

EcoStruxure Automation Device Maintenance

Outil de mise à niveau du micrologiciel

Aide en ligne

EIO0000004048.04
11/2022

Mentions légales

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce guide sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs. Ce guide et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce guide ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce guide ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Les produits et équipements Schneider Electric doivent être installés, utilisés et entretenus uniquement par le personnel qualifié.

Les normes, spécifications et conceptions sont susceptibles d'être modifiées à tout moment. Les informations contenues dans ce guide peuvent faire l'objet de modifications sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

En tant que membre d'un groupe d'entreprises responsables et inclusives, nous actualisons nos communications qui contiennent une terminologie non inclusive. Cependant, tant que nous n'aurons pas terminé ce processus, notre contenu pourra toujours contenir des termes standardisés du secteur qui pourraient être jugés inappropriés par nos clients.

© 2022 - Schneider Electric. Tous droits réservés.

Table des matières

Consignes de sécurité.....	5
Qualification du personnel	5
Instructions d'utilisation	6
Avant de commencer	6
Démarrage et test.....	7
Fonctionnement et réglages	8
Précautions de sécurité.....	8
A propos de ce document.....	10
Introduction	15
Présentation.....	15
Configuration système requise	16
Installation	17
Mise en route	18
Ecran de bienvenue.....	18
Interface utilisateur de EcoStruxure Automation Device	
Maintenance	20
Package de données	20
Equipement/Chargement	21
Ajouter un équipement.....	23
Configuration des paramètres.....	25
Fenêtre des erreurs et avertissements	26
Création d'un projet EcoStruxure Automation Device Maintenance.....	27
Enregistrement du projet.....	28
Ouverture du projet.....	29
Configuration de l'outil EcoStruxure Automation Device	
Maintenance	32
Configuration du mode de découverte des équipements.....	32
Configuration du scrutateur Modbus TCP	34
Configuration du scrutateur DPWS	36
Configuration des paramètres de communication.....	37
Configuration des emplacements de package.....	37
Affichage des fichiers journaux	38
Configuration de la langue.....	40
Réinitialisation des paramètres d'application.....	40
Configuration des fonctions de sécurité	41
Fonctions de sécurité.....	41
Gestion des certificats.....	43
Gestion de l'infrastructure à clé publique (PKI)	48
Activation de la journalisation des messages Syslog	49
Package de données.....	51
Onglet Package de données	51
Equipement/Chargement	55
Onglet Equipement/Chargement	55
Regroupement d'équipements dans la LISTE D'EQUIPEMENTS	56
Suppression d'équipement.....	57
Gestion des identifiants d'utilisateur	61

Accès aux extensions	64
Surveillance du statut de la découverte d'équipements	66
Affichage / confirmation des messages	67
Affichage des journaux.....	68
Centre de mise à jour	68
Mise à jour du micrologiciel	69
Mise à jour du fichier de configuration de la sécurité	71
Cybersécurité	74
Qu'est-ce que la cybersécurité ?	74
Consignes Schneider Electric	76
Vérification de la signature numérique.....	78
Fichiers nécessitant une désinstallation manuelle	79
Composants utilisés par EcoStruxure Automation Device	
Maintenance	80
Glossaire	83
Index	86

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.



La présence de ce symbole sur une étiquette "Danger" ou "Avertissement" signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.



Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

Remarque Importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

Qualification du personnel

Une personne qualifiée est une personne qui a les qualifications suivantes :

- Compétences et connaissances liées à la construction et à l'exploitation d'équipements électriques et à l'installation.
- Connaissances et expérience en programmation de contrôle industriel.

- A reçu une formation en sécurité permettant de reconnaître et d'éviter les dangers potentiels.

La personne qualifiée doit être capable de détecter d'éventuels dangers qui pourraient découler du paramétrage, de modifications des valeurs de paramétrage et plus généralement des équipements mécaniques, électriques ou électroniques. La personne qualifiée doit connaître les normes, dispositions et réglementations liées à la prévention des accidents de travail, et doit les observer lors de la conception et de l'implémentation du système.

Instructions d'utilisation

Ce produit est une bibliothèque destinée à être utilisée avec les systèmes de commande et les segments de moteur à stator long, aux seules fins décrites dans la présente documentation concernant le secteur industriel.

Observez en permanence les instructions applicables liées à la sécurité, les conditions spécifiques et les données techniques.

Réalisez une analyse des risques en rapport avec l'utilisation spécifique avant d'utiliser ce produit. Prenez les mesures de sécurité qui découlent des résultats.

Étant donné que ce produit est utilisé au sein d'un système qui l'englobe, vous devez assurer la sécurité du personnel par la conception même du système global (la conception de la machine, par exemple).

Aucune autre utilisation n'est prévue. Toute autre utilisation pourrait être dangereuse.

Avant de commencer

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

▲ AVERTISSEMENT

EQUIPEMENT NON PROTEGE

- N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.
- N'accédez pas aux machines pendant leur fonctionnement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automatisme et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE: La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

Démarrage et test

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

⚠ AVERTISSEMENT

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

Fonctionnement et réglages

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 (la version anglaise prévaut) :

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit dérégulé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.
- Seuls ces réglages fonctionnels, requis par l'opérateur, doivent lui être accessibles. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

Précautions de sécurité

Durant l'installation ou l'utilisation de ce logiciel, lisez bien les messages de sécurité affichés dans le logiciel et indiqués dans la documentation. Les messages de sécurité suivants s'appliquent à l'intégralité de ce logiciel.

⚠ AVERTISSEMENT

RISQUES DE FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

- N'utilisez pas ce logiciel pour des applications critiques de contrôle ou de protection dans lesquelles la sécurité des humains et des équipements repose sur le fonctionnement des actions de contrôle.
- N'utilisez pas le logiciel pour contrôler des fonctions temporisées cruciales. Des retards de communication peuvent se produire entre l'activation d'un contrôle et l'application de l'action.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

RISQUES D'INEXACTITUDE DES RÉSULTATS DE DONNÉES

- Configurez le logiciel correctement pour obtenir des rapports et/ou des résultats de données précis.
- N'effectuez pas les actions de maintenance ou de service uniquement en fonction des messages et des informations affichés par le logiciel.
- Ne vous fiez pas seulement aux messages et rapports du logiciel pour déterminer si le système fonctionne correctement ou respect les normes et exigences.
- Considérez les implications liées aux délais de transmission ou aux erreurs des liaisons de communication.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT**RISQUES POTENTIELS POUR LA DISPONIBILITÉ, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DU SYSTÈME**

Respectez les meilleures pratiques en matière de cybersécurité.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

NOTE: Pour plus d'informations sur la cybersécurité, reportez-vous au chapitre *Cybersécurité*, page 74.

A propos de ce document

Objectif du document

Ce document décrit l'outil EcoStruxure Automation Device Maintenance. EcoStruxure Automation Device Maintenance peut transférer des micrologiciels depuis un PC vers des équipements Schneider Electric pris en charge. Cet outil permet de détecter les équipements concernés dans le réseau, mais aussi de les identifier manuellement si la découverte automatique n'est pas possible.

