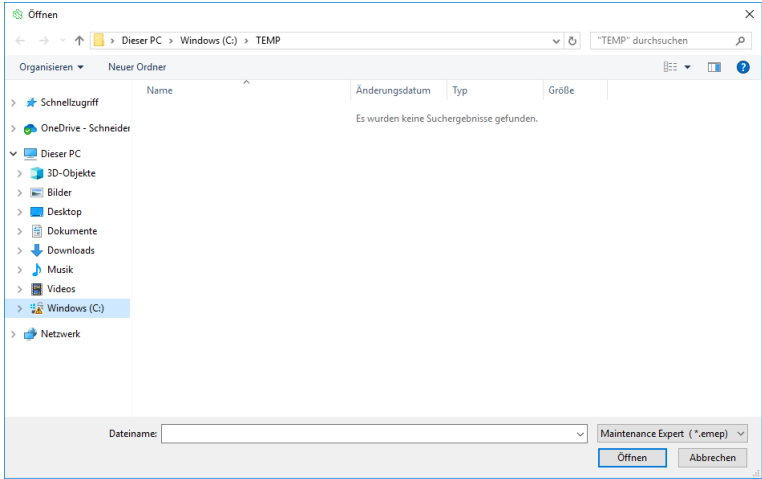

Gehen Sie zum Speichern der Projekteinstellungen wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf das Symbol  .
2	Um die Änderungen im aktuellen Projekt zu speichern, klicken Sie auf Speichern . Um eine Kopie des Projekts zu speichern, klicken Sie auf Speichern unter .
3	Wählen Sie den Ordner aus, in dem Sie das Projekt speichern möchten, und geben Sie den Dateinamen ein. 
4	Klicken Sie auf Speichern und geben Sie das gleiche Passwort in die beiden Felder im Dialogfeld Passwort festlegen ein. 
5	Klicken Sie auf OK , um fortzufahren.

Öffnen eines Projekts

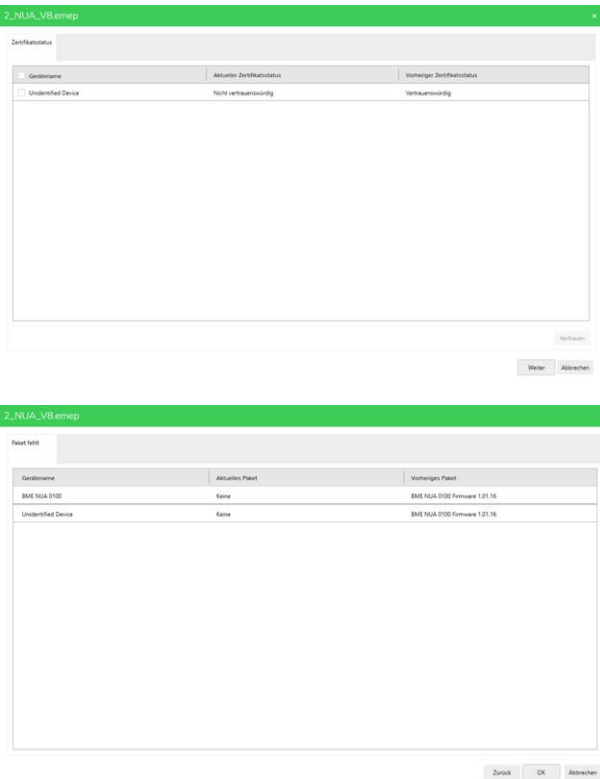
Öffnen eines Projekts

Gehen Sie vor wie folgt, um ein Projekt zu öffnen:

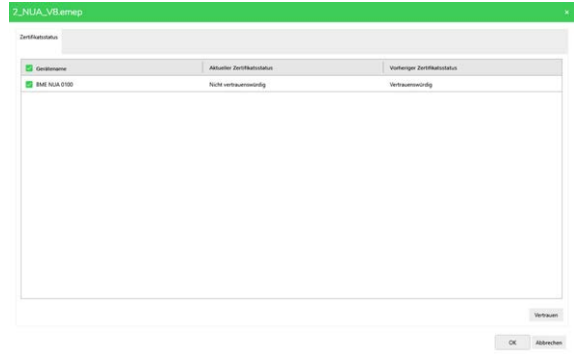
Schritt	Aktion
1	<p>Klicken Sie auf das Symbol .</p> 
2	<p>Wählen Sie den Ordner und das Projekt aus. Klicken Sie auf Öffnen und geben Sie das Passwort ein.</p> 
3	<p>Klicken Sie auf OK, um das Projekt zu öffnen.</p>

Vorgehensweise für auf einem anderen Computer erstellte Projektdateien

Wenn Sie versuchen, eine Projektdatei zu öffnen, die auf einem anderen Computer erstellt wurde, zeigt das Tool optional die Abweichungen zwischen Zertifikatsvertrauensstatus und Paketverfügbarkeit an.



Gehen Sie in diesem Fall folgendermaßen vor:


Schritt	Aktion
4	Wählen Sie die Geräte aus, denen Sie vertrauen möchten, und klicken Sie auf Vertrauen .
5	Klicken Sie auf Weiter . 
6	Klicken Sie auf OK , um das Projekt mit fehlenden Paketen zu öffnen, oder klicken Sie auf Abbrechen .

Optionsschritt für Projektdateien mit nicht identifizierten Geräten

Wenn Sie versuchen, Projektdateien zu öffnen, die mit EcoStruxure Automation Device Maintenance V3.0 und früheren Versionen erstellt wurden, die Geräte ohne Handelsreferenz enthalten, wird ein Dialogfeld angezeigt, in dem Sie zur Auswahl einer Handelsreferenz für jedes unbekannte Gerät in der Liste aufgefordert werden:

Unidentified_3.0.1.emep

Das Projekt enthält Geräte mit einer unbekannten Bestellreferenz.
Prüfen Sie die nachstehende Standardauswahl oder wählen Sie eine andere Bestellreferenz in der Dropdown-Liste aus.

 Das Projekt wurde höchstwahrscheinlich mit einer älteren Version von EcoStruxure Automation Device Maintenance erstellt.
Die Option zum manuellen Hinzufügen nicht identifizierter Geräte wird mit dieser Version nicht mehr unterstützt.

Dienstendpunkt	Handelsreferenz
COM3/255	ATV***
mbap://145.0.0.1:502	ATV***
mbap://145.0.0.2:502	ATV***

Hinweis: Modernisiert = Markteinführung nach 2019
Weitere Informationen hierzu finden Sie im [Produktkatalog von Schneider Electric](#).

OK Abbrechen

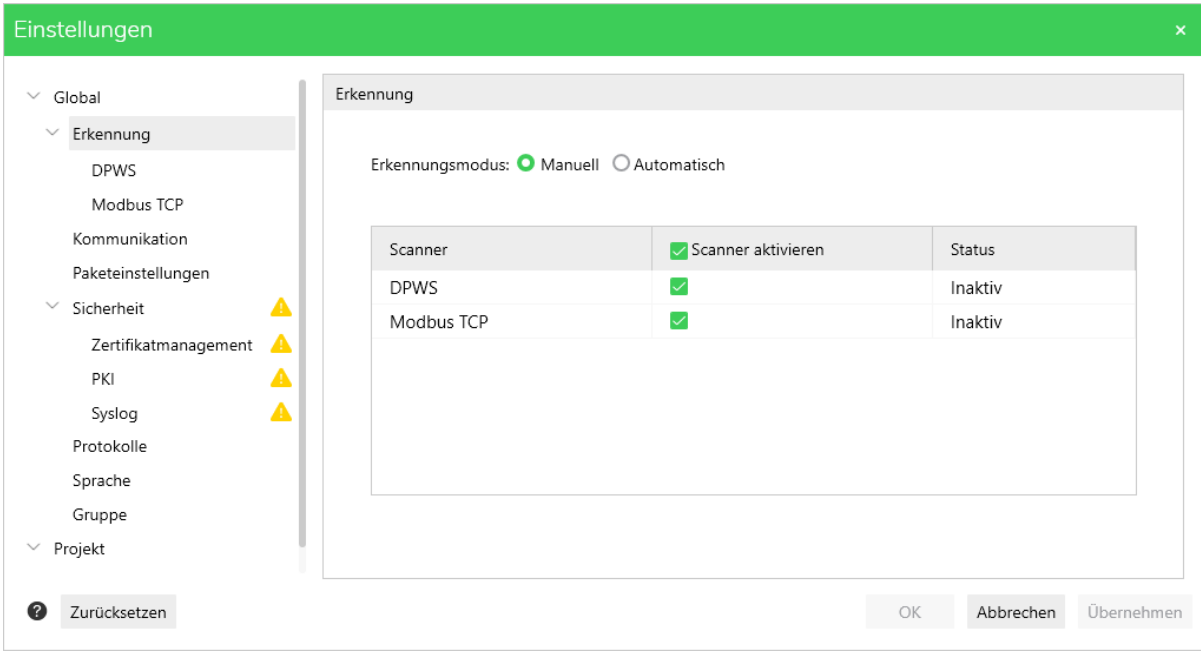
Wählen Sie die gewünschten Handelsreferenzen aus und klicken Sie auf **OK**, um das Projekt zu öffnen.

Konfiguration des EcoStruxure Automation Device Maintenance-Tools

Konfiguration des Geräteerkennungsmodus

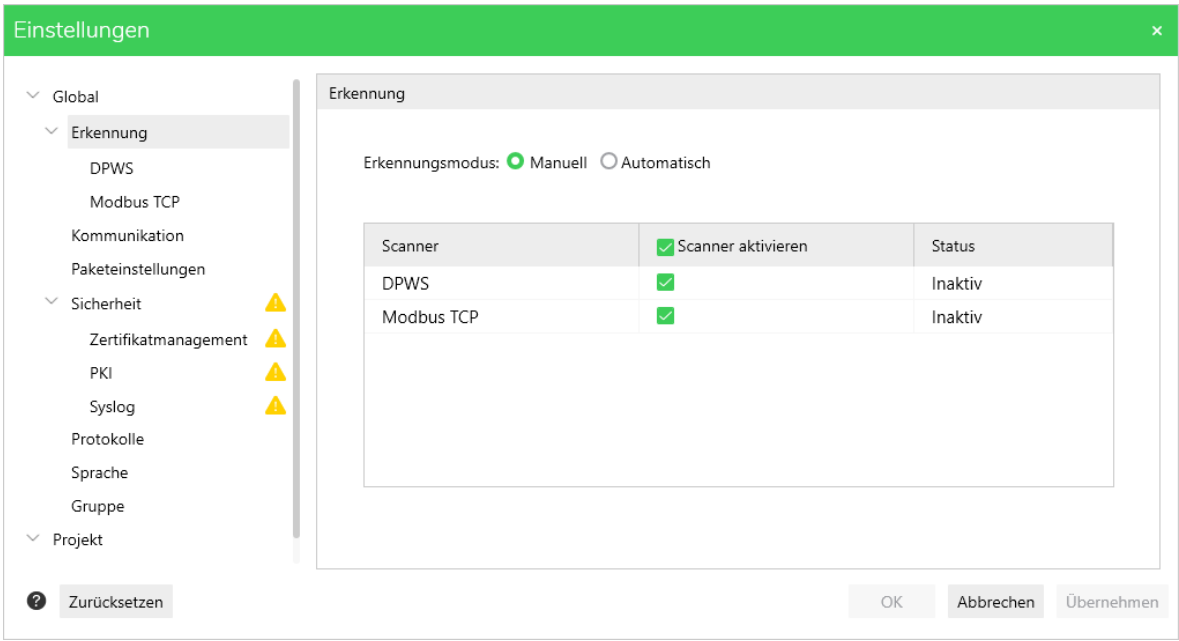
Konfigurieren des automatischen Erkennungsmodus

Sie haben die Wahl zwischen zwei Geräteerkennungsmethoden: **Automatisch** oder **Manuell**. Bei der Auswahl der Option **Automatisch** sendet das Tool in regelmäßigen Abständen im Hintergrund Informationen über das Netzwerk und empfängt Informationen von antwortenden Geräten.

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	<p>Klicken Sie auf die Option Erkennung.</p> 
3	Wählen Sie den Modus Automatisch aus.
4	Wählen Sie die Scanner aus, die für die Erkennung verwendet werden sollen. Verwenden Sie diese Einstellung, um das Scannen von Geräten zu verhindern, die bei diesem Vorgang ausgespart werden sollen.
5	Klicken Sie auf Anwenden und dann auf OK .

Konfigurieren der manuellen Erkennungsmethode

Wählen Sie die Erkennungsmethode **Manuell** aus, um nach Bedarf die Geräte zu identifizieren, die mit dem Netzwerk verbunden sind.

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Klicken Sie auf die Option Erkennung . 
3	Wählen Sie den Modus Manuell aus.
4	Wählen Sie die Scanner aus, die für die Erkennung verwendet werden sollen. Verwenden Sie diese Einstellung, um das Scannen von Geräten zu verhindern, die bei diesem Vorgang ausgespart werden sollen.
5	Klicken Sie auf Anwenden und dann auf OK .

Konfiguration des Modbus TCP-Scanners

Überblick

Der **Modbus TCP**-Scanner sendet Modbus-Requests mit dem Funktionscode 43 an alle IP-Adressen in einem Bereich, der über eine **IP-Startadresse** und eine **IP-Endadresse** definiert ist.

Sie können folgende **Modbus TCP**-Parameter konfigurieren:

Element	Standardwert	Beschreibung
Bereich IP-Adresse :		
Parameter Bereichsname	–	Optionaler Name des Adressbereichs.
Parameter IP-Startadresse	127.0.0.1	Erste Adresse im gescannten Adressbereich.
Parameter IP-Endadresse	127.0.0.1	Letzte Adresse im gescannten Adressbereich.
Schaltfläche Importieren	–	Klicken Sie auf die Schaltfläche Importieren , um eine Konfigurationsdatei zu importieren, die im .csv-Format verfügbar ist (siehe das Beispiel für eine Import-Konfigurationsdatei unten, Seite 34). HINWEIS: Dieser Befehl überschreibt die vorhandenen Konfigurationseinstellungen. Sichern Sie unbedingt vorher Ihre Einstellungen. Ergebnis: Das Windows Dialogfeld Datei öffnen wird geöffnet und Sie können das Netzwerk nach der csv-Datei durchsuchen. Klicken Sie auf Öffnen , um die Konfigurationseinstellungen aus der Datei zu importieren. Um die neuen Einstellungen anzuwenden, klicken Sie auf Anwenden oder auf OK .
Schaltfläche + Hinzufügen	–	Klicken Sie auf die Schaltfläche + Hinzufügen , um einen neuen Adressbereich zu erstellen. Ergebnis: Eine neue Zeile wird in die Tabelle eingefügt mit: Bereichsname = Standard IP-Startadresse = 127.0.0.1 IP-Endadresse = 127.0.0.1
Kontrollkästchen	–	Aktivieren/deaktivieren Sie ein Kontrollkästchen, um den ausgewählten Bereich für den Modbus-Scan ein-/auszuschließen.
Papierkorb-Schaltfläche	–	Klicken Sie auf die Papierkorb-Schaltfläche, um den ausgewählten Bereich (z. B. eine Zeile in der Tabelle) zu entfernen.
Bereich Erweiterte Einstellungen :		
Parameter Start-Port	502	Erster Port im gescannten Portbereich.
Parameter End-Port	502	Letzter Port im gescannten Portbereich.
Parameter Timeout	4000	Maximale Wartezeit zwischen dem Senden eines Pings an das Gerät und dem Empfang einer Antwort.
Parameter Einheits-ID	255	Modbus-Einheits-ID, die für den Zugang zum Gerät verwendet wird.

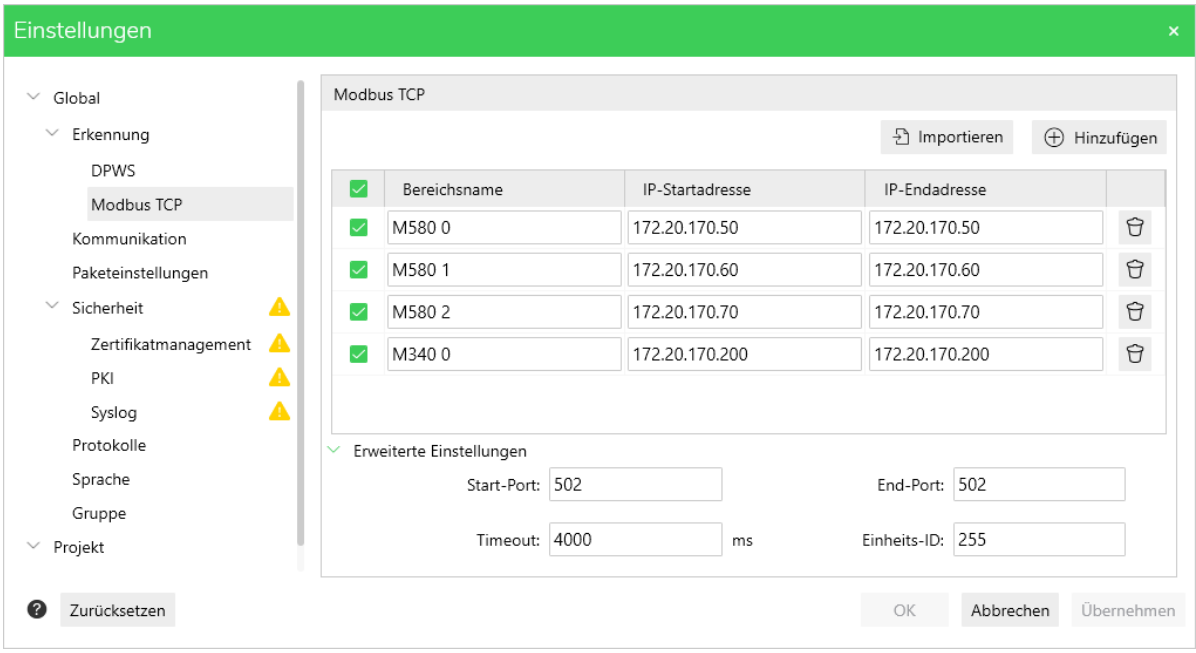
Beispiel für eine Import-Konfigurationsdatei

Das Format der Konfigurationsdatei (.csv-Datei) sollte dem folgenden Beispiel entsprechen:

```
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
```

Konfigurieren des Modbus TCP-Scanners

Gehen Sie zum Konfigurieren des **Modbus TCP**-Scanners wie folgt vor:

Schritt	Aktion
1	Erweitern Sie das Menü Erkennung auf der Seite Einstellungen .
2	Wählen Sie den Knoten Modbus TCP aus.
3	Klicken Sie in der Ansicht Modbus TCP auf der rechten Seite auf die Schaltfläche Hinzufügen , um einen neuen Adressbereich zu erstellen.
4	<p>Klicken Sie auf die Schaltfläche Importieren, um eine Konfigurationsdatei zu importieren oder um die folgenden Parameter zu konfigurieren:</p> <ul style="list-style-type: none">• Bereichsname• IP-Startadresse• IP-Endadresse• Start-Port• End-Port• Timeout• Einheits-ID 
5	Klicken Sie auf Anwenden , um die Modbus TCP-Einstellungen anzuwenden, oder auf OK , um alle Änderungen der Anwendungseinstellungen zu übernehmen und das Dialogfeld Einstellungen zu schließen.