Champ d'application

Ce document a été mis à jour pour EcoStruxure Automation Device Maintenance version 3.1.

Les caractéristiques décrites dans le présent document, ainsi que celles décrites dans les documents à consulter mentionnés ci-dessous, sont accessibles en ligne. Pour accéder aux informations en ligne, allez sur la page d'accueil de Schneider Electric www.se.com/ww/en/download/. Pour la documentation EcoStruxure Automation Device Maintenance, tapez *EcoStruxure Automation Device Maintenance* dans la zone de texte de recherche et appuyez sur la touche **Entrée**.

Les caractéristiques décrites dans le présent document doivent être identiques à celles fournies en ligne. Toutefois, en application de notre politique d'amélioration continue, nous pouvons être amenés à réviser le contenu du document afin de le rendre plus clair et plus précis. Si vous constatez une différence entre le document et les informations fournies en ligne, utilisez ces dernières en priorité.

Document(s) à consulter

Titre de documentation	Numéro de référence
Firmware Compatibility Rules, Modicon M580, Modicon Momentum, and Modicon X80 I/O Modules	EIO0000002634 (English)
Plates-formes automate Modicon - Cybersécurité, Manuel de référence	EIO0000001999 (English) EIO0000002001 (French) EIO0000002000 (German) EIO0000002003 (Spanish) EIO0000002002 (Italian) EIO0000002004 (Chinese)
Guide de spécifications et d'implémentation Modbus, Manuel de référence	Modbus Application Protocol Specification
Spécification DPWS (Devices Profile for Web Services), Manuel de référence	WSDD-DPWS

Titre de documentation	Numéro de référence
EcoStruxure™ Control Expert, Modes de fonctionnement	33003101 (English)
	33003102 (French)
	33003103 (German)
	33003104 (Spanish)
	33003696 (Italian)
	33003697 (Chinese)
EcoStruxure Automation Device Maintenance Altivar - Manuel utilisateur	JYT50472 (English)
	JYT50474 (French)
	JYT50482 (German)
	JYT50476 (Spanish)
	JYT50478 (Italian)
	JYT50483 (Chinese)
	JYT50484 (Turkish)
	JYT50485 (Portuguese)

Information spécifique au produit

⚠ AVERTISSEMENT
<p>PERTE DE CONTROLE</p> <ul style="list-style-type: none"> Le concepteur d'un système de commande doit envisager les modes de défaillance possibles des chemins de commande et, pour certaines fonctions de commande critiques, prévoir un moyen d'atteindre un état sécurisé en cas de défaillance d'un chemin, et après cette défaillance. Par exemple, l'arrêt d'urgence, l'arrêt en cas de surcourse, la coupure de courant et le redémarrage sont des fonctions de commande cruciales. Des canaux de commande séparés ou redondants doivent être prévus pour les fonctions de commande critiques. Les chemins de commande système peuvent inclure les liaisons de communication. Une attention particulière doit être prêté aux implications des délais de transmission non prévus ou des pannes de la liaison. Respectez toutes les réglementations de prévention des accidents ainsi que les consignes de sécurité locales.¹ Chaque implémentation de cet équipement doit être testée individuellement et entièrement pour s'assurer du fonctionnement correct avant la mise en service. <p>Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.</p>

¹ Pour plus d'informations, consultez le document NEMA ICS 1.1 (dernière édition), « Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control » (Directives de sécurité pour l'application, l'installation et la maintenance de commande statique) et le document NEMA ICS 7.1 (dernière édition), « Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems » (Normes de sécurité relatives à la construction et manuel de sélection, installation et opération de variateurs de vitesse) ou son équivalent en vigueur dans votre pays.

Avant de tenter de fournir une solution (machine ou processus) pour une application spécifique en utilisant les POU trouvés dans la bibliothèque, vous devez tenir compte de la réalisation et de l'exécution des bonnes pratiques. La liste non exhaustive de ces pratiques liées à cette bibliothèque inclut l'analyse des risques, la sécurité fonctionnelle, la compatibilité des composants, les tests et la validation du système.

⚠ AVERTISSEMENT

UTILISATION INCORRECTE DES UNITES ORGANISATIONNELLES DU PROGRAMME

- Effectuez une analyse de la sécurité de l'application et des équipements installés.
- Vérifiez que les POU sont compatibles avec les équipements du système et n'ont pas d'effets inattendus sur le bon fonctionnement du système.
- Utilisez les paramètres appropriés, notamment les valeurs limites, et observez l'usure de la machine et son comportement à l'arrêt.
- Vérifiez que les capteurs et déclencheurs sont compatibles avec les POU sélectionnés.
- Testez de manière approfondie toutes les fonctions durant la vérification et la mise en service dans tous les modes de fonctionnement.
- Indiquez des méthodes indépendantes pour les fonctions de contrôle critiques (arrêt d'urgence, conditions des valeurs limites dépassées, etc.) conformément à une analyse de sécurité, aux règles en vigueur et aux réglementations applicables.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les transferts incomplets, qu'il s'agisse de fichiers de données, d'application et/ou de micrologiciel, peuvent avoir des conséquences graves sur votre machine ou votre contrôleur. En cas coupure de courant (volontaire ou non) ou d'interruption de la communication pendant un transfert de fichier, votre machine peut devenir inopérante ou votre application peut tenter d'utiliser un fichier de données endommagé. En cas d'interruption, relancez le transfert. Veillez à inclure l'impact des fichiers de données endommagés dans votre analyse des risques.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT, PERTE DE DONNEES OU FICHIER ENDOMMAGE

- N'interrompez pas un transfert de données en cours.
- Si le transfert est interrompu pour une raison quelconque, relancez-le.
- Ne mettez pas votre machine en service tant que le transfert de fichier n'est pas terminé, sauf si vous avez pris en compte les fichiers endommagés dans votre analyse des risques et si vous avez mis en place des mesures appropriées pour prévenir les conséquences potentiellement graves dues à des échecs de transfert.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

L'utilisation de cette bibliothèque comme outil de contrôle d'une machine nécessite une attention et des dispositions particulières afin d'éviter des conséquences involontaires dues à l'exploitation de la machine commandée, à des changements d'état ou à l'altération de la mémoire de données ou des éléments de fonctionnement de la machine.

⚠ AVERTISSEMENT

FUNCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

- Placer les instruments de l'opérateur du système de commande près de la machine ou à un endroit qui permet d'avoir une vision parfaite de la machine.
- Protégez les commandes opérateur contre tout accès non autorisé.
- Si le contrôle à distance est une caractéristique nécessaire de l'application, veillez à ce qu'une personne qualifiée et compétente soit présente sur place pour surveiller le fonctionnement contrôlé à distance.
- Configurez et installez l'entrée Run/Stop (si elle est présente) ou un autre moyen externe dans l'application, afin que le contrôle local du démarrage ou de l'arrêt de l'équipement puisse être maintenu indépendamment des commandes envoyées à distance à l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant dans ou sur les produits proviennent généralement des normes internationales.

Dans les domaines des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, les termes employés sont *sécurité, fonction de sécurité, état sécurisé, défaut, réinitialisation du défaut, dysfonctionnement, panne, erreur, message d'erreur, dangereux*, etc.

Entre autres, les normes concernées sont les suivantes :

Norme	Description
IEC 61131-2:2007	Automates programmables - Partie 2 : exigences et essais des équipements
ISO 13849-1:2015	Sécurité des machines : parties des systèmes de commande relatives à la sécurité. Principes généraux de conception
EN 61496-1:2013	Sécurité des machines : équipements de protection électro-sensibles. Partie 1 : Prescriptions générales et essais
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Équipement électrique des machines - Partie 1 : règles générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
IEC 62061:2015	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmable relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité : prescriptions générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité : exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité : exigences concernant les logiciels.
IEC 61784-3:2016	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain de sécurité fonctionnelle - Règles générales et définitions de profils.
2006/42/EC	Directive Machines
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes peuvent être utilisés dans le présent document car ils proviennent d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* utilisé dans le contexte de la description de dangers spécifiques a la même signification que les termes *zone dangereuse* ou *zone de danger* employés dans la *directive Machines (2006/42/EC)* et la norme *ISO 12100:2010*.

NOTE: Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Introduction

Présentation

Introduction

EcoStruxure Automation Device Maintenance permet de mettre à niveau les packages de micrologiciel sur plusieurs équipements en même temps. Les équipements peuvent être détectés automatiquement ou ajoutés manuellement si la découverte automatique n'est pas prise en charge ou est désactivée sur l'équipement.

Voici les méthodes possibles de découverte des équipements :

- Code de fonction Modbus 43 (identification d'équipement)
- DPWS (Device Profile for Web Services)

Caractéristiques

EcoStruxure Automation Device Maintenance prend en charge les fonctionnalités suivantes :

- Découverte automatique des équipements
- Identification manuelle des équipements
- Fonctions de sécurité
- Mise à jour du micrologiciel pour plusieurs équipements simultanément
- Gestion des adresses IP

Equipements Schneider Electric pris en charge

Equipements Modicon :

- Modicon M340
- Modicon M580
- Modicon Momentum
- Modules d'E/S Modicon X80

Equipements Altivar :

- Familles de produits Altivar
 - Variateurs Altivar Process ATV6••
 - Variateurs Altivar Process ATV9••
 - Variateurs Altivar Machine ATV340
- Modules en option Altivar :
 - VW3A3720 Ethernet
 - VW3A3721 MultiDrive-Link
 - VW3A3530D ATV dPAC
- Démarreurs progressifs Altivar :
 - Altivar ATS480

Configuration système requise

Configuration matérielle requise

Composant	Spécifications minimales
Processeurs	Intel® Core i3 ou version ultérieure
RAM	Minimum 4 Go, recommandé : 8 Go ou plus
Disque dur	500 Mo d'espace disque disponible

Configuration logicielle requise

- Microsoft Windows® 10 Professionnel 32 bits/64 bits, ou version ultérieure
- Microsoft Windows Server 2016 standard 64 bits
- Microsoft Windows Server 2019 standard 64 bits

Protocoles de communication

L'outil prend en charge les protocoles suivants :

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

Résolution d'écran

Pour afficher le logiciel avec la meilleure résolution d'écran, utilisez la résolution de 1920 x 1080 pixels. La résolution minimale requise est 1280 x 1024 pixels.

Cybersécurité

Les ports suivants sont utilisés par le logiciel :

- DPWS (via le port 3702)
- FTP (via les ports 20, 21)
- HTTP (via le port 80) / HTTPS (via les ports 443 et 8080)
- Modbus (via le port 502)
- OPC UA (via le port 4840)

⚠ AVERTISSEMENT

RISQUES POTENTIELS POUR LA DISPONIBILITÉ, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DU SYSTÈME

Respectez les meilleures pratiques en matière de cybersécurité.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

NOTE: Pour plus d'informations sur la cybersécurité, reportez-vous au chapitre *Cybersécurité*, page 74.

Installation

Procédure

Vous pouvez installer le logiciel en téléchargeant les fichiers d'installation via le site Web *Schneider Electric*.

NOTE: Avant de double-cliquer sur le fichier *AutomationDeviceMaintenance.exe*, vérifiez l'intégrité du fichier comme expliqué dans le chapitre *Vérification de la signature numérique*, page 78.

NOTE: Vous devez disposer des droits administrateur pour installer le logiciel.

Pour installer le logiciel, procédez comme suit :

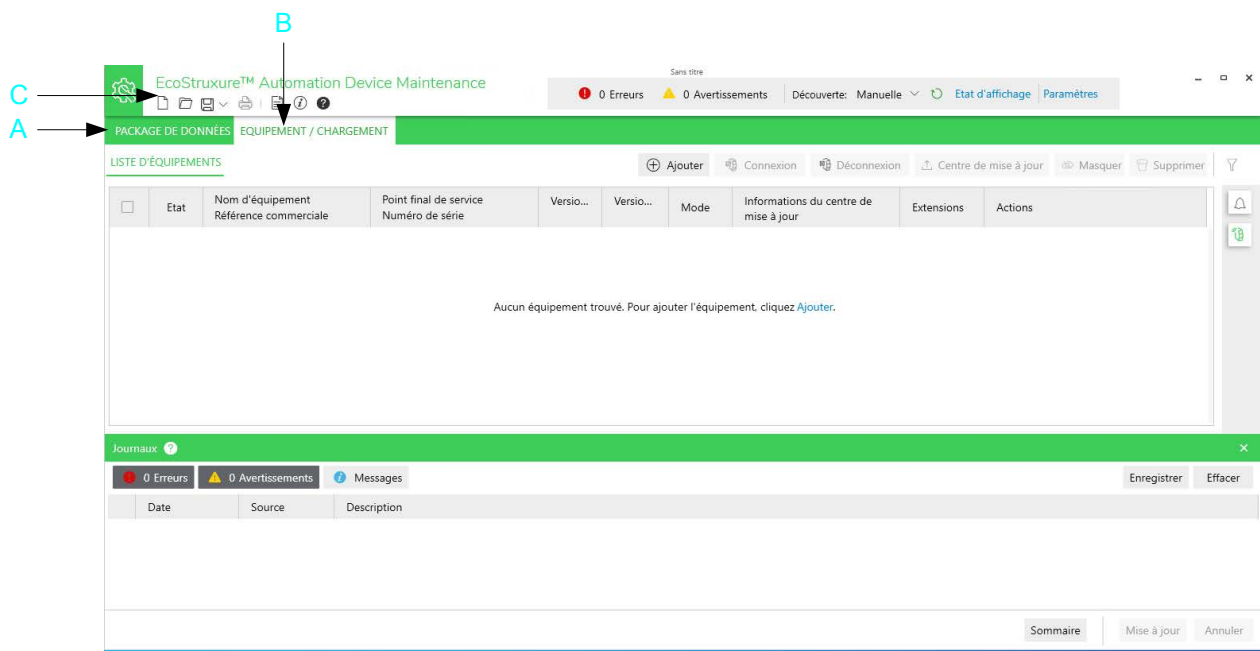
Étape	Action
1	Recherchez les fichiers d'installation à l'aide de Windows Explorer après avoir téléchargé les fichiers.
2	Double-cliquez sur le fichier de configuration <i>EcoStruxure Automation Device Maintenance</i> . L'écran Assistant InstallShield s'affiche.
3	Suivez les indications de l' Assistant InstallShield pour effectuer l'installation.