Konfiguration des DPWS-Scanners

Überblick

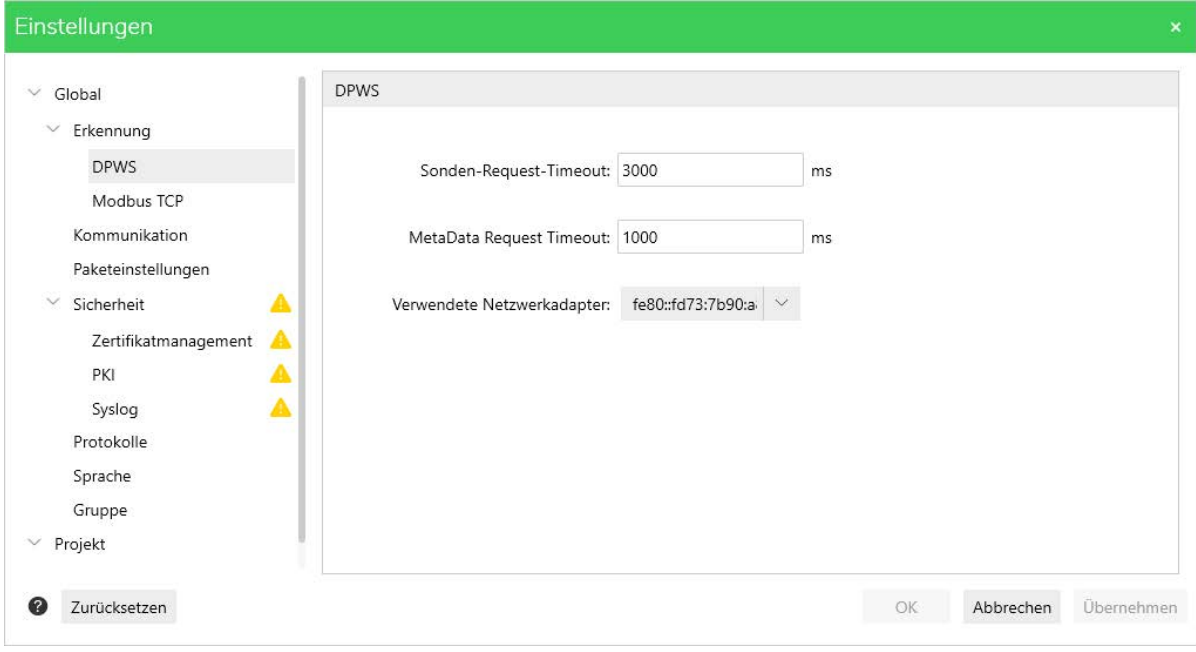
Der **DPWS**-Scanner ist eine clientseitige Implementierung des **DPWS**-Standards, der die Erkennung DPWS-kompatibler Geräte ermöglicht.

Weitere Informationen zu den DPWS-Standards finden Sie auf <http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>.

Sie können folgende **DPWS**-Parameter konfigurieren:

Parameter	Standardwert	Beschreibung
Sonden-Request-Timeout	3000 ms	Maximale Wartezeit zwischen dem Senden eines Sonden-Requests und dem Empfang entsprechender Antworten von den Geräten.
MetaData Request Timeout	1000 ms	Maximale Wartezeit zwischen dem Senden eines Metadaten-Requests und dem Empfang entsprechender Antworten von den Geräten.
Verwendete Netzwerkadapter	–	Liste der Netzwerkadapter, die für das Senden der DPWS -Sonden-Requests verwendet werden.

Gehen Sie zum Konfigurieren des **DPWS**-Scanners wie folgt vor:

Schritt	Aktion
1	Erweitern Sie das Menü Erkennung auf der Seite Einstellungen .
2	<p>Wählen Sie DPWS aus und geben Sie die folgenden Details ein:</p> <ul style="list-style-type: none"> • Sonden-Request-Timeout • MetaData Request Timeout • Verwendete Netzwerkadapter 
3	Klicken Sie auf Anwenden und dann auf OK .

Konfiguration der Kommunikationseinstellungen

Überblick

Sie können die folgenden Kommunikationseinstellungen für die Kommunikation zwischen EcoStruxure Automation Device Maintenance und Geräten konfigurieren:


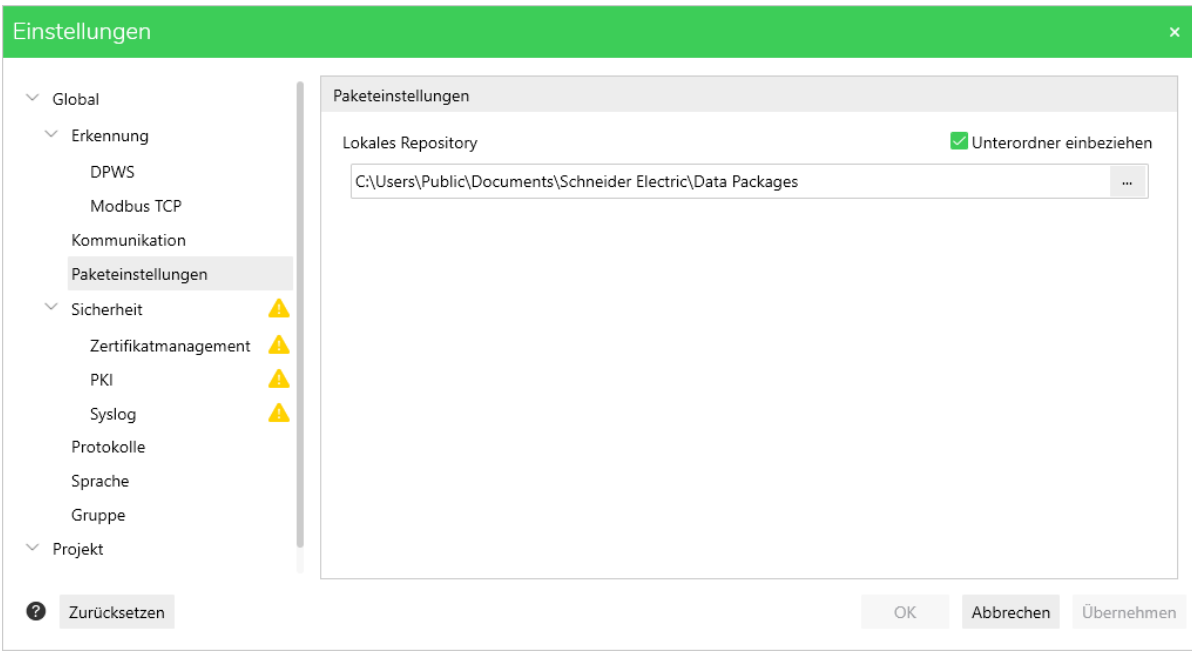
Parameter	Standardwert	Beschreibung
Bereich Timeout :		
Timeout	6000 ms	Maximale Wartezeit nach von EcoStruxure Automation Device Maintenance gesendeten/empfangenen Requests/Antworten (zum Beispiel Firmwareaktualisierungen, Festlegen der IP-Konfiguration). Informationen zu Timeouts bei Erkennungs-Requests finden Sie im Kapitel zum Modbus TCP-Scanner, Seite 34 und zum DPWS-Scanner, Seite 36.
Bereich Automatische Gerätestatusabfrage : Über diese Parameter wird definiert, wie häufig Abfrage-Requests an erkannte Geräte gesendet werden, um den Gerätestatus, Seite 21 auf dem neuesten Stand zu halten:		
Frequenz (hohe Priorität):	3000 ms	Abfragen mit hoher Priorität werden verwendet, wenn Firmwareaktualisierungen durchgeführt werden. Dadurch kann die Erkennung des Geräts nach einem Neustart beschleunigt werden.
Frequenz (niedrige Priorität):	10.000 ms	Im Normalbetrieb wird eine niedrige Priorität mit weniger häufigen Abfragezyklen verwendet.

Konfiguration der Speicherorte für Pakete

Sie können den Pfad der verfügbaren Firmwaredatenpakete im Tool konfigurieren. Dies ermöglicht die Aktualisierung der Firmwareversionen des Geräts. Darüber hinaus wird die spezifische Handelsreferenz, die von jedem Datenpaket bereitgestellt wird, zur Liste **Handelsreferenz** im Dialogfeld **Gerät hinzufügen**, Seite 23 hinzugefügt.

Ändern der Speicherorte für Pakete

Gehen Sie zum Ändern des Speicherorts für ein Paket wie folgt vor:


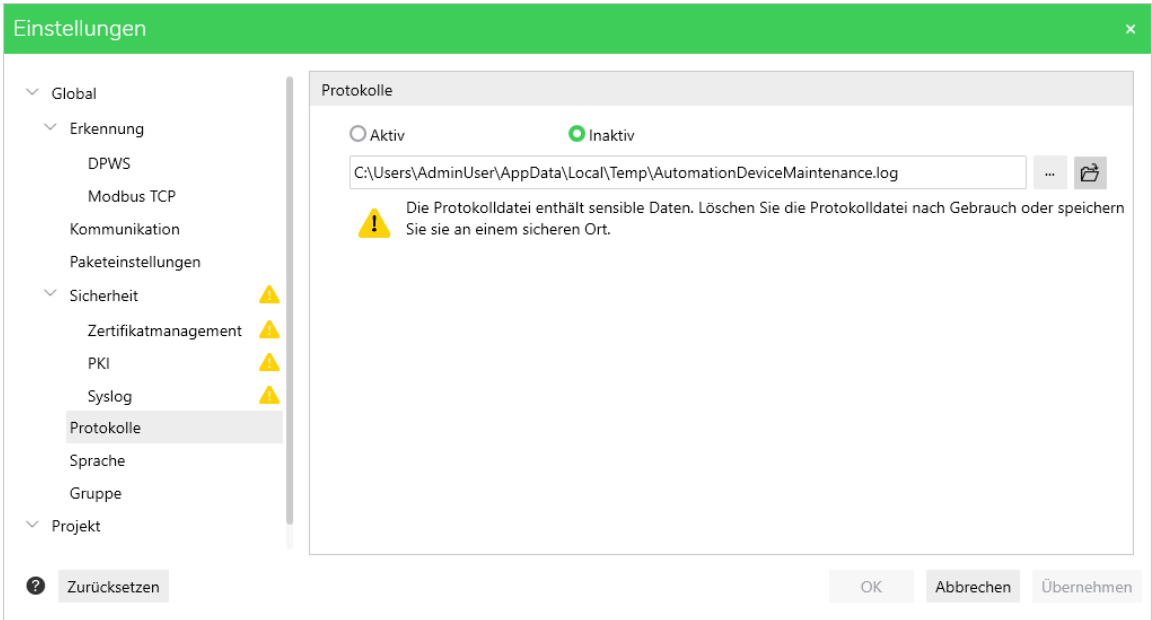
Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Paketeinstellungen aus.
3	Wählen Sie den Pfad aus, um den Speicherort für Lokales Repository zu ändern.
4	<p>Klicken Sie auf das Symbol  und wählen Sie den Zielordner aus, um den Pfad zu ändern.</p> 
5	Klicken Sie auf Anwenden und dann auf OK .

Anzeigen der Protokolldateien

Sie können die gespeicherten Protokolle anzeigen und mit Bezug auf das ausgewählte Gerät analysieren.

Gehen Sie zum Anzeigen der Protokolle wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Startseite (Home).
2	Wählen Sie die Option Protokolle aus.
3	Setzen Sie die Protokollerstellung auf Aktiv/Inaktiv .
4	Wählen Sie den Pfad, um den Speicherort für die Protokolldatei zu ändern.

Schritt	Aktion
5	<p>Klicken Sie auf das Symbol  und wählen Sie den Zielordner aus, um den Pfad zu ändern.</p>  <p>HINWEIS: Weitere Informationen zur Benachrichtigung zur Cybersicherheit finden Sie unter Empfehlung zur verbesserten Cybersicherheit, Seite 68.</p>
6	Klicken Sie auf Übernehmen und dann auf OK .

Konfigurieren der Sprache

Sie können die Sprache wählen, in der das Tool EcoStruxure Automation Device Maintenance auf dem Bildschirm erscheinen soll.

Folgende Sprachen werden unterstützt:

- English
- Deutsch
- Französisch
- Spanisch
- Italienisch
- Chinesisch

Gehen Sie zum Definieren der Sprache wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Sprache .
3	<div>Klicken Sie in der Dropdown-Liste auf Sprache wählen, um die gewünschte Sprache auszuwählen.</div> <div></div>
4	<div>Klicken Sie auf Übernehmen und dann auf OK.</div> <div>HINWEIS: Starten Sie EcoStruxure Automation Device Maintenance erneut, um die Spracheinstellungen anzuwenden.</div>

Zurücksetzen von Anwendungseinstellungen

Überblick

Die Dialogfelder im Menü **Einstellungen** enthalten in der unteren linken Ecke die Schaltfläche **Zurücksetzen**.

Klicken Sie auf die Schaltfläche **Zurücksetzen**, um die Werte aller Anwendungseinstellungen, die Sie über das Menü **Einstellungen** konfiguriert haben, auf ihre Standardwerte zurückzusetzen.

Konfiguration von Sicherheitsfunktionen

Überblick

Die Best Practices and Lösungen zur Cybersicherheit werden kontinuierlich in Übereinstimmung mit den jeweils neuesten Informationen überarbeitet. Im Rahmen des Entwicklungsprozesses integriert Schneider Electric stets die neuesten Erkenntnisse und Verfahren, um die Produkte widerstandsfähig gegenüber Cyberattacken zu machen. Der bei der Entwicklung berücksichtigte Sicherheitsaspekt bedeutet die Implementierung von Mechanismen zur Begrenzung von Bedrohungen, Reduzierung ausnutzbarer Schwachstellen und Verteidigung gegen vermeidbarer Datenschutzverletzungen und Cyberattacken.

HINWEIS:

Um die Sicherheit und den Schutz Ihrer Schneider Electric-Produkte zu gewährleisten, ist es in Ihrem besten Interesse, die bewährten Methoden im Bereich der Cybersicherheit umzusetzen, wie im Dokument zu den *Best Practices zur Cybersicherheit* auf der [Schneider Electric website](#) angegeben.

Aufgrund der rapide zunehmenden Vernetzung von Maschinen und Anlagen nehmen auch die potenziellen Bedrohungen rapide zu. Deshalb sind alle möglichen Sicherheitsmaßnahmen mit Bedacht zu berücksichtigen.

Sicherheitsmaßnahmen sind erforderlich, um Daten und Kommunikationskanäle vor unberechtigt Zugriff zu schützen.

HINWEIS: Bevor Sie Sicherheitsfunktionen konfigurieren, wenden Sie sich an Ihren Sicherheitsadministrator, um sicherzustellen, dass Sie die richtigen Sicherheitseinstellungen verwenden.

Sicherheitsfunktionen

Überblick

EcoStruxure Automation Device Maintenance unterstützt die folgenden Sicherheitsfunktionen:

- Verschlüsselte Kommunikation mit digitalen Zertifikaten in einer Public-Key-Infrastruktur (PKI).
- Handhabung digital signierter Pakete von Schneider Electric Data Package Secure (SEDPS).
- Syslog-Netzwerkprotokoll.

Aktivieren / Deaktivieren des Schutzmodus

Wenn Sie innerhalb eines geschützten Netzwerks arbeiten und keine Sicherheitsfunktionen verwenden, können die Benachrichtigungen zu Sicherheitsfunktionen (z. B. die gelben Ausrufezeichen) über die Option **Sicherheit** auf der Seite **Einstellungen** deaktiviert werden.

The screenshot shows the 'Einstellungen' (Settings) window. The left sidebar has a tree view with categories: Global, Erkennung, Kommunikation, Paketeinstellungen, Sicherheit (selected), and Projekt. Under 'Sicherheit', there are sub-items: Zertifikatmanagement, PKI, Syslog, Protokolle, Sprache, and Gruppe. The main content area is titled 'Sicherheit' and contains the 'Schutzmodus' section. It has two radio buttons: 'Standardschutz' (selected) and 'Kein Schutz'. Below this is the 'Sicherheitskonfigurationsdatei importieren:' section, which includes a text input field 'Datei auswählen', a three-dot menu icon, and an 'Importieren' button. At the bottom of the window, there are buttons for 'Zurücksetzen', 'OK', 'Abbrechen', and 'Übernehmen'.

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Sicherheit aus.
3	Wählen Sie die Option aus, um den Schutzmodus zu aktivieren und Benachrichtigungen zu den Sicherheitsfunktionen anzuzeigen.

Importieren einer Sicherheitskonfigurationsdatei

Mit EcoStruxure Automation Device Maintenance können Sie Sicherheitskonfigurationseinstellungen importieren, die Sie global für Ihr Netzwerk in der Anwendung EcoStruxure Cybersecurity Admin Expert konfiguriert haben. Wenn diese Einstellungen als Datei verfügbar sind, importieren Sie die Datei wie folgt:

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Sicherheit aus.
3	Klicken Sie im Bereich Sicherheitskonfigurationsdatei importieren auf die Schaltfläche Importieren , um zur Sicherheitskonfigurationsdatei zu navigieren.
4	Klicken Sie auf Öffnen , um die Sicherheitskonfigurationseinstellungen aus der Datei zu importieren.

Um die Sicherheitskonfigurationsdatei zu aktualisieren, verwenden Sie das **Aktualisierungszentrum** wie im Kapitel **Aktualisierung der Sicherheitskonfigurationsdatei**, Seite 72 beschrieben.

Verwaltung der Zertifikate

Überblick

Digitale Zertifikate sind für die gesicherte Kommunikation über die entsprechenden Protokolle (z. B. HTTPS) in einer Public-Key-Infrastruktur (PKI) erforderlich.

Im Kontext von TLS können Zertifikate verwendet werden, um die Kommunikationspartner zu überprüfen. Zertifikate werden beim Einrichten einer Verbindung gesendet. Dies ist der sogenannte TLS-Handshake. Das Senden des Zertifikats ist optional für den Client (in diesem Fall: das Anwendungszertifikat von EcoStruxure Automation Device Maintenance), es sei denn, der Server fordert das Client-Zertifikat an. Der Server sendet sein Zertifikat zu jeder Zeit. Nur wenn das Ergebnis der Überprüfung des Zertifikats positiv ist, kann eine Verbindung zum Kommunikationspartner eingerichtet werden.

EcoStruxure Automation Device Maintenance unterstützt die folgenden Zertifikatvertrauensmodi:

- **Manueller Vertrauensmodus:** Sie können den Zertifikaten der Teilnehmer einer gesicherten Kommunikation manuell vertrauen bzw. das Vertrauen aufheben. Der Vertrauensstatus wird auf den Registerkarten **Vertrauenswürdige Zertifikate / Nicht vertrauenswürdige Zertifikate** des Dialogfelds **Zertifikatmanagement**, Seite 46 verwaltet.
- **Allowlist-Vertrauensmodus:** Sie können eine Allowlist mit der Sicherheitskonfigurationsdatei, Seite 42 importieren. EcoStruxure Automation Device Maintenance vertraut dann automatisch den Zertifikaten in dieser Liste.
- **Zertifizierungsstelle (CA) / Registrierungs-Vertrauensmodus:** EcoStruxure Automation Device Maintenance vertraut automatisch den Zertifikaten, die mit den CA-Zertifikaten registriert sind, die im Ordner **Vertrauenswürdige Stammzertifizierungsstellen** des Windows-**Zertifikatspeichers** verfügbar sind.

Hinweise zur Verwendung von Zertifikaten

Beachten Sie Folgendes, wenn Sie Zertifikate für sichere Verbindungen verwenden:

- Zertifikate müssen verwaltet werden, da sie eine begrenzte Gültigkeit haben und daher in regelmäßigen Abständen aktualisiert werden müssen. Berücksichtigen Sie dies im Hinblick auf den Lebenszyklus Ihrer Maschine oder Steuerung.
- Die Daten- und Uhrzeiteinstellungen des Windows-PC werden zur Prüfung verwendet, ob das Zertifikat noch gültig ist. Überprüfen Sie die Einstellungen in regelmäßigen Abständen über Windows **Start > Einstellungen > Uhrzeit & Sprache > Datum & Uhrzeit**.
- Wenn der PC, auf dem EcoStruxure Automation Device Maintenance ausgeführt wird, permanent offline ist, müssen Sie die **Zertifikatsperrliste** (CRL: Certificate Revocation List) in regelmäßigen Abständen manuell aktualisieren. Um dies zu erreichen, stellen Sie eine Verbindung zu Ihrem CRL-Verteilungspunkt her, laden Sie die aktuelle Zertifikatsperrliste herunter und installieren Sie sie auf Ihrem PC.

Wenden Sie sich an den Sicherheitsadministrator, um die richtige URL des CRL-Verteilungspunkts zu erhalten.

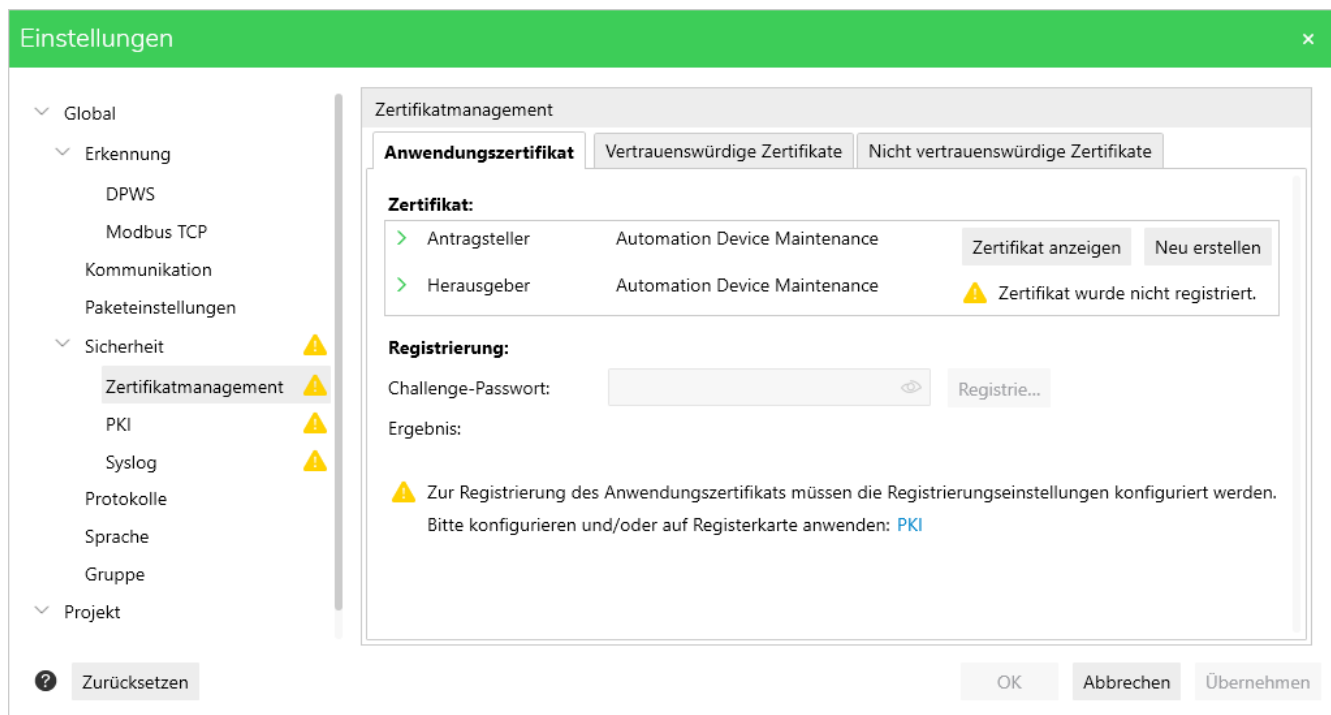
- Sie können Zertifikate in EcoStruxure Automation Device Maintenance auch als nicht vertrauenswürdig deklarieren, z. B. im Dialogfeld **Zertifikatmanagement**, Seite 46.

Dialogfeld Zertifikatmanagement

Nach der Erstinstallation steht ein selbstsigniertes Standard-Anwendungszertifikat für EcoStruxure Automation Device Maintenance zur Verfügung.

Das Dialogfeld **Zertifikatmanagement** enthält die folgenden Optionen für das Anwendungszertifikat:

- Neuerstellen des selbstsignierten Anwendungszertifikats und Zuweisen einzelner Eigenschaften (siehe Wiederherstellen des selbstsignierten Anwendungszertifikats, Seite 44).
- Das Anwendungszertifikat wird registriert, um die digitale Signatur einer Zertifizierungsstelle zuzuweisen und eine Vertrauenskette zu erstellen (siehe Registrieren des Anwendungszertifikats, Seite 45).
- Verwalten des Vertrauensstatus der digitalen Zertifikate der Kommunikationspartner (siehe Verwalten des Vertrauensstatus von Zertifikaten, Seite 46).



Wiederherstellen des selbstsignierten Anwendungszertifikats

Gehen Sie wie folgt vor, um das standardmäßige Anwendungszertifikat neu zu erstellen und Ihre individuellen Eigenschaften zuzuweisen:

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Sicherheit > Zertifikatmanagement aus.
3	Klicken Sie in der Registerkarte Anwendungszertifikat auf die Schaltfläche Neu erstellen . Ergebnis: Das Dialogfeld Zertifikat erstellen wird geöffnet.
4	Geben Sie die Eigenschaften ein, die Sie dem Zertifikat zuweisen möchten, und klicken Sie auf die Schaltfläche OK . Ergebnis: Das selbstsignierte Zertifikat von EcoStruxure Automation Device Maintenance wird für die anderen Teilnehmer der Kommunikation mit den von Ihnen definierten Eigenschaften angezeigt.

Registrieren des Anwendungszertifikats

Um eine Vertrauenskette zu erstellen, muss das Anwendungszertifikat EcoStruxure Automation Device Maintenance registriert und von einer Zertifizierungsstelle (CA) digital signiert werden.

Um das Zertifikat zu registrieren, konfigurieren Sie zunächst die **Registrierungseinstellungen** wie in der Option **Einstellungen > Sicherheit > PKI**, Seite 48 angegeben.

Führen Sie dann die folgenden Schritte aus, um das Anwendungszertifikat für EcoStruxure Automation Device Maintenance zu registrieren:

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Sicherheit > Zertifikatmanagement aus.
3	<p>Stellen Sie auf der Registerkarte Anwendungszertifikat sicher, dass das Anwendungszertifikat weiterhin selbstsigniert und noch nicht registriert ist:</p> <ul style="list-style-type: none"> Im Bereich Zertifikat zeigen sowohl der Betreff als auch der Aussteller denselben Inhalt an: Automation Device Maintenance. Die Meldung Zertifikat wurde nicht registriert wird in der Zeile Aussteller angezeigt.
4	Geben Sie Ihr Passwort für die Zertifizierungsstelle in das Textfeld Challenge-Passwort ein. Dieses Passwort wird zur Autorisierung der Registrierungsanforderung verwendet. Detaillierte Informationen erhalten Sie von Ihrem Administrator für Industrienetzwerke.
5	<p>Klicken Sie auf Registrieren.</p> <p>Ergebnis: EcoStruxure Automation Device Maintenance sendet eine Zertifikatsignaturanforderung vom Anwendungszertifikat zusammen mit dem Challenge-Passwort an die Zertifizierungsstelle. Wenn das Passwort nicht richtig ist, wird die Meldung Registrierung nicht erfolgreich zurückgegeben.</p> <p>HINWEIS: Dieses Verfahren ersetzt das selbstsignierte Standard-Anwendungszertifikat durch ein neues signiertes Zertifikat. Der Austausch kann nicht rückgängig gemacht werden.</p>
6	<p>Überprüfen Sie, ob der Prozess erfolgreich abgeschlossen wurde:</p> <ul style="list-style-type: none"> Ergebnis: Registrierung war erfolgreich wird auf der Registerkarte Anwendungszertifikat angezeigt. Auf der Registerkarte Allgemein des Dialogfelds Zertifikatinformationen wurde der Eintrag Aussteller zum Namen der Zertifizierungsstelle geändert, beispielsweise INT-DEV-SUB-CA. Die Registerkarte Zertifizierungspfad des Dialogfelds Zertifikatinformationen zeigt die Stamm-CA und die untergeordneten Zertifizierungsstellen in einer hierarchischen Struktur an, abhängig von Ihrer PKI-Konfiguration. Das letzte Entitätszertifikat am unteren Ende der hierarchischen Struktur ist das Zertifikat von EcoStruxure Automation Device Maintenance mit den folgenden Einträgen: <ul style="list-style-type: none"> CN (Common Name) = Automation Device Maintenance O (Organization) = Schneider Electric

Verwalten des Vertrauensstatus von Zertifikaten

Auf den Registerkarten **Vertrauenswürdige Zertifikate** und **Nicht vertrauenswürdige Zertifikate** des Dialogfelds **Zertifikatmanagement** können Sie den Vertrauensstatus von Zertifikaten verwalten, die in EcoStruxure Automation Device Maintenance verfügbar sind.

Auf beiden Registerkarten wird jedes Zertifikat mit den folgenden Informationen angezeigt:

Komponente	Beschreibung
Betreff	Enthält allgemeine Informationen zum Zertifikat: <ul style="list-style-type: none"> • CN = Allgemeiner Name (Common Name) • OU = Organisationseinheit (Organization Unit)
Gerätename	Gibt den Gerätenamen an, der in der GERÄTELISTE auf der Registerkarte Geräte/Ladevorgang angezeigt wird. Wenn das Zertifikat nicht zu einem Gerät gehört, wird N/A angezeigt.
Dienstendpunkt	Die Informationen zum Dienstendpunkt werden für Geräte bereitgestellt, die in dieser Sitzung von EcoStruxure Automation Device Maintenance verwendet werden. Wenn das Zertifikat nicht zu einem Gerät gehört, wird N/A angezeigt.
Aktion	Ermöglicht Ihnen das Öffnen des Dialogfelds Zertifikatinformationen über den Link Zertifikat anzeigen .
Zertifikatsstatus	Gibt den Status des Zertifikats an: <ul style="list-style-type: none"> • Vertrauenswürdige • Nicht vertrauenswürdige

Sie können folgende Aktionen für Zertifikate ausführen:

- Um die Vertrauenswürdigkeit von Zertifikaten aufzuheben, wählen Sie eines oder mehrere Zertifikate auf der Registerkarte **Vertrauenswürdige Zertifikate** aus und klicken Sie auf die Schaltfläche **Nicht vertrauen**.
- Um Zertifikaten zu vertrauen, wählen Sie eines oder mehrere Zertifikate auf der Registerkarte **Nicht vertrauenswürdige Zertifikate** aus und klicken Sie auf die Schaltfläche **Vertrauen**. Wenn Sie den ausgewählten Zertifikaten vorübergehend vertrauen möchten, wählen Sie die Option **Dieser Sitzung vertrauen** aus.
- Um Zertifikate zu entfernen, wählen Sie eines oder mehrere Zertifikate auf der Registerkarte **Vertrauenswürdige Zertifikate** oder **Nicht vertrauenswürdige Zertifikate** aus und klicken Sie auf die Schaltfläche **Löschen**.


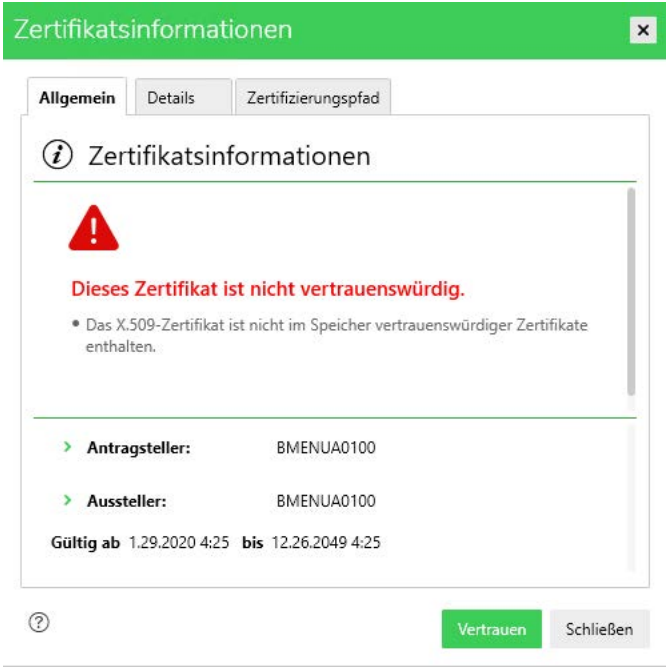
HINWEIS: Zertifikate von Geräten, die in dieser Sitzung von EcoStruxure Automation Device Maintenance verwendet werden, können nicht direkt gelöscht werden. Die Zertifikate werden vorübergehend in die Liste der **Nicht vertrauenswürdigen Zertifikate** verschoben und entfernt, sobald EcoStruxure Automation Device Maintenance geschlossen wird.

HINWEIS: Durch die Ausführung dieses Befehls werden die ausgewählten Zertifikate vom Windows-PC entfernt. Sie werden auch aus dem Windows-**Zertifikatspeicher** entfernt.

Verwalten des Vertrauensstatus von Zertifikaten auf der Registerkarte Geräte/Ladevorgang

Auf der Registerkarte **Geräte/Ladevorgang** können Sie den Zertifikaten von Geräten vertrauen bzw. deren Vertrauenswürdigkeit aufheben.

Gehen Sie wie folgt vor, um dem Gerätezertifikat auf der Registerkarte **Geräte/Ladevorgang** zu vertrauen:

Schritt	Aktion
1	<p>Klicken Sie auf das Symbol Gerätezertifikat  des Geräts.</p>  <p>HINWEIS: Sie können das Serverzertifikat vorübergehend als vertrauenswürdig erklären.</p>
2	Aktivieren Sie das Kontrollkästchen Dem Gerätezertifikat für die aktuelle Sitzung vorübergehend vertrauen .
3	Klicken Sie auf Dem Gerätezertifikat vertrauen .

Gehen Sie wie folgt vor, um die Vertrauenswürdigkeit des Gerätezertifikats auf der Registerkarte **Geräte/Ladevorgang** aufzuheben:

Schritt	Aktion
1	Klicken Sie auf das Symbol Gerätezertifikat  des Geräts.
2	Klicken Sie auf Dem Gerätezertifikat nicht vertrauen .

Verwalten der Public Key-Infrastruktur (PKI)

Einstellungen für die Registrierung des Anwendungszertifikats

Wenn die Option **Sicherheit** im Dialogfeld **Sicherheit** der Seite **Einstellungen** aktiviert ist, können Sie im Dialogfeld **PKI** die Verbindung mit der Zertifizierungsstelle (CA) für die Registrierung des Anwendungszertifikats von EcoStruxure Automation Device Maintenance konfigurieren.