Mise en route

Ecran de bienvenue

Présentation











Après le démarrage initial, EcoStruxure Automation Device Maintenance affiche l'écran suivant pour la mise à niveau des packages de micrologiciel sur plusieurs équipements. Lorsque vous fermez l'outil, l'état actuel de l'interface utilisateur est enregistré. Par conséquent, lorsque vous démarrerez à nouveau EcoStruxure Automation Device Maintenance, il affichera la vue qui était en cours lors de sa dernière fermeture.



Elément	Nom	Fonction
A	Package de données	Affichage du contenu du référentiel du package de données.
B	Equipement/Chargement	Affichage des informations sur les équipements détectés ou manuellement identifiés.
C	Barre d'outils	Affichage du groupe d'icônes permettant d'exécuter des fonctions.

Barre d'outils

La barre d'outils permet d'accéder aux fonctions générales du logiciel EcoStruxure Automation Device Maintenance.

Elément	Nom	Description
	Nouveau projet	Permet de créer un nouveau projet EcoStruxure Automation Device Maintenance, page 27.
	Ouvrir	Permet d'ouvrir un existing project, page 29.
	Enregistrer	Permet d'enregistrer les project settings, page 28.
	Imprimer	Fonction non disponible dans cette version.
	Journaux	Permet d'afficher les informations du journal.
	A propos de	Accès à : <ul style="list-style-type: none"> Informations sur EcoStruxure Automation Device Maintenance Détails de la copie Contrat de licence Informations sur les composants Informations système
	Aide	Accès à l'aide en ligne.
	Erreur	Affichage des erreurs détectées , page 26.
	Avertissement	Affichage des avertissements détectés , page 26.
	Découverte	Lancer la découverte des équipements lorsqu'elle est en mode Manuel .
–	Manuel / Automatique	Sélectionner le mode de découverte Manuel ou Automatique dans la liste. Pour plus d'informations, voir la section <i>Configuration du mode de découverte des équipements</i> , page 32.
–	Paramètres	Configurer les paramètres.

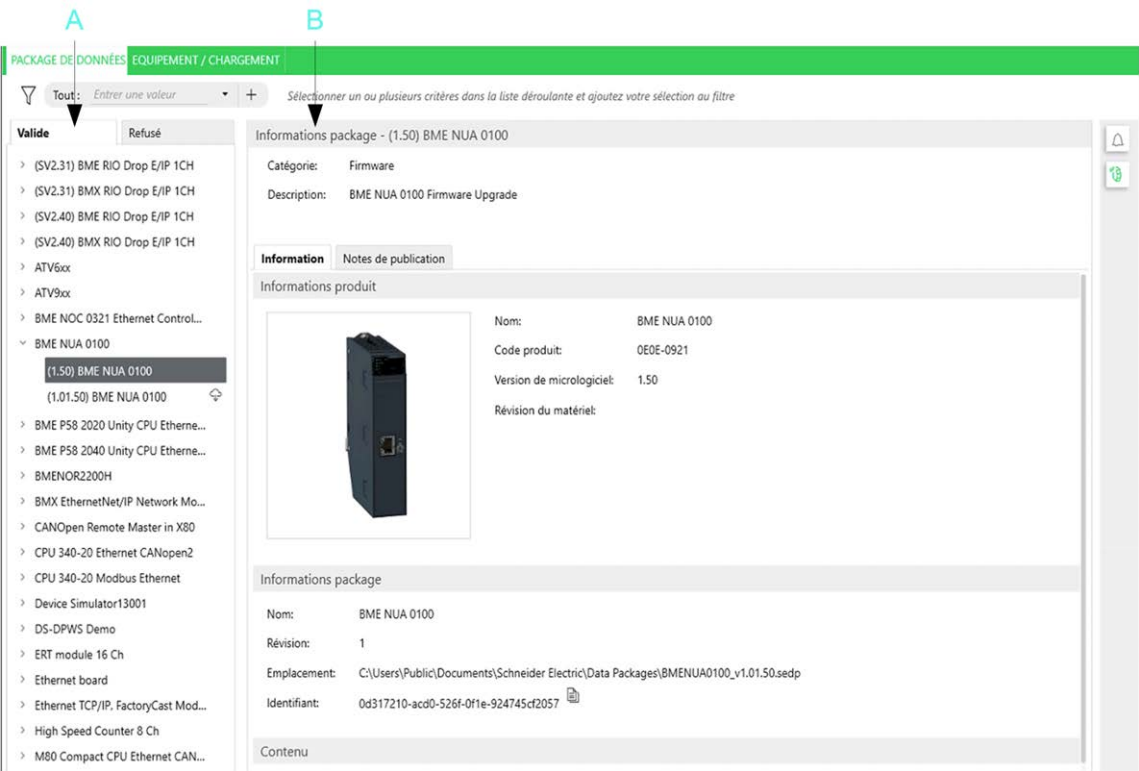
Boutons

Bouton	Description
Résumé	Après avoir effectué une mise à jour, cliquez sur le bouton Résumé pour récupérer les informations sur les équipements mis à jour.
Mise à jour	Après avoir défini les paramètres de mise à jour du micrologiciel, page 69 ou de mise à jour du fichier de configuration de la sécurité, page 71, cliquez sur le bouton Mise à jour pour lancer le processus de mise à jour tel que configuré.
Annuler	Le bouton Annuler vous permet d'annuler une opération de mise à jour.

Interface utilisateur de EcoStruxure Automation Device Maintenance

Package de données

La fonction **Package de données** contient le référentiel du package et affiche les packages du micrologiciel disponibles dans l'outil.



Elément	Nom	Description
A	Liste PACKAGE DE DONNEES avec les onglets Validé et Refusé	Affiche la liste des packages de micrologiciel disponibles localement. Les packages disponibles dans le réseau sont affichés si le module complémentaire requis est installé. Pour plus d'informations, reportez-vous à la section qui décrit l'onglet <i>Package de données</i> , page 51.
B	Informations sur le package	Affiche la description et le contenu du package de données sélectionné, avec dans la partie supérieure des informations statiques concernant la Catégorie et la Description et dans la partie inférieure les onglets Informations et Notes de publications . Pour plus d'informations, reportez-vous à la section qui décrit l'onglet <i>Package de données</i> , page 51.

Equipement/Chargement

Présentation



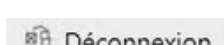





L'onglet **Equipement/Chargement** affiche les détails des équipements connus de l'outil.

NOTE: Les informations affichées dans cet onglet ne sont mises à jour automatiquement que si le mode de détection est défini sur **Automatique**.

Cliquez sur l'icône  de la barre d'outils pour afficher les dernières valeurs.









PACKAGE DE DONNÉES EQUIPEMENT / CHARGEMENT									
LISTE D'EQUIPEMENTS									
<div>Ajouter Connexion Déconnexion Centre de mise à jour Masquer Supprimer</div>									
<input type="checkbox"/>	Etat	Nom d'équipement Référence commerciale	Point final de service Numéro de série	Versio...	Version d...	Mode	Informations du centre de mise à jour	Extensions	Actions
<input checked="" type="checkbox"/>		Groupe par défaut de l'équipement (7)							
<input checked="" type="checkbox"/>		ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-			
<input type="checkbox"/>		ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64767000N	3.5IE94B04	-	-			
<input type="checkbox"/>		ATV930U07M3_b3a CR: ATV930U07M3	mbap://1fe80c280:14ff:feb3:aa7d:502 SN: 4030000HL704004007	3.5IE94B04	-	-			



Boutons de l'onglet :

Bouton	Description
	Cliquez sur le bouton Ajouter pour ajouter un nouvel équipement. Pour plus d'informations, reportez-vous à la section Ajouter un équipement , page 23.
	Cliquez sur le bouton Connecter pour établir une connexion aux équipements sélectionnés.
	Cliquez sur le bouton Déconnecter pour mettre fin à la connexion aux équipements sélectionnés.
	Cliquez sur le bouton Centre de mise à jour pour ouvrir la boîte de dialogue Centre de mise à jour . Elle vous permet de configurer des paramètres pour effectuer une mise à jour de micrologiciel ou une mise à jour du fichier de configuration de la sécurité pour les équipements sélectionnés. Pour plus d'informations, reportez-vous à la section Centre de mise à jour , page 68.
	Cliquez sur le bouton Masquer pour masquer les équipements détectés. Pour plus d'informations, reportez-vous à la section Vue Equipement/Chargement , page 55.
	Cliquez sur le bouton Mettre au rebut pour supprimer les équipements détectés. Pour plus d'informations, reportez-vous à la section Vue Equipement/Chargement , page 55.
	Cliquez sur le bouton Zone de notification pour afficher la zone de notification à droite de l'onglet Equipement/Chargement . Pour plus d'informations, reportez-vous à la section Affichage/confirmation des messages , page 67.
	Cliquez sur le bouton Statut de la découverte d'équipements pour afficher la vue Statut de la découverte d'équipements à droite de l'onglet Equipement/Chargement . Pour plus d'informations, reportez-vous à la section Surveillance du statut de la découverte d'équipements , page 66.

Eléments du tableau :

Elément	Description
Groupe	Vous pouvez affecter les équipements affichés dans la LISTE D'EQUIPEMENTS à différents groupes, comme décrit dans le chapitre Regroupement d'équipements dans la LISTE D'EQUIPEMENTS , page 56. Pour sélectionner tous les équipements appartenant à un groupe , cochez la case du groupe .
Cases à cocher	Cochez plusieurs cases à gauche pour effectuer la même opération sur plusieurs équipements simultanément, par exemple Connecter / Déconnecter ou des opérations de mise à jour.

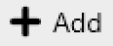
Elément	Description
Etat	Indique l'état de l'équipement : <ul style="list-style-type: none"> Gris : L'équipement est déconnecté du réseau. Jaune : L'équipement est connecté au réseau mais les identifiants valides n'ont pas été saisis. Vert : Des identifiants valides ont été saisis. Bleu : L'outil est en train de charger du contenu sur l'équipement. Rouge : L'équipement est en train de redémarrer après un téléchargement de micrologiciel afin d'achever l'installation.
Nom d'équipement Référence commerciale	Affiche le nom et la référence commerciale (CR) de l'équipement. NOTE : Si vous avez attribué un Pseudonyme à votre équipement, ce nom défini par l'utilisateur s'affiche uniquement si le protocole de communication prend en charge ce paramètre. Modbus TCP, par exemple, ne le prend pas en charge.
Point final de service Numéro de série	Affiche l'adresse du point final de service sous forme d'URI (Uniform Resource Identifier) et le numéro de série (SN) de l'équipement.
Version de micrologiciel	Affichage de la version actuelle du micrologiciel de l'équipement.
Mode	Disponible uniquement après connexion : Indique le mode de l'équipement : RUN, STOP, BUSY, NOCONF, RESERVED, ENTERED, LOADING, COMPLETED, REQUIRERESTART, ERROR . Le contenu de cette cellule est actualisé périodiquement. NOTE : Selon le nombre d'équipements auxquels vous êtes connecté, la surveillance du mode peut avoir un impact sur la bande passante de votre réseau.
Informations du centre de mise à jour	Affiche les paramètres de mise à jour qui ont été configurés dans la boîte de dialogue Centre de mise à jour : Micrologiciel sélectionné, Configuration de sécurité sélectionnée, La mise à jour de micrologiciel a réussi, La mise à jour de micrologiciel a été annulée, La mise à jour de micrologiciel a échoué . Pour plus d'informations, reportez-vous à la section Centre de mise à jour , page 68.
Extensions	Les équipements modulaires disposent d'une liaison (Extensions) qui vous permet d'accéder aux différentes extensions de l'équipement. Pour plus d'informations, reportez-vous à la section Accès aux extensions , page 64.
Actions	Des icônes permettent d'effectuer différentes opérations spécifiques à l'équipement :
	Cliquez sur l'icône Définir les identifiants de connexion et entrez les informations d'identification permettant de se connecter à l'équipement dans la boîte de dialogue Définir les identifiants de connexion . L'icône noire indique qu'aucun identifiant de connexion n'est stocké pour l'équipement. L'icône jaune indique que des identifiants ont été stockés, mais qu'aucune connexion à l'équipement n'a été effectuée. Vous pouvez également configurer des informations d'identification globales pour le projet via Paramètres > Projet > Paramètres d'identification utilisateur . Pour plus d'informations, reportez-vous à la section Gestion des identifiants d'utilisateur , page 61.
	L'icône Définir les identifiants de connexion verte indique que les identifiants correspondant à l'équipement ont été validés et que la connexion a réussi.
	L'icône Définir les identifiants de connexion rouge indique que la tentative de connexion à l'équipement a échoué. Effectuez à nouveau la procédure de connexion et veillez à utiliser les identifiants corrects.
	Cliquez sur l'icône Connecter / Déconnecter pour établir ou terminer une connexion à l'équipement.
	Cliquez sur l'icône Centre de mise à jour pour ouvrir la boîte de dialogue Centre de mise à jour . Elle vous permet de configurer des paramètres pour effectuer une mise à jour de micrologiciel ou une mise à jour du fichier de configuration de la sécurité pour l'équipement. Pour plus d'informations, reportez-vous à la section Centre de mise à jour , page 68.
	Cliquez sur l'icône Journal d'équipement pour afficher les informations du journal.
	Cliquez sur l'icône Démarrer équipement pour démarrer l'équipement. NOTE : Effectuez un test de démarrage avant d'utiliser un équipement de commande électrique et d'automatisation en mode d'exploitation normale après une installation ou une mise à jour. Pour plus d'informations, reportez-vous à la section Démarrage et test , page 7.
	Affiche l'état du certificat. <ul style="list-style-type: none"> Gris : Certificat approuvé Rouge : Certificat non approuvé Cliquez sur l'icône Certificat d'équipement pour ouvrir la boîte de dialogue Informations sur le certificat . Pour plus d'informations, reportez-vous à la section Gestion de l'état d'approbation des certificats dans l'onglet Équipement/Chargement , page 47.