Komponente	Beschreibung
Registrierungs-URL	Geben Sie den Uniform Resource Locator (URL) der Zertifizierungsstelle (CA) ein, die das Zertifikat ausstellt.
Aussteller-ID	Geben Sie den Bezeichner des Ausstellers der Zertifizierungsstelle ein.
Timeout	Geben Sie ein Zeitlimit (in Millisekunden) ein, das Ihren Internetübertragungsraten entspricht. Standardwert: 10.000 ms
Nur Signatur überprüfen	Wenn diese Option nicht aktiviert ist, muss das CA-Zertifikat als vertrauenswürdiges Zertifikat im Windows- Zertifikatspeicher verfügbar sein. Wählen Sie diese Option aus, um nur die digitalen Signaturen zu überprüfen.
Schaltfläche Verbindung prüfen	Klicken Sie auf die Schaltfläche Verbindung prüfen , um eine Verbindung zur Website der Zertifizierungsstelle herzustellen.
Schaltfläche Zertifikat anzeigen	Nachdem die Verbindung zur Zertifizierungsstelle erfolgreich hergestellt wurde, wird die Schaltfläche Zertifikat anzeigen angezeigt. Klicken Sie auf die Schaltfläche, um das Dialogfeld Zertifikatinformationen zu öffnen und die Attribute des Zertifikats zu überprüfen, um sicherzustellen, dass Sie mit der richtigen Zertifizierungsstelle verbunden sind.

Wenn die Verbindung mit der Website der Zertifizierungsstelle erfolgreich hergestellt wurde, wählen Sie die Option **Sicherheitszertifikat-Management** > , und fahren Sie mit der Registrierung des Anwendungszertifikats fort.

Aktivierung der Syslog-Meldungsprotokollierung


Überblick

Das Dialogfeld **Syslog** ermöglicht Ihnen die Aktivierung der Funktion syslog und die Konfiguration von EcoStruxure Automation Device Maintenance als syslog-Client. EcoStruxure Automation Device Maintenance übergibt dann eine Teilmenge der generierten Protokollmeldungen an den entsprechenden syslog-Server, wobei die in diesem Dialogfeld konfigurierten syslog-Einstellungen verwendet werden.

The screenshot shows the 'Einstellungen' (Settings) window with the 'Syslog' tab selected. The left sidebar lists various settings categories: Global, Erkennung (Detection), DPWS, Modbus TCP, Kommunikation, Paketeinstellungen, Sicherheit (Security), Zertifikatmanagement, PKI, Syslog, Protokolle, Sprache, Gruppe, and Projekt. The 'Sicherheit' category is expanded, and 'Syslog' is highlighted. The main area displays the 'Syslog' configuration. At the top, there are radio buttons for 'Aktivieren' (Activate) and 'Deaktivieren' (Deactivate), with 'Deaktivieren' selected. A yellow warning triangle is next to the 'Deaktivieren' option. Below this, the 'Serveradresse' (Server address) is set to '127.0.0.1' and the 'Port' is '6514'. The 'Netzwerkprotokoll' (Network protocol) section has radio buttons for 'UDP', 'TCP', and 'TLS', with 'TLS' selected. A 'Verbindung prüfen' (Check connection) button is located below the protocol selection. At the bottom of the dialog, there are three buttons: 'Zurücksetzen' (Reset), 'OK', 'Abbrechen' (Cancel), and 'Übernehmen' (Apply).

Aktivieren der Syslog-Meldungsprotokollierung

Gehen Sie wie folgt vor, um die syslog-Funktion zu aktivieren und die Verbindung zum syslog-Server zu konfigurieren:

Schritt	Aktion
1	Klicken Sie auf das Menü Einstellungen am oberen Rand in der Mitte der Home -Seite.
2	Wählen Sie die Option Sicherheit > Syslog aus.
3	Wählen Sie die Option Aktivieren aus, um die syslog-Funktion zu aktivieren.
4	Geben Sie die IP-Adresse Ihres syslog-Servers im Textfeld Serveradresse ein.
5	Geben Sie den Port ein, den der Server auf syslog-Meldungen von den Clients überwacht.
6	Wählen Sie die Option Netzwerkprotokoll aus: <ul style="list-style-type: none"> • UDP (User Datagram-Protokoll) • TCP (Transmission Control-Protokoll) • TLS (Transport Layer Security)
7	<p>Bei TCP- oder TLS-Verbindungen können Sie optional auf die Schaltfläche Verbindung prüfen klicken, um den syslog-Server zu überprüfen.</p> <p>Ergebnisse:</p> <p>Für TCP-Verbindungen: Es wird eine Meldung angezeigt, die angibt, ob eine Serververbindung hergestellt wurde.</p> <p>Für TLS-Verbindungen:</p> <ul style="list-style-type: none"> • Es wird eine Meldung angezeigt, die angibt, ob eine Serververbindung hergestellt wurde. • Ein Symbol zeigt an, ob das Zertifikat des syslog-Servers bereits als vertrauenswürdig deklariert wurde. Wenn das Zertifikat nicht vertrauenswürdig ist, klicken Sie auf das Symbol , um das Dialogfeld Zertifikatinformationen zu öffnen, in dem Sie das Zertifikat überprüfen und als vertrauenswürdig deklarieren können. <p>HINWEIS: Da UDP auf einem verbindungslosen Kommunikationsmodell basiert, kann EcoStruxure Automation Device Maintenance keine Lösung zur Überprüfung der Verbindung bereitstellen. Sie müssen manuell überprüfen, ob syslog-Meldungen auf dem angegebenen Server empfangen werden.</p>

Datenpaket

Registerkarte „Datenpaket“

Unterstützte Datenpakettypen

Folgende Dateitypen werden unterstützt:

- *.fwp
- *.idx
- *.sedp
- *.sedps

Gesicherte Datenpakete

EcoStruxure Automation Device Maintenance unterstützt Datenpakete des Typs *.sedps (Schneider Electric Data Package Secure), die digital signiert sind: Wenn der Schutzmodus aktiviert ist, überprüft EcoStruxure Automation Device Maintenance, ob dieses Paket von einem verifizierten Ursprung stammt, und zeigt Sicherheitsbenachrichtigungen an, wenn die Signatur nicht korrekt ist. Eine allgemeine Beschreibung der Handhabung von Zertifikaten finden Sie in Kapitel [Verwaltung der Zertifikate](#), Seite 43.

Wenn der Schutzmodus aktiviert, Seite 42 ist, gilt Folgendes:

- Die folgenden Paketdateien sind durch das gelbe Benachrichtigungssymbol in der Liste der Pakete auf der Registerkarte **Datenpaket** gekennzeichnet, und die Meldung **Die Vertrauenskette des Pakets kann nicht geprüft werden.** wird auf der rechten Seite angezeigt:
 - Nicht signierte Paketdateien
 - Selbstsignierte Paketdateien
 - Paketdateien, die ein nicht vertrauenswürdiges Stammzertifikat verwenden
- Diese Pakete werden ebenfalls auf der Registerkarte **Geräte/Ladevorgang** durch das gelbe Benachrichtigungssymbol gekennzeichnet.
- Wenn Sie versuchen, mit einem dieser Datenpakete einen Firmwareaktualisierungsprozess durchzuführen, wird der Vorgang angehalten und die Meldung **Vertrauenskette des ausgewählten Pakets kann nicht überprüft werden. Der Download könnte dem Gerät schaden. Möchten Sie fortfahren?** wird im Benachrichtigungsbereich, Seite 67 angezeigt. Lesen Sie sich die Meldung sorgfältig durch und bewerten Sie die Risiken. Nachdem Sie die Meldung bestätigt haben, wird der Vorgang fortgesetzt.
- Wenn Sie versuchen, eine Firmwareaktualisierung mit einem dieser Datenpakete durchzuführen, werden die erkannten Fehler im Fenster **Protokolle**, Seite 68 angezeigt.

HINWEIS

BESCHÄDIGTE GERÄTE

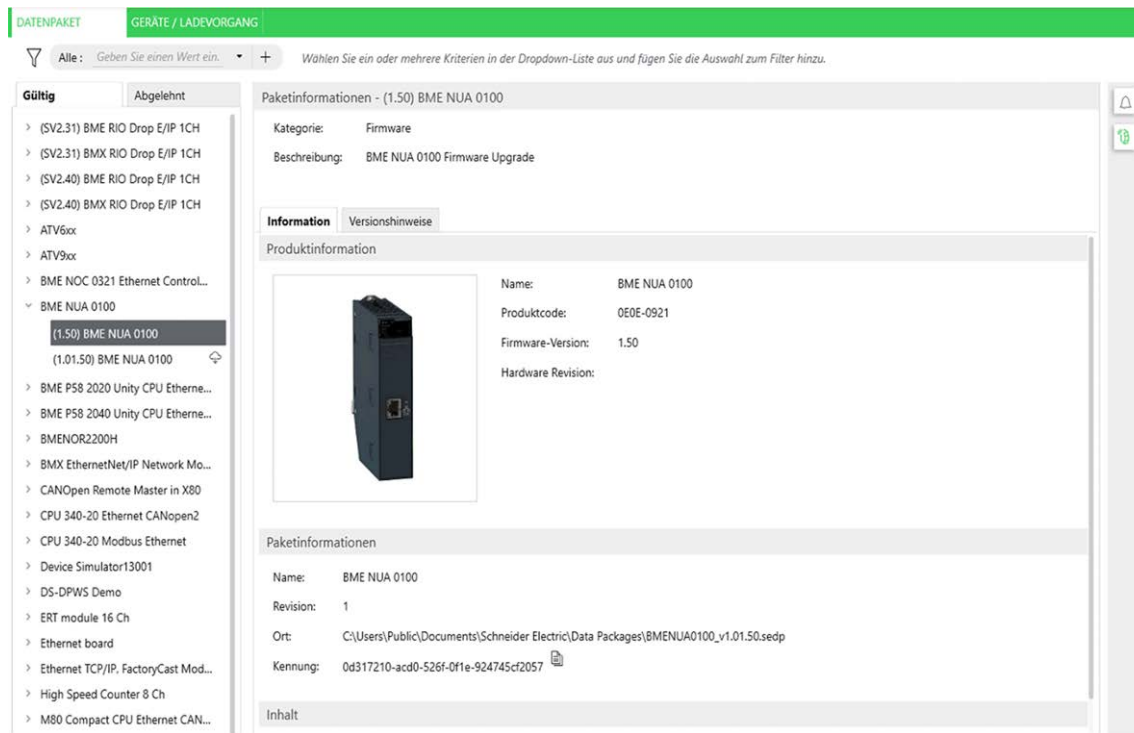
Überprüfen Sie sorgfältig, ob das Datenpaket von einer vertrauenswürdigen Quelle stammt, da das Herunterladen eines manipulierten Datenpakets Ihr Gerät beschädigen kann.

Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.

Übersicht über die Registerkarte Datenpaket

Sie können den Inhalt der Datenpaketbibliothek anzeigen, um nach Details zu einzelnen Paketen und Inhalten zu suchen.

Auf der linken Seite der Registerkarte wird die Liste der lokal verfügbaren Datenpakete gruppiert nach Gerätefamilie angezeigt. Auf der rechten Seite der Registerkarte werden die Details des ausgewählten Pakets angezeigt.




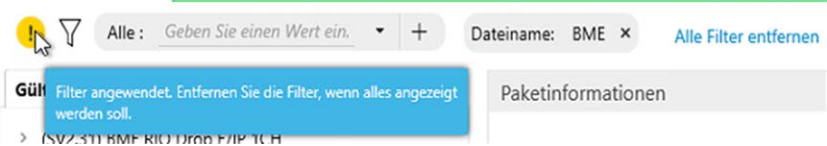
Liste der Datenpakete

Die Liste der Datenpakete auf der linken Seite umfasst zwei Registerkarten:

- Auf der Registerkarte **Gültig** sind die Datenpakete, die lokal auf Ihrem PC verfügbar sind, nach Gerätefamilie gruppiert aufgelistet.
- Auf der Registerkarte **Abgelehnt** sind die Datenpakete aufgelistet, die Sie auf Ihren PC heruntergeladen haben, die aber aus einem beliebigen Grund nicht verarbeitet werden können. Da die Datenpaketdatei möglicherweise beim Downloadvorgang beschädigt wurde, kann es hilfreich sein, wenn Sie sie ein zweites Mal herunterladen. Lässt sich das Problem hiermit nicht beheben, wenden Sie sich zwecks weiterer Unterstützung an Ihren Ansprechpartner bei Schneider Electric.

Filtern der Liste der Datenpakete

Um die Anzahl der in der Liste angezeigten Datenpakete zu reduzieren, können Sie wie folgt Suchkriterien anwenden:

Schritt	Aktion
1	<p>Geben Sie eine Zeichenfolge in das Textfeld Alle ein. Um die Suche auf eine bestimmte Datenpaketeigenschaft zu begrenzen, können Sie die Liste öffnen und ein Suchkriterium auswählen.</p> 
2	<p>Klicken Sie auf die Schaltfläche mit dem Pluszeichen auf der rechten Seite der Suchliste, um mit der Suche zu beginnen.</p> <p>Ergebnis: Die Liste der Datenpakete enthält Einträge, die dem von Ihnen eingegebenen Suchkriterium entsprechen. Links neben dem Suchfeld wird ein gelbes Symbol angezeigt, das darauf hinweist, dass ein Filter angewendet wird und die Liste der Einträge daher auf diejenigen Datenpakete beschränkt ist, die dem Suchkriterium entsprechen.</p> 
3	<p>Wiederholen Sie die Schritte 1 und 2, um einen anderen Filter zu definieren. Die Filter werden mit AND kombiniert.</p> <p>Ergebnis: Die Liste der Datenpakete enthält Einträge, die beiden Suchkriterien entsprechen.</p>
4	<p>Um einen einzelnen Filter zu löschen, klicken Sie auf die Kreuz-Schaltfläche dieses Filters.</p> <p>Um alle von Ihnen definierten Filter zu entfernen, können Sie auch auf den Link Alle Filter entfernen klicken. Daraufhin wird die vollständige Liste der Datenpakete angezeigt.</p>

Paketinformationen

Der Bereich **Paketinformationen** auf der rechten Seite enthält Informationen zu dem in der Liste der Datenpakete ausgewählten Datenpaket.

Der obere Teil enthält die folgenden Informationen:

- **Kategorie**
- **Beschreibung**

Die Registerkarte **Informationen** enthält die folgenden Details:

- Bereich **Produktinformationen**:
 - Abbildung – falls im Datenpaket verfügbar
 - **Name**
 - **Produktcode**
 - **Firmwareversion**
 - **Hardware-Version**
- Bereich **Paketinformationen**:
 - **Name**
 - **Revision**
 - **Position**
 - **Kennung**: Mit der Schaltfläche **In Zwischenablage kopieren** können Sie die Kennungszeichenfolge in die Zwischenablage Ihres PC kopieren.
- Bereich **Inhalt**: Stellt den Inhalt des Datenpakets in einer Liste bereit.

Der Inhalt wird auf der Registerkarte **Versionshinweise** angezeigt, wenn das Datenpaket ein als `ReleaseNotes` bezeichnetes Dokument enthält. Wenn kein derartiges Dokument für das Datenpaket vorhanden ist, ist die Registerkarte leer.


Gerät/Laden

Registerkarte Geräte/Ladevorgang

Überblick

EcoStruxure Automation Device Maintenance zeigt eine Reihe von Geräteeigenschaften (z. B. Gerätename, Dienstendpunkt, Firmwareversion) auf der Registerkarte **Geräte/Ladevorgang** an.


HINWEIS: Die auf dieser Registerkarte angezeigten Informationen werden nur automatisch aktualisiert, wenn der Erkennungsmodus auf **Automatisch**

eingestellt ist. Klicken Sie auf das Symbol  in der Symbolleiste, um die neuesten Werte anzuzeigen.

DATENPAKET	GERÄTE / LADEVORGANG									
GERÄTELISTE	<div> + Hinzufügen 🔌 Verbinden 🔌 Verbindung trennen 🔄 Aktualisierungscenter 👁 Ausblenden 🗑 Entsorgen 🔍 </div>									
<input type="checkbox"/>	Status	Gerätename Handelsreferenz	Dienstendpunkt Seriennummer	Firmw... Version	Sicherhei...	Modus	Infos zum Aktualisierungscenter	Erweiterungen	Aktionen	
<input checked="" type="checkbox"/>		Gerätstandardgruppe (8)								
<input checked="" type="checkbox"/>	●	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-		Erweiterungen	⚠ 🔌 📄 ▶ ⏏ ⌵	
<input type="checkbox"/>	●	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B04	-	-		-	⚠ 🔌 📄 ▶ ⏏ ⌵	
<input type="checkbox"/>	●	ATV930_Spare CR: ATV930D11M3	mbap://172.20.170.208:502 SN: 40211008536202002	3.5IE94B04	-	-		-	⚠ 🔌 📄 ▶ ⏏ ⌵	

Detaillierte Informationen zu den jeweils anzuzeigenden Geräten können Sie dem Kapitel Geräte/Ladevorgang, Seite 21 entnehmen.

Nach der Anmeldung verfügbare Details

Nachdem Sie sich erfolgreich bei einem Gerät angemeldet haben und der Gerätestatus zu grün gewechselt ist, klicken Sie auf die Schaltfläche , um auf die folgenden Befehle für jedes Gerät zuzugreifen:

Befehl	Beschreibung
Optisch	Das Gerät gibt ein optisches Signal aus, damit Sie es in einem Hardware-Rack für Geräte, die diese Funktion unterstützen, ermitteln können.
Optisch und akustisch	Das Gerät gibt ein optisches und ein akustisches Signal aus, damit Sie es in einem Hardware-Rack für Geräte, die diese Funktion unterstützen, ermitteln können.
Eigenschaften	<p>Öffnen ein zusätzliches Dialogfeld mit Eigenschaften, das auf verschiedenen Registerkarten weitere Informationen zu dem Gerät enthält:</p> <ul style="list-style-type: none"> Die Registerkarte Geräteinformationen enthält die folgenden allgemeinen Informationen zum Gerät: <ul style="list-style-type: none"> Produkt-ID Produktname Firmwareversion Hardware-Version Hardware-ID MAC-Adresse Die Registerkarte Gerätestatus enthält Informationen zum aktuellen Status des Geräts. Die Registerkarte Konfiguration enthält Informationen zu den Konfigurationseinstellungen des Geräts. Sofern vom Gerät unterstützt, können auf dieser Registerkarte die Konfigurationseinstellungen bearbeitet werden. <p>HINWEIS: Bei Änderungen an den Konfigurationseinstellungen muss das Gerät möglicherweise neu gestartet werden, was dazu führen kann, dass die Steuerung in den STOP-Modus gesetzt wird. Die Auswirkungen wird durch Meldungen im Benachrichtigungsbereich ausgewiesen. Lesen Sie jede Meldung sorgfältig durch und bestätigen Sie sie nach der Durchführung einer Risikobewertung. Nachdem Sie jede Meldung bestätigt haben, wird der Vorgang fortgesetzt.</p> <p>Die angezeigten Eigenschaften richten sich nach dem jeweiligen Gerät. Weitere Informationen finden Sie in der Benutzerdokumentation Ihres Geräts.</p>

Gruppierung von Geräten in der GERÄTELISTE

Überblick

EcoStruxure Automation Device Maintenance ermöglicht Ihnen die Strukturierung der Geräte, die in der **GERÄTELISTE** angezeigt werden, durch das Erstellen von Gruppen.