Elément	Description
	Indique que l'équipement est équipé d'une carte mémoire SD. Cliquez sur cette icône pour télécharger le logiciel directement vers la carte mémoire SD.
	Cliquez sur l'icône Options matérielles supplémentaires pour afficher la liste des commandes disponibles pour les équipements après une connexion réussie. Pour plus d'informations, reportez-vous à la section <i>Détails disponibles après connexion</i> , page 56.
Avancement	Indique l'état d'avancement de la mise à jour du micrologiciel.

Ajouter un équipement

Présentation

Vous accédez à la boîte de dialogue **Ajouter un appareil** en cliquant sur le

bouton  **Add** dans l'onglet **Equipement/Chargement** ou en cliquant sur le lien **Aucun appareil trouvé. Pour ajouter l'équipement, cliquez ici** qui s'affiche lorsque la liste d'équipements est vide, par exemple si vous créez un nouveau projet.

Ajouter l'équipement

Rechercher la référence commerciale

Référence commerciale:*

140***
140*** (modernisé)
171***
171*** (modernisé)
ATS***
ATS*** (modernisé)
ATV***
ATV*** (modernisé)

Connexion:*

HTTP/HTTPS

☒ Sécuriser


Adresse IP:*

172.10.15.25

x

:

443

 Remarque : Modernisé = commercialisé après 2019.
Pour en savoir plus, consultez le [Catalogue des produits Schneider Electric](#)

Ajouter l'équipement

Annuler

Elle vous permet d'ajouter manuellement des équipements s'ils ne peuvent pas être détectés automatiquement par EcoStruxure Automation Device Maintenance, soit parce que l'équipement ne prend pas en charge la fonction de découverte, soit parce que cette fonction est désactivée. Pour cela, sélectionnez la référence commerciale.

Par défaut, la liste des **Références commerciales** contient uniquement des modèles de références commerciales (par exemple **BME*****, **BMX***** ou **Tout équipement**). Dans ce cas, vous avez deux options :

- Sélectionnez le modèle correspondant à votre produit : Par exemple, pour BMEP582020, sélectionnez **BME***** dans la liste.

NOTE: Deux variantes sont fournies pour chaque modèle : l'ancienne version (par exemple, **BME*****) et la version récente (par exemple, **BME*** (modernisé)**). Elles diffèrent au niveau des protocoles pris en charge. Par conséquent, si vous ne trouvez pas le protocole de votre choix dans la liste **Connexion**, sélectionnez la deuxième option fournie pour votre produit.

- Pour remplir la liste avec les références commerciales des équipements que vous utilisez, copiez les packages de données correspondants dans le dossier que vous avez configuré en tant que **Référentiel local** dans la boîte de dialogue **Paramètres > Paramètres de package**. (Pour plus de détails, reportez-vous au chapitre [Configuration des emplacements de package](#), page 37.) Le tableau affichera alors des références spécifiques (telles que **BMEP582020** ou **BMXNOR0200**).

Composant	Description
Référence commerciale	Sélectionnez le numéro de référence commerciale de votre équipement dans la liste et entrez les informations appropriées en fonction du protocole sélectionné dans la liste Connexion à droite.
Connexion	<p>Sélectionnez dans la liste le protocole utilisé pour la communication :</p> <ul style="list-style-type: none"> • HTTP/HTTPS • MODBUS (SL) • MODBUS (TCP) • OPC UA • FTP • USB <p>Les paramètres sont adaptés au protocole sélectionné.</p>
Sécuriser	<p>Cette option n'est disponible que pour la communication HTTP/HTTPS :</p> <p>Sélectionnez l'option si l'équipement est connecté via une connexion sécurisée (HTTPS).</p>
Adresse IP	Entrez l'adresse IP de l'équipement que vous ajoutez ainsi que le port utilisé pour la communication.
ID d'unité	<p>Cette option n'est disponible que pour la communication MODBUS (TCP) :</p> <p>Entrez le noeud d'identification de l'unité pour la communication Modbus TCP.</p> <p>Pour plus d'informations sur les spécifications Modbus, consultez Modbus Specifications and Implementation Guides.</p>

NOTE: EcoStruxure Automation Device Maintenance V3.1 et les versions ultérieures prennent en charge l'ajout d'équipements par référence commerciale. Si vous essayez d'ouvrir des fichiers de projet créés avec EcoStruxure Automation Device Maintenance V3.0 ou des versions antérieures qui contiennent des équipements sans référence commerciale, vous serez invité à sélectionner une référence commerciale pour chaque équipement inconnu.

Voir aussi [Ouverture du projet](#), page 29.

Configuration des paramètres

Présentation

La page **Paramètres** vous permet de configurer des paramètres généraux.

Paramètres

Global

Découverte

DPWS

Modbus TCP

Communication

Configuration package

Sécurité

Gestion du certificat

PKI

Syslog

Journaux

Langue

Groupe

Projet

?

Réinitialiser

Découverte

Mode de découverte: ☒ Manuelle ☐ Automatique

Scrutateur	<input checked="" type="checkbox"/> Activer le scrutateur	Etat
DPWS	<input checked="" type="checkbox"/>	Inactif
Modbus TCP	<input checked="" type="checkbox"/>	Inactif


OK

Annuler

Appliquer

Composants	Description
Découverte	Sélectionnez cette option pour configurer le mode de découverte. Pour plus d'informations, voir Configuration du mode de découverte des équipements, page 32.
DPWS	Sélectionnez cette option pour configurer les informations relatives au scrutateur DPWS. Pour plus d'informations, voir Configuration du scrutateur DPWS, page 36.
Modbus TCP	Sélectionnez cette option pour configurer les informations relatives au scrutateur Modbus. Pour plus d'informations, voir Configuration du scrutateur Modbus TCP, page 34.
Communication	Sélectionnez cette option pour configurer les paramètres de communication. Pour plus d'informations, voir Configuration des paramètres de communication, page 37.
Paramètres de package	Sélectionnez cette option pour configurer les paramètres de package. Pour plus d'informations, voir Configuration des emplacements de package, page 37.
Sécurité	Sélectionnez cette option pour activer le mode de protection et afficher des notifications concernant les fonctions de sécurité telles que la communication chiffrée à l'aide de certificats, les packages sécurisés ou la prise en charge de syslog. Pour plus d'informations, voir Fonctions de sécurité, page 41.
Gestion de certificats	Sélectionnez cette option pour inscrire le certificat d'application EcoStruxure Automation Device Maintenance et gérer l'état d'approbation des certificats numériques des partenaires de communication. Pour plus d'informations, voir Gestion des certificats, page 43.
PKI	Sélectionnez cette option pour configurer l'infrastructure à clé publique (PKI). Pour plus d'informations, voir Gestion de l'infrastructure à clé publique (PKI), page 48.
Journaux	Sélectionnez cette option pour afficher les fichiers journaux EcoStruxure Automation Device Maintenance et configurer les paramètres du journal. Pour plus d'informations, voir Affichage des fichiers journaux, page 38.
Langue	Sélectionnez cette option pour configurer la langue souhaitée. Pour plus d'informations, voir Configuration de la langue, page 40.
Groupe	Sélectionnez cette option pour regrouper les équipements affichés dans la LISTE D'EQUIPEMENTS . Pour plus d'informations, voir Regroupement d'équipements dans la LISTE D'EQUIPEMENTS, page 56.
Projet > Paramètres d'identification utilisateur	Sélectionnez cette option pour saisir des informations d'identification globales pour les équipements du projet. Pour plus d'informations, voir Gestion des identifiants d'utilisateur, page 61.

Application des modifications

Chaque fois que vous modifiez des paramètres dans un onglet de la page **Paramètres**, cet onglet est signalé par l'icône d'actualisation  indiquant que des modifications de cette page n'ont pas encore été appliquées.

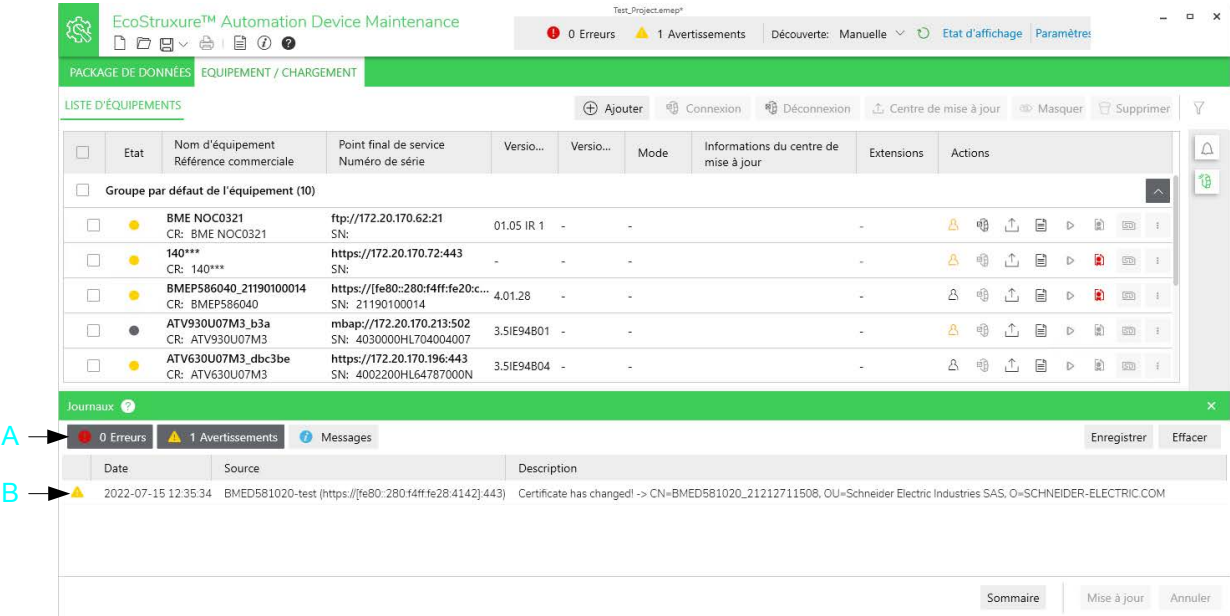
Pour appliquer les modifications à cette page, cliquez sur le bouton **Appliquer**.

Pour appliquer les modifications effectuées dans tous les onglets et fermer la page **Paramètres**, cliquez sur le bouton **OK**.

Fenêtre des erreurs et avertissements

Présentation

Vous pouvez afficher les informations détaillées relatives aux erreurs détectées dans l'outil, dans une fenêtre d'affichage des journaux. Les journaux d'erreur fournissent des informations permettant de corriger les erreurs détectées sur l'équipement sélectionné. La mise à jour du micrologiciel n'est possible que si toutes les erreurs détectées ont été résolues.



Elément	Nom	Description
A	Etat des erreurs et avertissements	Affichage du nombre d'erreurs et d'avertissements détectés.
B	Journaux	Affichage du nombre d'erreurs et d'avertissements détectés avec la description.

Affichage des journaux d'erreurs et d'avertissements

Étape	Action
1	<p>Cliquez sur l'état Erreurs ou Avertissements dans la barre d'outils.</p> <p>La fenêtre Journaux affiche les informations suivantes :</p> <ul style="list-style-type: none">Nombre d'erreurs détectées, avertissements détectés, et informations.Description des erreurs détectées.
2	<p>Sélectionnez les messages d'erreur, d'avertissement ou d'information qui vous intéressent.</p>




Étape	Action
3	Cliquez sur Enregistrer pour enregistrer l'erreur détectée, l'avertissement détecté et les messages d'informations que vous avez sélectionnés.
4	Cliquez sur Effacer pour supprimer du journal tous les messages relatifs aux erreurs et avertissements détectés.

Création d'un projet EcoStruxure Automation Device Maintenance

Procédure

Cette option permet de créer un projet EcoStruxure Automation Device Maintenance.

Procédez comme suit pour créer un projet :

Étape	Action
1	<p>Cliquez sur l'icône .</p> <p>Résultat : La boîte de dialogue Projet modifié s'affiche si un projet ouvert qui a été modifié n'a pas encore été enregistré.</p>
2	<p>Dans la boîte de dialogue Projet modifié, cliquez sur Oui pour enregistrer les modifications apportées au projet ouvert ou sur Non pour fermer le projet sans l'enregistrer.</p> <div><div>Projet modifié</div><div> Le projet en cours comporte des modifications non sauvegardées</div><div>Voulez-vous enregistrer le projet en cours ?</div><div> <input type="button" value="Oui"/> <input type="button" value="Non"/> <input type="button" value="Annuler"/></div></div> <p>Résultat : Le projet ouvert est fermé et un nouveau projet s'ouvre sur l'onglet Équipement/Chargement où la liste d'équipements est vide.</p>


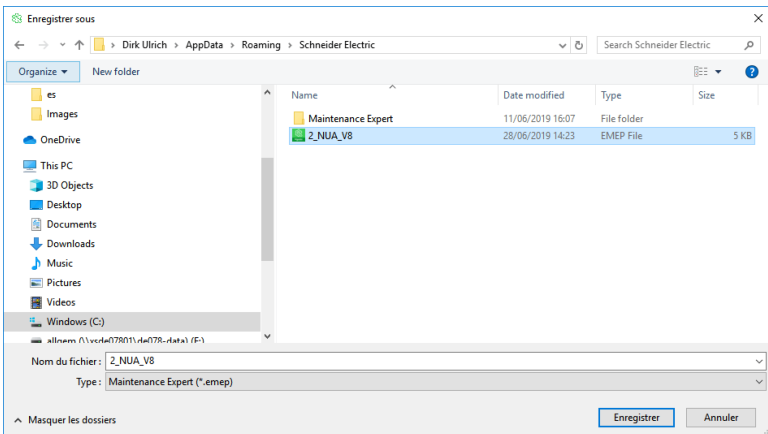
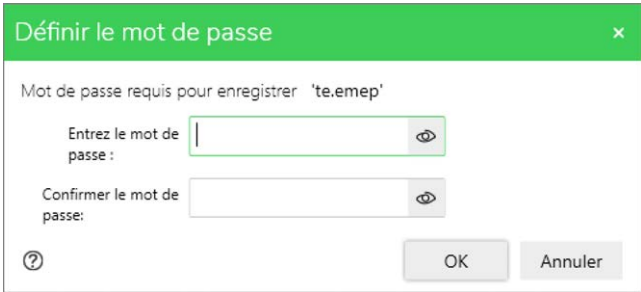
Lorsque vous créez un nouveau projet, les tâches suivantes sont exécutées automatiquement :

- Le mode de découverte est réglé sur **Manuel**.
- Les entrées du fichier journal sont effacées.