EcoStruxure Automation Device Maintenance V3.0 unterstützt eine Gruppierung nach den IP-Adressen der Geräte durch die Definition von IP-Adressbereichen. Bei neueren Versionen von EcoStruxure Automation Device Maintenance können zusätzliche Gruppierungskriterien hinzugefügt werden.

HINWEIS: Diese Gruppierungsfunktion gilt ausschließlich für IPv4-Adressen. Der IPv6-Standard wird nicht von EcoStruxure Automation Device Maintenance V3.0 unterstützt.

Erstellen von Gruppen

Gehen Sie wie folgt vor, um Geräte zu gruppieren:

Schritt	Aktion
1	Wählen Sie auf der Seite Einstellungen die Option Gruppe aus.
2	Erweitern Sie die Liste Gruppieren nach und wählen Sie die Option Netzwerkbereich aus.
3	Klicken Sie auf die Schaltfläche + Hinzufügen , um einen neuen Adressbereich zu erstellen. Ergebnis: Eine Tabelle mit einer leeren Zeile wird angezeigt.
4	Geben Sie in der Zelle Gruppenname einen Namen für die Gerätegruppe ein.
5	Geben Sie die erste IP-Adresse des Adressbereichs für Ihre Gerätegruppe in der Zelle IP-Startadresse ein.
6	Geben Sie die letzte IP-Adresse des Adressbereichs für Ihre Gerätegruppe in der Zelle IP-Endadresse ein.
7	Klicken Sie auf die Schaltfläche + Hinzufügen , um eine weitere Gruppe zu erstellen. Oder Klicken Sie auf Anwenden , um die Einstellungen für die Gruppe anzuwenden. Oder Klicken Sie auf OK , um alle Änderungen an den Anwendungseinstellungen zu übernehmen und das Dialogfeld Einstellungen zu schließen.

Entfernen eines Geräts

Überblick







Sie können Geräte entfernen, indem Sie sie vorübergehend ausblenden oder auf der Registerkarte **Geräteliste** im Menü **Geräte/Ladevorgang** endgültig entfernen.

Das Gerät kann durch das Ausführen folgender Funktionen entfernt werden:

- Ausblenden eines aktiven Geräts
- Entsorgen eines aktiven Geräts
- Entsorgen eines ausgeblendeten Geräts




Ausblenden eines aktiven Geräts

Gehen Sie zum Ausblenden eines aktiven Geräts wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf die Registerkarte Geräte/Ladevorgang . Erkannte aktive Geräte werden auf der Registerkarte Geräteliste aufgelistet.
2	Auf der Registerkarte Geräte/Ladevorgang : <ul style="list-style-type: none"> Wählen Sie ein einzelnes Gerät aus, indem Sie auf eine Zelle in der Zeile des Geräts klicken. ODER Wählen Sie mehrere Geräte aus, indem Sie die Kontrollkästchen auf der linken Seite jeder Zeile aktivieren oder die gesamte Gruppe auswählen.
3	Für die ausgewählten Geräte sind folgende Symbole aktiviert: <div> <div>  Hide </div> <div>  Dispose </div> </div>
4	<div> <div>  Hide </div> </div> <p>Klicken Sie auf das Symbol .</p> <p>Es erscheint die Meldung Gerät ausblenden.</p> <div> <div>Gerät ausblenden</div> <div>×</div> </div> <div>  Sind Sie sicher, dass Sie die ausgewählten Geräte in die LISTE DER AUSGEBLENDETEN GERÄTE verschieben möchten? <p>Sobald das Gerät ausgeblendet ist, können Sie das Gerät über die LISTE DER AUSGEBLENDETEN GERÄTE erneut aktivieren.</p> <div>  <div>Ja</div> <div>Nein</div> </div> </div>
5	Klicken Sie auf Ja , um fortzufahren. Das ausgewählte Gerät wird in die Registerkarte Liste der ausgeblendeten Geräte verschoben. HINWEIS: Über die Liste der ausgeblendeten Geräte können Sie ausgeblendete Geräte erneut aktivieren.






Einblenden eines zuvor ausgeblendeten Geräts

Gehen Sie zum Einblenden eines zuvor ausgeblendeten Geräts wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf die Registerkarte Geräte/Ladevorgang . Die ausgeblendeten Geräte erscheinen auf der Registerkarte Liste der ausgeblendeten Geräte .
2	<ul style="list-style-type: none"> Wählen Sie ein einzelnes Gerät aus, indem Sie auf eine Zelle in der Zeile des Geräts klicken. ODER Wählen Sie mehrere Geräte aus, indem Sie die Kontrollkästchen auf der linken Seite jeder Zeile aktivieren oder die gesamte Gruppe auswählen.
3	Für die ausgewählten Geräte sind folgende Symbole aktiviert: <ul style="list-style-type: none">  Unhide  Dispose
4	Klicken Sie auf das Symbol  Unhide. Das ausgewählte Gerät wird in die Registerkarte Geräteliste verschoben.






Entsorgen eines aktiven Geräts

Gehen Sie zum Entsorgen eines aktiven Geräts wie folgt vor:

Schritt	Aktion
1	<p>Klicken Sie auf die Registerkarte Geräte/Ladevorgang.</p> <p>Die erkannten aktiven Geräte werden auf der Registerkarte Geräteliste aufgeführt.</p>
2	<ul style="list-style-type: none"> Wählen Sie ein einzelnes Gerät aus, indem Sie auf eine Zelle in der Zeile des Geräts klicken. ODER Wählen Sie mehrere Geräte aus, indem Sie die Kontrollkästchen auf der linken Seite jeder Zeile aktivieren oder die gesamte Gruppe auswählen.
3	<p>Für die ausgewählten Geräte sind folgende Symbole aktiviert:</p> <ul style="list-style-type: none">  Hide  Dispose
4	<p> Dispose</p> <p>Klicken Sie auf das Symbol .</p> <p>Es erscheint die Meldung Gerät entsorgen.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p style="background-color: #28a745; color: white; padding: 5px; display: flex; justify-content: space-between;">Gerät entsorgen ×</p> <p> Sind Sie sicher, dass Sie die ausgewählten Geräte dauerhaft entfernen wollen?</p> <p style="font-size: 0.8em; margin-top: 5px;">Die Entsorgung eines Geräts kann nicht rückgängig gemacht werden. Ein entsorgtes Gerät kann erneut erkannt werden, wenn die automatische Erkennung ausgewählt wurde und das Gerät weiterhin im Netzwerk erreichbar ist.</p> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> ? <div> Ja Nein </div> </div> </div>
5	<p>Klicken Sie auf Ja, um fortzufahren.</p> <p>HINWEIS: Mit einem Klick auf Ja wird das Gerät endgültig aus dem Tool entfernt. Wenn das Gerät erneut hinzugefügt werden soll, muss es entweder erkannt oder manuell hinzugefügt werden.</p>

Entsorgen eines ausgeblendeten Geräts

Gehen Sie zum Entsorgen eines ausgeblendeten Geräts wie folgt vor:

Schritt	Aktion
1	Klicken Sie auf die Registerkarte Geräte/Ladevorgang . Die ausgeblendeten Geräte erscheinen auf der Registerkarte Liste der ausgeblendeten Geräte .
2	<ul style="list-style-type: none"> Wählen Sie ein einzelnes Gerät aus, indem Sie auf eine Zelle in der Zeile des Geräts klicken. ODER Wählen Sie mehrere Geräte aus, indem Sie die Kontrollkästchen auf der linken Seite jeder Zeile aktivieren oder die gesamte Gruppe auswählen.
3	Für die ausgewählten Geräte sind folgende Symbole aktiviert: <div>  Unhide </div> <ul style="list-style-type: none"> • <div>  Dispose </div> •
4	<div>  Unhide </div> <p>Klicken Sie auf das Symbol</p> <p>Es erscheint die Meldung Gerät entsorgen.</p> <div> <div>Gerät entsorgen</div> <div>×</div> </div> <div>  Sind Sie sicher, dass Sie die ausgewählten Geräte dauerhaft entfernen wollen? </div> <p>Die Entsorgung eines Geräts kann nicht rückgängig gemacht werden. Ein entsorgtes Gerät kann erneut erkannt werden, wenn die automatische Erkennung ausgewählt wurde und das Gerät weiterhin im Netzwerk erreichbar ist.</p> <div>  <div>Ja</div> <div>Nein</div> </div>
5	Klicken Sie auf Ja , um fortzufahren. HINWEIS: Durch Anklicken von Ja wird das Gerät endgültig aus dem Tool entfernt und kann nicht mehr aufgerufen werden.

Verwaltung der Benutzeranmeldedaten

Überblick


EcoStruxure Automation Device Maintenance ermöglicht die Eingabe von Anmeldedaten für den autorisierten Zugriff auf die Geräte global für das Projekt und individuell für jedes Gerät.

Globale Verwaltung von Benutzeranmeldedaten

Um die Anmeldedaten global für das Projekt zu verwalten, rufen Sie die Seite **Einstellungen** auf und wählen die Option **Projekt > Einstellungen für die Benutzeranmeldedaten** aus.


Wählen Sie **Authentifizierungstyp > Benutzername** oder **Authentifizierungstyp > Benutzerdefiniert** aus und geben Sie die angeforderten Anmeldedaten ein. Klicken Sie auf **OK**, um die Anmeldedaten zu speichern. Infolgedessen wird das Symbol **Anmeldedaten festlegen** für die entsprechenden Geräte auf der Seite **Geräte/Ladevorgang** gelb angezeigt, und

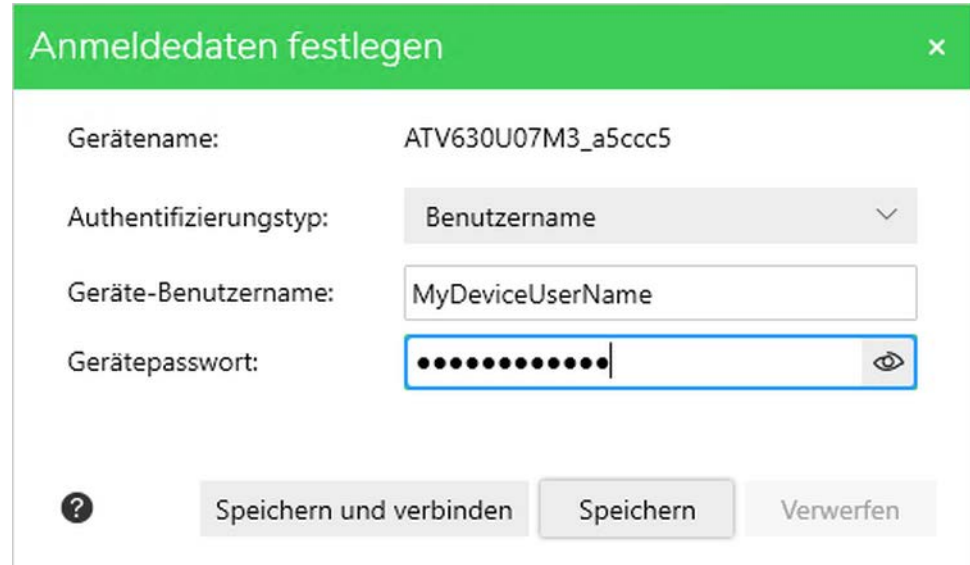
Sie können auf das Symbol **Verbinden**  oder auf die Schaltfläche

 **Verbinden**



klicken, um sich anzumelden, ohne die Anmeldedaten erneut einzugeben.

Verwalten der Benutzeranmeldedaten pro Gerät

Um die Anmeldedaten für jedes Gerät einzeln zu verwalten, öffnen Sie die Seite **Geräte/Ladevorgang** und klicken Sie auf das Symbol **Anmeldedaten festlegen**  in der Gerätezeile der Tabelle:



Sie können auf **Speichern und verbinden** klicken, um die Anmeldedaten zu speichern und eine Verbindung zum Gerät herzustellen. Nach erfolgreicher Anmeldung wird das Symbol **Anmeldedaten festlegen** grün angezeigt. Sie können auch auf **Speichern** klicken, um die Anmeldedaten für dieses Gerät zu einem späteren Zeitpunkt für die Anmeldung zu speichern. In diesem Fall wird das Symbol **Anmeldedaten festlegen** gelb, und Sie können für die Anmeldung auf

das Symbol **Verbinden**  oder auf die Schaltfläche  **Verbinden** klicken, ohne die Anmeldedaten erneut eingeben zu müssen.

Benutzeranmeldungsparameter

Die angezeigten Parameter sind gerätespezifisch und erfordern die Eingabe der Anmeldedaten, die für die Anmeldung beim jeweiligen Gerät erforderlich sind. Weitere Informationen finden Sie in der Benutzerdokumentation Ihres Geräts.











Für die Anmeldung bei Modicon M340-, Modicon M580- oder Momentum-Steuerungen sind drei Passwörter erforderlich. Detaillierte Informationen zu den Passwörtern für den Anwendungsschutz, für die Datenspeicherung und für den Firmwareschutz finden Sie in den entsprechenden Kapiteln in folgendem Handbuch: *EcoStruxure Control Expert Operating Modes* or the legacy *Unity Pro Operating Modes* manual. Die Download-Links für die übersetzten Versionen dieses Handbuchs finden Sie in der Liste der weiterführenden Dokumente in dieser Online-Hilfe, Seite 10.

Zugriff auf Erweiterungen

Überblick

Ein modulares Gerät in der **GERÄTELISTE** auf der Registerkarte **Geräte/Ladevorgang** stellt eine Verbindung bereit, über die Sie auf die einzelnen Erweiterungen des Geräts zugreifen können.

Beispiel für ein modulares Gerät:

DATENPAKET GERÄTE / LADEVORGANG									
GERÄTELISTE									
	Status	Gerätename Handelsreferenz	Dienstendpunkt Seriennummer	Firmw- Version	Sicherhel...	Modus	Infos zum Aktualisierungscenter	Erweiterungen	Aktionen
Gerätstandardgruppe (9)									
	●	ATV630EIP CR: ATV630U07M3	mhttp://172.20.170.209-502 SN: 4004000HL44718401Y	2.6IE94B13	-	STOP		Erweiterungen	    
	●	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196-443 SN: 4002200HL64787000N	3.5IE94B04	-	-			    

Wenn vom Gerät unterstützt, öffnet der Link **Erweiterungen** ([Erweiterungen](#)) eine neue Registerkarte **Erweiterungen** und stellt die modularen Geräte nach **Erweiterung** gruppiert bereit.

DATENPAKETGERÄTE / LADEVORGANGERWEITERUNGEN

ATV630EIP

ATV630EIP

CR: ATV630U07M3

mhttp://172.20.170.209-502


SN: 4004000HL44718401Y


Firmware-Version: 2.6IE94B13

Aktualisierungscenter

0

Status	Gerätename Handelsreferenz	Dienstendpunkt Seriennummer	Firmware- Version	Infos zum Aktualisierungscenter	Aktionen
<div><div></div><div></div></div>	EtherNet/IP ModbusTCP module CR: VW3A3721	1 SN:	1.8IE13B02		<div><div></div><div></div></div>


Auf beiden Registerkarten können Sie auf das Dialogfeld **Aktualisierungscenter** zugreifen (über das Symbol **Aktualisierungscenter** oder die Schaltfläche 

Aktualisierungscenter  **Aktualisierungscenter**), in dem Sie das Firmware-Datenpaket über die Schaltfläche **Firmware** auswählen können.

Für Geräte, die die Erweiterungen nicht auf Anforderung laden können, indem Sie auf den Link **Erweiterungen** klicken, folgen Sie dem im nächsten Abschnitt beschriebenen Verfahren, um auf einzelne Erweiterungen zuzugreifen.


Manueller Zugriff auf Erweiterungen

Für Geräte, die die Erweiterungen nicht auf Anforderung laden können, indem Sie auf den Link **Erweiterungen** klicken, gehen Sie wie folgt vor:

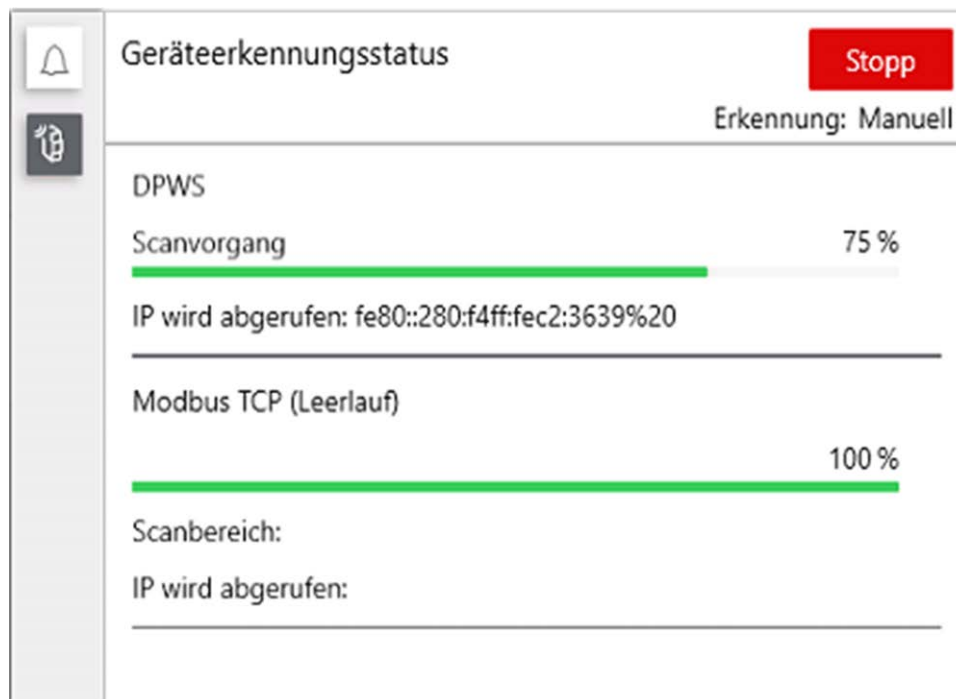
Schritt	Aktion
1	<p>Klicken Sie auf den Link Erweiterungen des modularen Geräts.</p> <p>Ergebnis: Die Registerkarte Erweiterungen wird geöffnet. Wenn das Gerät die Erweiterungen nicht auf Anforderung laden kann, indem Sie auf den Link Erweiterungen klicken, wird die Schaltfläche Hinzufügen angezeigt.</p>
2	<p>Klicken Sie auf die Schaltfläche Hinzufügen oder auf den Link Kein Modul gefunden. Zum Hinzufügen eines Moduls hier klicken.</p> <p>Ergebnis: Das Dialogfeld Modul hinzufügen wird geöffnet.</p>
3	<p>Im Dialogfeld Modul hinzufügen konfigurieren Sie die Parameter für den Zugriff auf die Erweiterungen des Geräts:</p> <ul style="list-style-type: none"> • Rack-Nummer • Steckplatz-Nummer
4	<p>Klicken Sie auf die Schaltfläche OK, um den Erkennungsscan zu starten.</p> <p>Wenn die Erweiterungen erfolgreich erkannt wurden, wird die Registerkarte Erweiterungen angezeigt.</p> 
5	Schließen Sie die Registerkarte Erweiterungen .

Überwachen des Geräteerkennungsstatus

Überblick

Immer dann, wenn die Geräteerkennung ausgeführt wird, können Sie den Status des Prozesses abrufen, indem Sie auf die Schaltfläche  auf der Registerkarte **Geräte/Ladevorgang** klicken.

Die Ansicht **Geräteerkennungsstatus** wird auf der rechten Seite geöffnet:



Sie enthält die folgenden Informationen:

- Fortschrittsinformationen werden für jeden Scanner einzeln angegeben.
- Wenn verschiedene Bereiche für einen Scanner konfiguriert sind, werden die Fortschrittsinformationen für jeden Bereich einzeln angegeben (z. B. für Modbus TCP-Scanner, Seite 34).

Mit der Schaltfläche **Start/Stopp** können Sie direkt von dieser Ansicht aus eine manuelle Geräteerkennung starten oder eine laufende Geräteerkennung stoppen.

Anzeigen/Bestätigen von Meldungen

Überblick

Für einige der von EcoStruxure Automation Device Maintenance ausgeführten Vorgänge sind Benutzerinteraktionen erforderlich. Immer dann, wenn eine Bestätigung erforderlich ist, wird der Vorgang, wie beispielsweise die Aktualisierung der Firmware, angehalten, und im Benachrichtigungsbereich wird eine Meldung angezeigt. Lesen Sie jede Meldung sorgfältig durch und bestätigen Sie sie nach der Durchführung einer Risikobewertung. Nachdem Sie jede Meldung bestätigt haben, wird der Vorgang fortgesetzt.

Um den Benachrichtigungsbereich zu öffnen, klicken Sie auf die Schaltfläche **Ladevorgang**.



auf der Registerkarte **Geräte/**

DATENPAKET

GERÄTE / LADEVORGANG

GERÄTELISTE

Hinzufügen
Verbinden
Verbindung trennen
Aktualisierungscenter
Ausblenden
Entsorgen

Status	Gerätename Handelsreferenz	Dienstendpunkt Seriennummer	Firmw... Version	Sicherhei...	Modus	Infos zum Aktualisierungscenter
Gerätstandardgruppe (10)						
<input checked="" type="checkbox"/>	BME NOC0321 CR: BME NOC0321	ftp://172.20.170.62:21 SN:	01.06 IR 2	- Bestätigung erforderlich	Firmware ausgewählt	
<input type="checkbox"/>	140*** CR: 140***	https://172.20.170.72:443 SN:	-	-	-	
<input type="checkbox"/>	BMEP586040_21190100014 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	3.5IE94801	-	-	
<input type="checkbox"/>	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94804	-	-	
<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: PRODD006115	22.0.2215...	-	-	
<input type="checkbox"/>	ATV630U07M3 CR: ATV630U07M3	mbap://[fe80::280:f4ff:fec2:3639%17]:... SN: 18c23639	3.5IE94802	-	-	
<input type="checkbox"/>	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94802	-	-	

Benachrichtigungsbereich

Sicherheitshinweis

☒ BME NOC0321
ftp://172.20.170.62:21

Vor dem Übertragen von Daten zur SPS sollte sichergestellt werden, dass die Verbindung mit dem richtigen Gerät besteht, indem die auf der Registerkarte Firmware angezeigte SPS- und MAC-Adresse überprüft wird. Die Übertragung von Daten an ein falsches Gerät kann Ihren Prozess gefährlich beeinträchtigen.

Möchten Sie die Datenübertragung fortsetzen?

Bestätigen
Ablehnen

Historie
Aktualisieren
Abbrechen

Im Benachrichtigungsbereich können zwei verschiedene Arten von Meldungen angezeigt werden:

- **Bestätigungsmeldungen:** Wählen Sie die Meldung aus, indem Sie das entsprechende Kontrollkästchen aktivieren, und klicken Sie dann auf **Bestätigen**, um die Meldung zu bestätigen und den Vorgang wieder aufzunehmen. Klicken Sie auf **Ablehnen**, um den Vorgang zu stoppen.
- **Benachrichtigungen:** Wählen Sie die Meldung aus, indem Sie das entsprechende Kontrollkästchen aktivieren, und klicken Sie dann auf **OK**, um die Meldung zu bestätigen und den Vorgang wieder aufzunehmen.

Über die Option **Benachrichtigungen nicht anzeigen** können Sie die Anzeige von Benachrichtigungen deaktivieren. Wenn die Option ausgewählt wird, werden die Vorgänge automatisch ohne Unterbrechung für Benutzerinteraktionen ausgeführt, wobei vorausgesetzt wird, dass die Meldungen bestätigt wurden.

HINWEIS: Aktivieren Sie diese Option nur, wenn Sie im Wartungsmodus arbeiten und der Bediener den Sicherheitsstatus Ihrer Maschinen- oder Prozessumgebung überprüft hat.

Anzeigen der Protokolle


Sie können die gespeicherten Protokolle anzeigen und analysieren, um Details zum ausgewählten Gerät zu erhalten.


Die Protokollinformationen können in den folgenden Bereichen angezeigt werden:

- Für jedes Gerät auf der Seite **Geräte/Ladevorgang**
- Für das gesamte Projekt im Fenster **Protokolle**

HINWEIS: Im Fenster **Protokolle** werden erkannte Fehler, erkannte Warnungen und Informationsmeldungen in einem einzigen Fenster angezeigt.

Gehen Sie wie folgt vor, um die Protokolle anzuzeigen, die sich ausschließlich auf das ausgewählte Gerät beziehen:

Schritt	Aktion
1	Rufen Sie die Seite Geräte/Ladevorgang auf.
2	<p>Klicken Sie auf das Symbol Geräteprotokoll  eines Geräts.</p> <p>Ergebnis: Eine kleine Ansicht Protokollinfo wird direkt in der Tabelle unterhalb der Gerätezeile geöffnet. Verwenden Sie die Bildlaufleiste auf der rechten Seite, um bei Bedarf alle Protokolleinträge anzuzeigen.</p>

Um die **Protokollinfo** für ein Gerät auszublenden, klicken Sie erneut auf das Symbol **Geräteprotokoll** .

Empfehlung zur verbesserten Cybersicherheit

Die Protokolldatei enthält normalerweise sensible Daten wie


- Geräteadressen
- Gerätenamen
- Details der Netzwerktopologie
- Details der Netzwerkkonfiguration


Sie wird auf der Festplatte Ihres PC gespeichert. Löschen Sie die Protokolldatei, sobald sie nicht mehr benötigt wird, oder speichern Sie sie an einem sicheren Ort, an dem kein unbefugter Zugriff möglich ist.

Aktualisierungscenter

Überblick

Im Dialogfeld **Aktualisierungscenter** können Sie die Einstellungen für die Durchführung einer Firmwareaktualisierung oder einer Aktualisierung der Sicherheitskonfigurationsdatei konfigurieren. Diese Konfigurationseinstellungen können auf ein einzelnes Gerät oder auf verschiedene Geräte gleichzeitig angewendet werden.

- Um Aktualisierungen für ein einzelnes Gerät durchzuführen, klicken Sie auf das Symbol **Aktualisierungscenter**  in der Gerätezeile der Tabelle auf der Registerkarte **Geräte/Ladevorgang**.
- Um gleichzeitig Aktualisierungen für verschiedene Geräte des Projekts durchzuführen, wählen Sie die Geräte auf der Registerkarte **Geräte/Ladevorgang** aus und klicken Sie auf die Schaltfläche

Aktualisierungscenter  **Aktualisierungscenter** in der Schaltflächenleiste.

Dialogfeld Aktualisierungscenter

Beide Vorgänge öffnen das Dialogfeld **Aktualisierungscenter**, in dem Sie Folgendes auswählen können:

- **Firmware:** Zum Konfigurieren der Einstellungen für die Aktualisierung der Firmware des bzw. der ausgewählten Geräte. Für weitere Informationen siehe *Aktualisierung der Firmware*, Seite 70.
- **Sicherheit:** Zum Konfigurieren von Einstellungen für die Aktualisierung der Sicherheitskonfigurationsdatei des bzw. der ausgewählten Geräte. Für weitere Informationen siehe *Aktualisierung der Sicherheitskonfigurationsdatei*, Seite 72.
- **Zurücksetzen:** Zum Zurücksetzen der Aktualisierungseinstellungen für das bzw. die ausgewählten Geräte.

Um die Einstellungen zu bestätigen und das Dialogfeld **Aktualisierungscenter** zu schließen, klicken Sie auf die Schaltfläche **Speichern**. Daraufhin wird die von Ihnen vorgenommene Konfiguration in den **Infos zum Aktualisierungscenter**-Zellen des bzw. der Geräte auf der Registerkarte **Geräte/Ladevorgang**, Seite 21 angegeben.

Um den Aktualisierungsvorgang wie konfiguriert auszuführen, klicken Sie auf die Schaltfläche **Aktualisieren**.

Aktualisierung der Firmware

Überblick

EcoStruxure Automation Device Maintenance ermöglicht die Aktualisierung der Gerätefirmware, die auf der Registerkarte **Geräte/Ladevorgang** angezeigt wird.



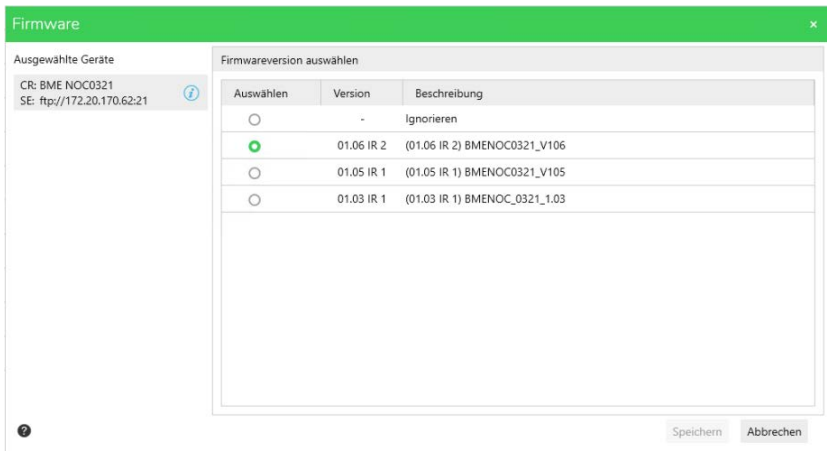
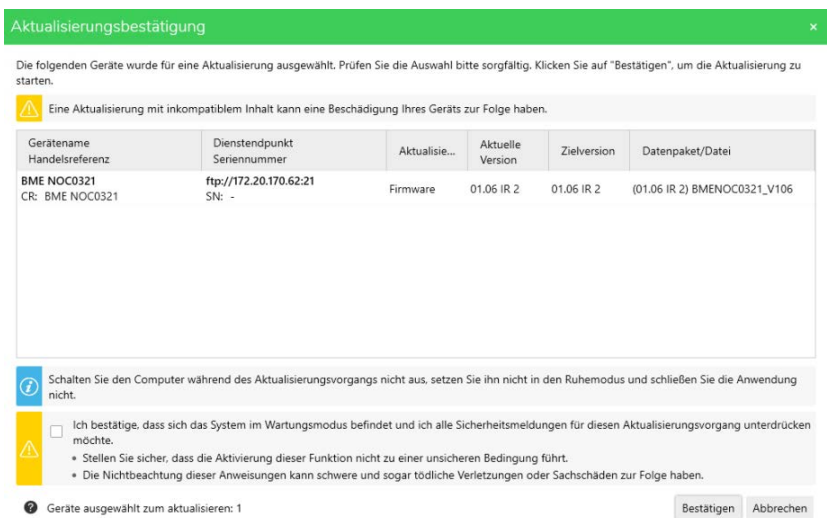
Um die Firmware modularer Geräte zu aktualisieren, können Sie wie im Kapitel [Zugriff auf Erweiterungen](#), Seite 64 beschrieben auf die einzelnen Erweiterungen zugreifen.

Sie können Datenpakete für mehrere Erweiterungen und/oder Rack-Module auswählen. EcoStruxure Automation Device Maintenance aktualisiert die Firmware dieser Geräte gleichzeitig.

HINWEIS: Wenn Sie für die Steuerung und die Module gleichzeitig eine Aktualisierung durchführen, stellen Sie sicher, dass Sie die Steuerung nicht neu startet, während die Aktualisierung der Module noch läuft. Siehe nachstehende wichtige [Gefahrenhinweise](#).

Aktualisieren der Firmware

Gehen Sie zur Aktualisierung der Firmware vor wie folgt:

Schritt	Aktion
1	Rufen Sie die Seite Geräte/Ladevorgang auf.
2a	Um eine Aktualisierung für ein einzelnes Gerät auszuführen, klicken Sie auf das Symbol Aktualisierungscenter  in der Gerätezeile.
2b	Um gleichzeitig Aktualisierungen für verschiedene Projektgeräte durchzuführen, aktivieren Sie die entsprechenden Kontrollkästchen oder aktivieren Sie das Kontrollkästchen für die gesamte Gruppe und klicken Sie auf die Schaltfläche Aktualisierungscenter  Aktualisierungscenter in der Symbolleiste.
3	Klicken Sie im Dialogfeld Aktualisierungscenter auf die Schaltfläche Firmware .
4	Wählen Sie im Dialogfeld Firmware das Firmware-Datenpaket für jedes Gerät aus. 
5	Klicken Sie auf Speichern , um die Firmware-Aktualisierungskonfiguration zu speichern und das Dialogfeld Firmware zu schließen. Ergebnis: In der oder den Infos zum Aktualisierungscenter -Zellen des bzw. der Geräte auf der Registerkarte Geräte/Ladevorgang , Seite 21 wird der Text Firmware ausgewählt angezeigt.
6	Klicken Sie auf die Schaltfläche Aktualisieren auf der Registerkarte Geräte/Ladevorgang , um den Aktualisierungsvorgang zu starten. Ergebnis: Daraufhin erscheint das Dialogfeld Aktualisierungsbestätigung . 
7	Überprüfen Sie im Dialogfeld Aktualisierungsbestätigung sorgfältig die Liste der Geräte, die Sie für die Aktualisierung ausgewählt haben, und die vorgenommenen Einstellungen.

Schritt	Aktion
8	Klicken Sie auf die Schaltfläche Bestätigen , um den Aktualisierungsvorgang zu starten. Ergebnis: Das Verfahren zur Aktualisierung der Firmware wird gestartet. Immer dann, wenn eine Benutzerinteraktion erforderlich ist, wird das Verfahren angehalten und eine Meldung im Benachrichtigungsbereich, Seite 67 angezeigt. Lesen Sie jede Meldung sorgfältig durch und bestätigen Sie sie nach der Durchführung einer Risikobewertung. Nachdem Sie jede Meldung bestätigt haben, wird der Vorgang fortgesetzt.
9	Klicken Sie nach dem erfolgreichen Abschluss des Firmwareprozesses auf die Schaltfläche Zusammenfassung , Seite 19 am unteren Rand des EcoStruxure Automation Device Maintenance, um das Dialogfeld Aktualisierungshistorie anzuzeigen. Es enthält Informationen zum Aktualisierungsstatus für jedes Gerät mit Verweis auf die vorherige und die Zielversion sowie zum Datenpaket bzw. zur Datendatei.

HINWEIS

BESCHÄDIGTE GERÄTE

Schalten Sie den PC nicht aus, schließen Sie die Anwendung und stellen Sie sicher, dass der PC nicht in den Ruhezustand wechselt, während der Firmwareaktualisierungsprozess läuft, da eine Prozessunterbrechung das Gerät beschädigen kann.

Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.

Sie können optional das Kontrollkästchen **Ich bestätige, dass sich das System im Wartungsmodus befindet und ich alle Sicherheitshinweise für diese Aktualisierungssequenz unterdrücken möchte** aktivieren. Dadurch wird verhindert, dass der Vorgang unterbrochen wird.

HINWEIS: Aktivieren Sie diese Option nur, wenn Sie im Wartungsmodus arbeiten und der Bediener den Sicherheitsstatus Ihrer Maschinen- oder Prozessumgebung überprüft hat.

Nach erfolgreichem Abschluss des Firmwareprozesses können Sie für Steuerungen auf der Registerkarte **Geräte/Ladevorgang** optional auf das Symbol **Gerät starten**, Seite 21 klicken, um das Gerät zu starten.

HINWEIS: Führen Sie zuerst einen Anlauftest durch, bevor Sie elektrische Steuerungs- und Automatisierungsgeräte für einen regulären Betrieb nach der Installation bzw. einer Aktualisierung verwenden. Für weitere Informationen siehe *Start und Test*, Seite 7.

Aktualisierung der Sicherheitskonfigurationsdatei



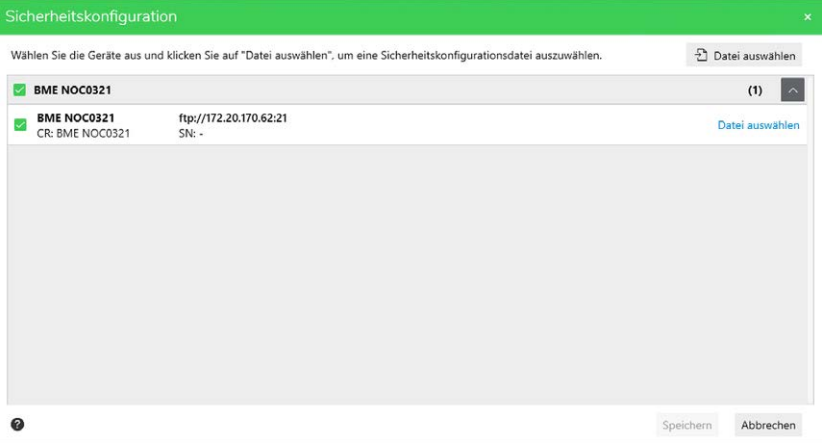
Überblick

EcoStruxure Automation Device Maintenance ermöglicht die Aktualisierung der Sicherheitskonfigurationsdatei mit den Sicherheitskonfigurationseinstellungen, die Sie global für Ihr Netzwerk in der Anwendung EcoStruxure Cybersecurity Admin Expert konfiguriert haben.

HINWEIS: Die neue Sicherheitskonfigurationsdatei kann dem oder den Geräten neue Anmeldedaten zuweisen. Für alle weiteren Anmeldungen müssen dann die neuen Anmeldedaten eingegeben werden.

Aktualisieren der Sicherheitskonfigurationsdatei

Führen Sie die folgenden Schritte aus, um die Sicherheitskonfigurationsdatei zu aktualisieren:

Schritt	Aktion
1	Rufen Sie die Seite Geräte/Ladevorgang auf.
2a	Um eine Aktualisierung für ein einzelnes Gerät auszuführen, klicken Sie auf das Symbol Aktualisierungscenter  in der Gerätezeile.
2b	Um gleichzeitig Aktualisierungen für verschiedene Projektgeräte durchzuführen, aktivieren Sie die entsprechenden Kontrollkästchen oder aktivieren Sie das Kontrollkästchen für die gesamte Gruppe und klicken Sie auf die Schaltfläche Aktualisierungscenter  Aktualisierungscenter in der Symbolleiste.
3	Klicken Sie im Dialogfeld Aktualisierungscenter auf die Schaltfläche Sicherheit .
4	<p>Wählen Sie im Dialogfeld Sicherheitskonfiguration ein einzelnes Gerät aus und klicken Sie auf den Link Dateiauswahl für dieses Gerät. Oder wählen Sie mehrere Geräte aus und klicken Sie dann oben im Dialogfeld auf die Schaltfläche Datei auswählen.</p>  <p>Ergebnis: Ein Windows-Dialogfeld zum Öffnen von Dateien wird angezeigt. Es ermöglicht Ihnen, Ihr Netzwerk nach der Sicherheitskonfigurationsdatei zu durchsuchen.</p>
5	<p>Wählen Sie die Sicherheitskonfigurationsdatei aus und klicken Sie auf die Schaltfläche Öffnen.</p> <p>Ergebnis: Das Dialogfeld Sicherheitskonfiguration zeigt die Geräte mit den ausgewählten Dateien an.</p>
6	<p>Klicken Sie auf die Schaltfläche Speichern, um die Konfiguration zu speichern und das Dialogfeld Sicherheitskonfiguration zu schließen.</p> <p>Ergebnis: In den Zellen Infos zum Aktualisierungscenter der Geräte auf der Registerkarte Geräte/Ladevorgang, Seite 21 wird der Text Sicherheitskonfiguration ausgewählt angezeigt.</p>
7	<p>Klicken Sie auf die Schaltfläche Aktualisieren auf der Registerkarte Geräte/Ladevorgang, um den Aktualisierungsvorgang zu starten.</p> <p>Ergebnis: Daraufhin erscheint das Dialogfeld Aktualisierungsbestätigung.</p>
8	Überprüfen Sie im Dialogfeld Aktualisierungsbestätigung sorgfältig die Liste der Geräte, die Sie für die Aktualisierung ausgewählt haben, sowie die vorgenommenen Einstellungen.
9	<p>Klicken Sie auf die Schaltfläche Bestätigen, um den Aktualisierungsvorgang zu starten.</p> <p>Ergebnis: Der Aktualisierungsvorgang wird gestartet. Immer dann, wenn eine Benutzerinteraktion erforderlich ist, wird das Verfahren angehalten und eine Meldung im Benachrichtigungsbereich, Seite 67 angezeigt. Lesen Sie jede Meldung sorgfältig durch und bestätigen Sie sie nach der Durchführung einer Risikobewertung. Nachdem Sie jede Meldung bestätigt haben, wird der Vorgang fortgesetzt.</p>

HINWEIS

BESCHÄDIGTE GERÄTE

Schalten Sie den PC nicht aus, schließen Sie die Anwendung und stellen Sie sicher, dass der PC nicht in den Ruhezustand wechselt, während der Firmwareaktualisierungsprozess läuft, da eine Prozessunterbrechung das Gerät beschädigen kann.

Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.

Sie können optional das Kontrollkästchen **Ich bestätige, dass sich das System im Wartungsmodus befindet und ich alle Sicherheitshinweise für diese Aktualisierungssequenz unterdrücken möchte.** aktivieren. Dadurch wird verhindert, dass der Vorgang unterbrochen wird.

HINWEIS: Aktivieren Sie diese Option nur, wenn Sie im Wartungsmodus arbeiten und der Bediener den Sicherheitsstatus Ihrer Maschinen- oder Prozessumgebung überprüft hat.

Cybersicherheit

Einführung

Cybersicherheit ist ein Teilgebiet der Netzwerkadministration, bei dem es darum geht, Angriffe auf Computersysteme bzw. von Computersystemen sowie über Computernetzwerke zu verhindern, die zu unabsichtlichen oder vorsätzlichen Schäden und Ausfällen führen können. Ziel der Cybersicherheit ist es, einen höheren Schutzgrad für Daten und physische Ressourcen bereitzustellen, um diese vor Diebstahl, Beschädigung, Missbrauch oder Unfällen zu schützen, und dabei gleichzeitig den Zugriff für die vorgesehenen Benutzer aufrechtzuerhalten.

Kein einziger Cybersicherheitsansatz ist ausreichend. Schneider Electric empfiehlt einen tiefgreifenden Ansatz zur Verteidigung. Bei diesem von der amerikanischen National Security Agency (NSA) entwickelten Ansatz werden mehrere Schichten von Sicherheitsfunktionen, Appliances und Prozessen im Netzwerk implementiert. Die grundlegenden Komponenten dieses Ansatzes sind:

- Risikobewertung
- Ein auf den Ergebnissen der Risikobewertung aufbauender Sicherheitsplan
- Eine mehrphasige Schulungskampagne
- Physische Trennung der industriellen Netzwerke von den Unternehmensnetzwerken mittels einer „Demilitarized Zone“ (DMZ, entmilitarisierte Zone) sowie der Verwendung von Firewalls und Routing zur Schaffung weiterer Sicherheitszonen
- Systemzugriffssteuerung
- Geräte-Hardening
- Netzwerküberwachung und -wartung

In diesem Kapitel werden Elemente definiert, mit deren Hilfe Sie ein System so konfigurieren können, dass es weniger anfällig für Cyber-Angriffe ist. Ausführliche Informationen über den Ansatz für tiefgreifende Sicherheit finden Sie in *Systemspezifische technische Hinweise: Wie kann ich... Reduce Vulnerability to Cyber Attacks* auf der [Schneider Electric website](#).

Was ist Cybersicherheit?

Überblick

Cyberbedrohungen sind vorsätzliche oder unbeabsichtigte Handlungen, durch die der normale Betrieb von Computersystemen und Netzwerken gestört werden kann. Diese Aktionen können von der physischen Anlage selbst oder von einem externen Standort ausgehen. In Steuerungsumgebungen sind u. a. folgende Herausforderungen im Hinblick auf die Sicherheit gegeben:

- Unterschiedliche physische und logische Grenzen
- Mehrere Standorte und große geografische Entfernungen
- Negative Auswirkungen der Sicherheitsimplementierung auf die Prozessverfügbarkeit
- Erhöhtes Risiko einer Übertragung von Würmern und Viren von Geschäftssystemen auf Steuerungssysteme aufgrund einer offeneren Kommunikation zwischen diesen Systemen
- Erhöhtes Risiko einer Übertragung von Malware über USB-Geräte, Laptops von Anbietern und Wartungstechnikern und das Unternehmensnetzwerk
- Direkte Auswirkungen der Steuerungssysteme auf physische und mechanische Systeme

Quellen von Cyberangriffen

Implementieren Sie einen Plan für die Cybersicherheit, bei dem die verschiedenen potenziellen Quellen von Cyberangriffen und unbeabsichtigten Vorfällen berücksichtigt werden:

Quelle	Beschreibung
Intern	<ul style="list-style-type: none"> • Unangemessenes Verhalten von Mitarbeitern oder Vertragsnehmern • Verärgerte Mitarbeiter oder Vertragsnehmer
Extern gelegentlichsbasiert (nicht gezielt)	<ul style="list-style-type: none"> • Scriptkiddies* • Freizeit-Hacker • Virenprogrammierer
Extern vorsätzlich (gezielt)	<ul style="list-style-type: none"> • Kriminelle Gruppen • Aktivisten • Terroristen • Behörden ausländischer Staaten
Versehentlich	
* Slang-Begriff für Hacker, die programmierte, bösartige Skripts von anderen verwenden, ohne dabei unbedingt wirklich zu verstehen, wie das Skript funktioniert oder welche Auswirkungen es auf ein System haben kann	

Ein vorsätzlicher Cyberangriff auf ein Steuerungssystem kann verschiedene böswillige Ziele verfolgen. Beispiel:

- Beeinträchtigung des Produktionsprozesses durch Blockierung oder Verzögerung des Informationsflusses
- Beschädigung, Deaktivierung oder Herunterfahren von Geräten zur Beeinträchtigung der Produktion oder Umgebung
- Modifizierung oder Deaktivierung von Sicherheitssystemen, um vorsätzlich Schaden zuzufügen

Wie Angreifer Zugang erhalten

Ein Cyberangreifer umgeht die Schutzmaßnahmen am Netzwerkperimeter, um Zugriff auf das Netzwerk des Steuerungssystems zu erhalten. Gängige Zugangspunkte sind u. a. Folgende:

- Wählzugriff auf RTU-Geräte (Remote Terminal Unit)
- Zulieferer-Zugangspunkte (z. B. Zugangspunkte für technischen Support)
- IT-gesteuerte Netzwerkprodukte
- Unternehmens-VPN (virtuelles privates Netzwerk)
- Datenbank-Links
- Schlecht konfigurierte Firewalls
- Peer-Dienstprogramme

Cybersicherheitszertifikate

Die von Schneider Electric entwickelten Richtlinien für Cybersicherheit basieren auf den folgenden Empfehlungen:

- Achilles
- ISA Secure

Bei Fragen, News oder Berichterstattungsproblemen

Wenn Sie eine Frage zur Cybersicherheit stellen möchten, die neuesten Nachrichten von Schneider Electric erhalten oder Schwachstellen melden möchten, besuchen Sie unsere [website](#).

Richtlinien von Schneider Electric

Einführung

Auf Ihrem PC-System können verschiedene Anwendungen ausgeführt werden, um die Sicherheit in Ihrer Steuerungsumgebung zu erhöhen. Das System verfügt über werkseitige Standardeinstellungen, die umkonfiguriert werden müssen, um den Empfehlungen von Schneider Electric für das Geräte-Hardening im Rahmen eines Ansatzes für tiefgreifende Sicherheit zu entsprechen.

Die folgenden Richtlinien beschreiben die Vorgehensweisen bei einem Windows-Betriebssystem und dienen lediglich als Beispiel. Für Ihr Betriebssystem und Ihre Anwendungen können unterschiedliche Voraussetzungen oder Verfahren erforderlich sein.

Hardening von Engineering-Workstations

Kunden können verschiedene kommerzielle PCs wählen, um ihre Anforderungen für eine Engineering-Workstation zu erfüllen. Schlüsseltechniken des Hardening sind unter anderem:

- Starke Passwortverwaltung.
- Benutzerkontenverwaltung.
- Anwendung des Prinzips der geringsten Rechte für Anwendungs- und Benutzerkonten.
- Entfernen oder Deaktivieren ungenutzter Dienste.
- Entfernen von dezentralen Verwaltungsrechten.
- Systematische Patch-Verwaltung.

Nicht genutzte Netzwerkschnittstellenkarten deaktivieren

Stellen Sie sicher, dass nicht für die Anwendung erforderliche Netzwerkkarten deaktiviert werden. Wenn Ihr System beispielsweise über zwei Karten verfügt, die Anwendung jedoch nur eine davon verwendet, vergewissern Sie sich, dass die zweite Netzwerkkarte (LAN-Verbindung 2) deaktiviert ist.

So deaktivieren Sie eine Netzwerkkarte in Windows:

Schritt	Aktion
1	Öffnen Sie Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptoreinstellungen ändern .
2	Klicken Sie mit der rechten Maustaste auf die nicht genutzte Verbindung. Wählen Sie Deaktivieren aus.

LAN-Verbindung konfigurieren

Verschiedene Windows-Netzwerkeinstellungen bieten erhöhte Sicherheit in Einklang mit dem von Schneider Electric empfohlenen Ansatz für tiefgreifende Sicherheit.

In Windows-Systemen erfolgt der Zugriff auf diese Einstellungen unter **Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptereinstellungen ändern > LAN-Verbindung (x)**.

In Folgenden werden Beispiele für Konfigurationsänderungen angeführt, die Sie im Fenster **Eigenschaften von LAN-Verbindung** an Ihrem System vornehmen können:

- Deaktivieren Sie alle IPv6-Stapel auf den entsprechenden Netzwerkkarten. (Für dieses Systembeispiel ist der IPv6-Adressbereich nicht erforderlich, und durch Deaktivierung der IPv6-Stapel wird die Anfälligkeit für potenzielle IPv6-Sicherheitsrisiken begrenzt.)
- Deaktivieren Sie **Datei- und Druckerfreigabe für Microsoft Network**.

Zu von Schneider Electric empfohlenen tiefgreifenden Sicherheitsmaßnahmen zählen zudem die Folgenden:

- Definieren Sie ausschließlich statische IPv4-Adressen, Subnetzmasken und Gateways.
- Verwenden Sie im Leitstand weder DHCP noch DNS.

Windows-Firewall verwalten

Die Empfehlungen von Schneider Electric für tiefgreifende Sicherheit umfassen die Aktivierung der Windows-Host-Firewall auf allen System-PCs. Aktivieren Sie die Firewalls für alle aufgeführten öffentlichen oder privaten Profile.

Es wird Benutzern grundsätzlich empfohlen, Firewallregeln zu definieren, die jegliche Verbindung an oder von einem unbekannten/nicht vertrauenswürdigen externen Host verweigern.

Remotedesktopprotokoll deaktivieren

Zu den Empfehlungen des Defense-in-Depth-Ansatzes von Schneider Electric gehören die Deaktivierung des Remotedesktopprotokolls (RDP), sofern Ihre Anwendung nicht die RDP erfordert.

Führen Sie die folgenden Schritte aus, um das Protokoll für Windows 10-Systeme zu deaktivieren:

Schritt	Aktion
1	Klicken Sie mit der rechten Maustaste auf die Schaltfläche Windows Start , und führen Sie den Befehl System aus.
2	Führen Sie im Menü Einstellungen den Befehl Remotedesktop aus.
3	Deaktivieren Sie in der Ansicht Remotedesktop die Option Remotedesktop aktivieren (Umschalten zu Aus).

Führen Sie für andere Windows-Betriebssysteme entsprechende Verfahren aus.

Aktualisieren von Sicherheitsrichtlinien

Aktualisieren Sie die Sicherheitsrichtlinien auf den PCs in Ihrem System, indem Sie `gpupdate` in einem Befehlsfenster ausführen. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu `gpupdate`.

LANMAN und NTLM deaktivieren

Das Microsoft LAN Manager-Protokoll (LANMAN oder LM) und sein Nachfolger NT LAN Manager (NTLM) weisen Schwachstellen auf, aufgrund derer ihre Verwendung in Steuerungsanwendungen nicht ratsam ist.

Gehen Sie wie folgt vor, um LM und NTLM in einem Windows-System zu deaktivieren:

Schritt	Aktion
1	Führen Sie in einem Befehlsfenster den Befehl <code>secpol.msc</code> aus, um das Fenster Lokale Sicherheitsrichtlinie zu öffnen.
2	Öffnen Sie Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen .
3	Wählen Sie Nur NTLMv2-Antworten senden/ LM NTLM verweigern im Feld Netzwerksicherheit: LAN Manager-Authentifizierungsebene aus.
4	Markieren Sie das Kontrollkästchen Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern .
5	Führen Sie in einem Befehlsfenster den Befehl <code>gpupdate</code> aus, um die geänderte Sicherheitsrichtlinie festzuschreiben.

Verwalten von Updates

Aktualisieren Sie vor der Bereitstellung alle PC-Betriebssysteme mithilfe der Dienstprogramme auf der **Windows Update**-Webseite von Microsoft. Für den Zugriff auf dieses Tool in Windows wählen Sie **Start > Alle Programme > Windows Update** aus.

Prüfung der digitalen Signatur

Überprüfen der Integrität von EcoStruxure Automation Device Maintenance nach dem Download

Nachdem Sie die ausführbare Datei von EcoStruxure Automation Device Maintenance von der Website von Schneider Electric heruntergeladen haben, überprüfen Sie die Integrität der Datei, indem Sie die folgenden Schritte ausführen:

Schritt	Aktion
1	Klicken Sie mit der rechten Maustaste auf die Datei <code>AutomationDeviceMaintenance.exe</code> und führen Sie im Kontextmenü den Befehl Eigenschaften aus.
2	Wählen Sie im Dialogfeld AutomationDeviceMaintenance.exe Properties die Registerkarte Digitale Signaturen .
3	Wählen Sie in der Signaturenliste den Eintrag Schneider Electric USA, INC. aus und klicken Sie auf die Schaltfläche Details , um die Digital Signature Details (Details zu digitalen Signaturen) anzuzeigen.
4	Stellen Sie im Dialogfeld Digital Signature Details (Details zu digitalen Signaturen) sicher, dass die Meldung This digital signature is OK. (Diese digitale Signatur ist OK.) angezeigt wird.

Sie können jetzt auf die .exe-Datei doppelklicken, um EcoStruxure Automation Device Maintenance zu starten.

Prüfen der Komponenten während des Hochfahrens

Beim Start von EcoStruxure Automation Device Maintenance wird jede geladene DLL (Dynamic-Link Library) gescannt, um zu überprüfen, ob sie vertrauenswürdig ist oder nicht. Dies ist eine integrierte Sicherheitsfunktion gegen Cyberangriffe und zur Erhöhung der Vertrauensebene.

Vorgehensweise bei Erkennung nicht vertrauenswürdiger Komponenten

Wenn nicht vertrauenswürdige Komponenten erkannt werden, wird der Start von EcoStruxure Automation Device Maintenance abgebrochen und eine Meldung mit dem Hinweis angezeigt, dass eine Ausnahme erkannt wurde.

In diesem Fall haben Sie die folgenden Optionen:

- Installieren Sie EcoStruxure Automation Device Maintenance neu.
- Wenn Sie den geringsten Verdacht haben, dass dies durch einen Cyberangriff verursacht wurde, rufen Sie das [Schneider Electric Cybersecurity services portal](#) auf, um weitere Beratung oder Unterstützung zu erhalten.

Um die für das Problem verantwortliche Komponente zu identifizieren, können Sie ein Debugging-Tool wie WinDbg verwenden: Starten Sie das Debugging-Tool und dann EcoStruxure Automation Device Maintenance und überwachen Sie den Inhalt der Protokolldatei auf Einträge, die darauf hinweisen, dass die Gültigkeit der Codesignatur einer DLL nicht bestimmt werden kann.

Für eine manuelle Deinstallation erforderliche Dateien

Überblick

Wenn Sie EcoStruxure Automation Device Maintenance auf Ihrem PC deinstallieren, werden Programmdateien automatisch entfernt. Es gibt jedoch einige benutzerspezifische Dateien, die Sie einzeln verarbeiten müssen, um Probleme mit der Cybersicherheit zu vermeiden.

Einstellungsdatei von EcoStruxure Automation Device Maintenance

Die Einstellungsdatei von EcoStruxure Automation Device Maintenance *AutomationDeviceMaintenanceSettings.emes* wird von EcoStruxure Automation Device Maintenance erstellt, um die im Dialogfeld **Einstellungen** vorgenommene Konfiguration zu speichern (z. B. Modbus TCP-Scanbereiche oder Erkennungseinstellungen). Sie wird bei der Deinstallation von EcoStruxure Automation Device Maintenance nicht von Ihrem PC entfernt, sondern muss manuell entfernt werden.

Entfernen Sie die Datei aus dem Ordner *%APPDATA%\Schneider Electric\Automation Device Maintenance*. Verwenden Sie dazu Windows Explorer oder andere Dateisystemtools.

Zertifikate

Das Zertifikat von EcoStruxure Automation Device Maintenance sowie die **Vertrauenswürdigen Zertifikate** und **Nicht vertrauenswürdigen Zertifikate**, die im Dialogfeld **Einstellungen** unter **Sicherheit > Zertifikatmanagement** (auch

Dialogfeld **Zertifikatmanagement**, Seite 44) verwaltet werden, werden bei der Deinstallation von EcoStruxure Automation Device Maintenance vom Windows-PC entfernt. Sie werden auch aus dem Windows-Zertifikatspeicher entfernt.

Datenpakete

Datenpakete, Seite 20, die lokal gespeichert wurden, werden bei der Deinstallation von EcoStruxure Automation Device Maintenance nicht von Ihrem PC entfernt. Standardmäßig werden die Datenpakete im Ordner *%PUBLIC%\Public Documents\Schneider Electric\Data Packages* abgelegt. Sie können Ihren individuellen Pfad im Dialogfeld **Einstellungen > Paketeinstellungen**, Seite 37 konfigurieren.

Entfernen Sie den Standardordner oder den konfigurierten Standardordner manuell in Windows Explorer oder in anderen Dateisystemtools.

Projektdateien von EcoStruxure Automation Device Maintenance

Die Projektdateien von EcoStruxure Automation Device Maintenance werden bei der Deinstallation von EcoStruxure Automation Device Maintenance nicht von Ihrem PC entfernt. Suchen Sie nach Dateien mit der Dateierweiterung **.emep* und entfernen Sie sie manuell oder bewahren Sie sie für eine spätere Verwendung an einem sicheren Ort auf, auf den kein unbefugter Zugriff möglich ist.

Protokolldateien

Die Protokolldateien, die lokal unter dem im Dialogfeld **Einstellungen > Protokolle**, Seite 38 angegebenen Pfad abgelegt wurden, werden bei der Deinstallation von EcoStruxure Automation Device Maintenance nicht von Ihrem PC entfernt. Entfernen Sie den Ordner manuell in Windows Explorer bzw. in anderen Dateisystemtools oder speichern Sie die Protokolldateien zur späteren Verwendung an einem sicheren Ort, auf den kein unbefugter Zugriff möglich ist.



Von EcoStruxure Automation Device Maintenance verwendete Komponenten

Überblick

EcoStruxure Automation Device Maintenance bietet einen Überblick über die Komponenten und die aktuellen Versionen. Wenn eine Ausnahme erkannt wird, kann diese Liste von Komponenten und Versionen bei der Suche nach der Komponente helfen, die die Ursache sein könnte.

Abrufen einer Liste von Komponenten

Gehen Sie wie folgt vor, um eine Liste der Komponenten abzurufen, die von EcoStruxure Automation Device Maintenance geladen werden:

Schritt	Aktion																																	
1	<p>Klicken Sie auf die Schaltfläche Info über  in der Symbolleiste.</p> <p>Ergebnis: Das Dialogfeld Info über wird geöffnet.</p>																																	
2	<p>Klicken Sie auf den Link Komponentenspezifische Informationen.</p> <p>Ergebnis: Das Dialogfeld Komponentenspezifische Informationen wird geöffnet.</p> <div><div>Info über</div><div><div>Komponentenspezifische Informationen</div><table><thead><tr><th>Komponentenname</th><th>Version</th><th>Beschreibung</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>Zurück zu 'Info über' Details kopieren</div><div><div>Life Is On</div><div></div></div><div>OK</div></div></div>	Komponentenname	Version	Beschreibung	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
Komponentenname	Version	Beschreibung																																
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>Klicken Sie auf den Link Details kopieren, um die Liste der Komponenten und Versionen in die Zwischenablage zu kopieren.</p> <p>Sie können den Inhalt jetzt in eine *.txt-Datei einfügen, die Ihnen praktische Suchvorgänge nach bestimmten Komponenten und entsprechenden Versionen ermöglicht.</p>																																	

Glossar

D

Datenpaket, Firmware-Paket:

Ein Datenpaket ist eine Datei, die für den Datenaustausch zwischen einem Werkzeug und Geräten verwendet werden kann. Der Austausch kann im Format SEDP erfolgen. Ein Datenpaket enthält neben Firmware-Paketen u. U. auch Konfigurationen, SPS-Applikationen usw.

DHCP: Dynamic Host Configuration-Protokoll

DNS: Domain Name System

DPWS:

Das Akronym steht für „Device Profile for Web Services“, einem Standard für die Erkennung und Beschreibung von Geräten, die Internetdienste unterstützen.

G

Geräteerkennung:

Die automatische Erkennung von Geräten und Dienstleistungen, die über die jeweiligen Geräte in einem Computer-Netzwerk zur Verfügung stehen.

Gerätefamilie:

Eine Gruppe von Geräten ähnlichen Typs, die anhand einer Produkt-ID erkennbar ist.

Gerätezertifikat:

Ein Public-Key-Zertifikat des Typs X.509, das von einem Werkzeug und einem Gerät für die Einrichtung eines sicheren Kommunikationskanals (z. B.: HTTPs) verwendet wird.

H

HTTP:

Hypertext Transfer Protocol

HTTPs:

Hypertext Transfer Protocol Secure wird auch als HTTP over TLS bezeichnet.

I

ICS: (Industrielle Steuerungs- und Systemtechnik) Industrielle Steuerungs- und Systemtechnik

IEC:

(*International Electrotechnical Commission*) Gemeinnütziges, internationales Normungsgremium, das sich die Ausarbeitung und Veröffentlichung internationaler Normen für die Elektro- und Elektronikindustrie sowie zugehörige Technologien zur Aufgabe gemacht hat.

IP-Adresse:

Die Adresse eines Geräts entsprechend den IP-Protokollstandards. Die Adressen können im Format IPv4 oder IPv6 vorliegen.

IP:

Internetprotokoll

ISO: International Organization for Standardization

N

NEMA:

(*National Electrical Manufacturers Association*) Standard für verschiedene Klassen elektrischer Gehäuse. Die NEMA-Standards befassen sich mit der Korrosionsbeständigkeit, dem Schutz vor Regen, dem Eindringen von Wasser usw. Für IEC-Mitgliedsländer gilt die Norm IEC 60529 mit ihrer Klassifizierung der verschiedenen Schutzarten (IP-Codes) für Gehäuse.

O

OPC UA:

OPC Unified Architecture: OPC UA ist ein Standard für Interoperabilität für den gesicherten und zuverlässigen Datenaustausch in der industriellen Automatisierungstechnik. Es handelt sich um ein plattformunabhängiges Kommunikationsprotokoll, welches das Client/Server-Modell nutzt. Die Verbindung zwischen Client und Server basiert für gewöhnlich auf dem zuverlässigen Transportschichtprotokoll (TCP, Transmission Control Protocol).

Weitere Informationen zu OPC, insbesondere OPC UA, finden Sie auf der offiziellen Website der OPC Foundation unter <https://opcfoundation.org>.

P

PLC:

(*Programmable Logic Controller: Speicherprogrammierbare Steuerung*) Industrieller Computer, der zur Automatisierung von Fabrikations-, Industrie- und anderen elektromechanischen Prozessen eingesetzt wird. SPS (PLCs) unterscheiden sich von allgemein gängigen Computern dadurch, dass sie mit zahlreichen Ein- und Ausgangs-Arrays ausgestattet sind und robusteren Spezifikationen in Bezug auf beispielsweise Erschütterungen, Vibrationen, Temperaturen und elektrischen Störgrößen entsprechen.

POU:

(*Program Organization Unit: Programmierorganisationseinheit*) Variablendeklaration im Quellcode und der entsprechende Anweisungssatz. POU's ermöglichen die modulare Wiederverwendung von Softwareprogrammen, Funktionen und Funktionsbausteinen. Sobald POU's deklariert sind, stehen sie sich gegenseitig zur Verfügung.

Produkt-ID:

Produktkennung, verweist auf die Produktfamilie eines Geräts.

S

SEDP:

Das Akronym steht für „Schneider Electric Data Package“, einem standardisierten Dateiformat für den Datenaustausch zwischen Werkzeugen und Geräten.

T

TCP:

Transmission Control Protocol

TLS:

Transport Layer Security

U

UDP: User Datagram-Protokoll

URL:

Uniform Resource Locator

Index

A		
Abfragehäufigkeit	37	
Abgelehnte Datenpakete	52	
Aktualisieren der Firmware	70	
Aktualisieren der Sicherheitskonfigurationsdatei	72	
Aktualisierungszentrum	69	
Aktualisierungssymbol	26	
Alarm		
Speichern, Löschen	26	
Änderungen auf der Seite Einstellungen	26	
Anmeldedaten	25, 61, 70	
Anmeldung für Firmwareaktualisierung	70	
Ansichten	21	
Anwenden von Änderungen	26	
Anwendungszertifikat	43	
Ausnahme	79	
B		
Benachrichtigungen	67	
Benachrichtigungsbereich	67	
Bestätigungsmeldungen	67	
C		
CA (Certificate Authority)	43	
csv-Datei für den Import	34	
Cybersicherheit	75	
Einführung	75	
Firewall	78	
LAN-Verbindung	78	
LANMAN / NTLM	79	
Netzwerkschnittstellenkarten	77	
Remotedesktop	78	
Richtlinien	77	
Zertifizierungen	75	
D		
Datei AutomationDeviceMaintenanceSettings.		
emes	80	
Daten		
Firmware, Konfigurieren	52	
Datenpaket	51	
Paketname, Paketinformationen	20	
Deinstallation	80	
Dialogfeld Aktualisierungsbestätigung	70	
Dialogfeld Aktualisierungshistorie	70	
Dialogfeld Firmware	70	
Dialogfeld für die Anmeldung	61	
Dialogfeld Projekt geändert	27	
DLL nicht vertrauenswürdig	79	
DPWS-Scanner		
Sonden-Request, Metadaten-Request,		
Netzwerkadapter	36	
E		
Entfernen von Dateien	80	
Entfernen von Zertifikaten	43	
Erkennen		
Manuell, automatisch	25	
Erkennung		
Automatisch, manuell	32	
Erweiterungen	64	
F		
Fehler		
Fehler, Warnung	19	
Speichern, Löschen	26	
Firmware		
Aktualisierung, Geräte/Ladevorgang,		
Datenpaket	70	
Version, Upgrade-Info, Fortschritt	21	
Firmwarepaket		
Paketinformationen, Paketname	18	
fwp-Paketdateien	51	
G		
Gerät		
Aktualisierung, Konfigurationsoptionen,		
Anmeldedaten	61	
Geräte/Ladevorgang		
Gerätename, Status, Datenpaket	21	
Geräteanmeldung Dialogfeld	61	
Geräteerkennung		
Modbus, DPWS (Device Profile for Web Services,		
Geräteprofil für Web-Dienste)	15	
Geräteerkennungsstatus	66	
Gerätezertifikat		
Vertrauenswürdig, nicht vertrauenswürdig	21	
Gesicherte sedps-Paketdateien	51	
Gruppieren von Geräten	56	
Gültige Datenpakete	52	
H		
Hardware		
CPU, RAM, HDD	16	
Häufigkeit der Abfrage	37	
Hinzufügen von Geräten	23	
HTTP/HTTPS-Kommunikation	23	
I		
Import einer csv-Datei	34	
Import einer Konfigurationsdatei	34	
Importieren der		
Sicherheitskonfigurationsdatei	41	
Importieren einer Konfigurationsdatei	34	
Information		
Paket, Produkt	52	
Speichern, Löschen	26	
Installation		
Vorgehensweise, Installationsassistent, Installieren,		
Lizenzvereinbarung	17	
K		
Kennung		
Kopieren	54	
Kommunikationsprotokolle	16	
Komponenten und Versionen	81	
Komponentenspezifische Informationen	81	
Konfiguration		
DPWS-Scanner	36	
Erkennung	32	

Erkennung, Modbus, Paketeinstellung, Sprache, Zertifikate	25	Funktionen, unterstützte Firmwarepakete	15
Kommunikationseinstellungen	37	Speicherort für Pakete	38
Modbus TCP	34	Hinzufügen	38
Speicherorte für Pakete	37	Symbolleiste	19
Konfigurieren		Info, Hilfe, Erkennen	19
Sprache, ändern	40	syslog	49
Kopieren der Kennung	54	Systemanforderungen	
		Hardware, Software, Kommunikationsprotokolle, Bildschirmauflösung, Cybersicherheit	16
L		T	
Idx-Paketdateien	51	TCP	49
Lokales Repository	37	Timeout	
Löschen von Zertifikaten	43	Kommunikationseinstellungen	37
		TLS	49
M		U	
Modbus TCP		Überwachen des Geräteerkennungsstatus	66
Geräte-ID, Ping-Timeout, Port	34	UDP	49
Modbus TCP-Kommunikation	23	Unterstützte Geräte	15
Modulare Geräte	64		
N		V	
Neues Projekt	27	Vertrauen von Zertifikaten	43
Nicht Vertrauen von Zertifikaten	43		
Nicht vertrauenswürdige DLL	79	W	
O		Willkommen-Fenster	
Option Gruppe	56	Datenpaket, Geräte/Ladevorgang, Symbolleiste ...	18
P		Z	
Passwörter	61, 70	Zertifikat	
PKI	48	Validieren, vertrauen, nicht vertrauen, entfernen ...	43
Projekt		Zertifikate	43
Neu	27	Zertifikatmanagement	43
Offen	29	Zertifizierungsstelle (CA)	43
Öffnen, Speichern	19	Zugriff auf Erweiterungen	64
Speichern	28	Zurücksetzen von Anwendungseinstellungen	40
Projektdateien mit nicht identifizierten Geräten	31		
Projektdateien von einem anderen Computer	30		
Protokolle			
Ansichten	68		
Public Key-Infrastruktur (PKI)	48		
R			
Rack-Module	64		
Registerkarte Erweiterungen	64		
Registerkarte Geräte/Ladevorgang	55		
Registrieren des Anwendungszertifikats	43		
S			
Schaltfläche Anwenden	26		
Schaltfläche In Zwischenablage kopieren	54		
Schaltfläche OK	26		
SD-Speicherkarte	21		
sedp-Paketdateien	51		
sedps-Paketdateien	51		
Sicherheitsfunktionen	41		
Sicherheitskonfigurationsdatei	41, 72		
Software			

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, ist es unerlässlich, dass Sie die in dieser Veröffentlichung gegebenen Informationen von uns bestätigen.

© 2022 Schneider Electric. Alle Rechte vorbehalten.

EIO0000004046.04