Enregistrement du projet

Cette fonction permet d'enregistrer une copie du projet en cours sous un autre nom ou dans un autre emplacement. Elle vous évite de devoir ajouter à nouveau les équipements chaque fois que vous ouvrez l'outil EcoStruxure Automation Device Maintenance.


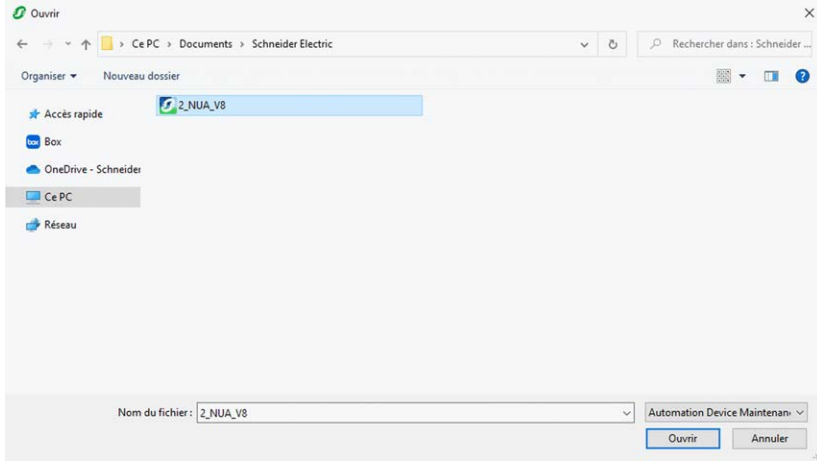

Pour enregistrer les paramètres du projet, procédez comme suit :

Étape	Action
1	Cliquez sur l'icône  .
2	Pour enregistrer les modifications du projet en cours, cliquez sur Enregistrer . Pour enregistrer une copie du projet, cliquez sur Enregistrer sous .
3	Sélectionnez le dossier où enregistrer le projet et entrez le nom du fichier dans Nom de fichier . 
4	Cliquez sur Enregistrer et entrez le même mot de passe dans les deux champs de la boîte de dialogue Définir le mot de passe . 
5	Cliquez sur OK pour continuer.

Ouverture du projet

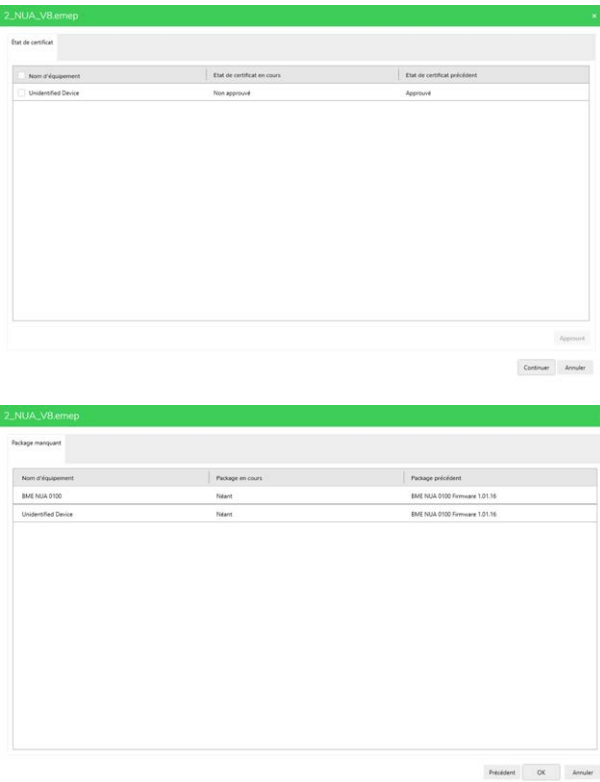
Ouverture d'un projet

Pour ouvrir un projet, procédez comme suit :

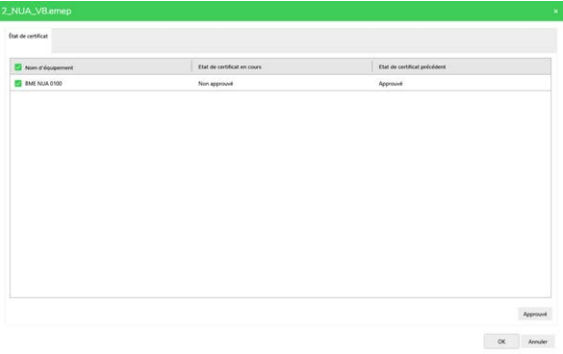
Étape	Action
1	<p>Cliquez sur l'icône .</p> 
2	<p>Sélectionnez le dossier et le projet. Cliquez sur Ouvrir et entrez le mot de passe.</p> 
3	<p>Cliquez sur OK pour ouvrir le projet.</p>

Etapas facultatives pour les fichiers de projet créés sur un autre ordinateur

Si vous essayez d'ouvrir un fichier de projet qui a été créé sur un autre ordinateur, l'outil indique éventuellement les différences de statut d'approbation des certificats et les différences de disponibilité des packages.



Dans ce cas, procédez comme suit :

Étape	Action
4	Sélectionnez les équipements que vous souhaitez approuver et cliquez sur Approuvé .
5	Cliquez sur Continuer . 
6	Cliquez sur OK pour ouvrir le projet avec les packages manquants ou cliquez sur Annuler .

Etape facultative pour les fichiers de projet contenant des équipements non identifiés

Si vous essayez d'ouvrir des fichiers de projet créés avec EcoStruxure Automation Device Maintenance V3.0 ou une version antérieure qui contiennent des équipements sans référence commerciale, une boîte de dialogue vous invite à sélectionner une référence commerciale pour chaque équipement inconnu :

Unidentified_3.0.1.emep

Le projet contient des équipements dont la référence commerciale est inconnue.
Vérifiez la sélection par défaut ci-dessous ou sélectionnez une autre référence commerciale dans la liste déroulante.

i Le projet a probablement été créé avec une version plus ancienne d'EcoStruxure Automation Device Maintenance.
L'option permettant d'ajouter manuellement des équipements non identifiés n'est plus prise en charge dans cette version.

Point final de service	Référence commerciale
COM3/255	ATV***
mbap://145.0.0.1:502	ATV***
mbap://145.0.0.2:502	ATV***

i Remarque : Modernisé = commercialisé après 2019.
Pour en savoir plus, consultez le [Catalogue des produits Schneider Electric](#).

OK Annuler

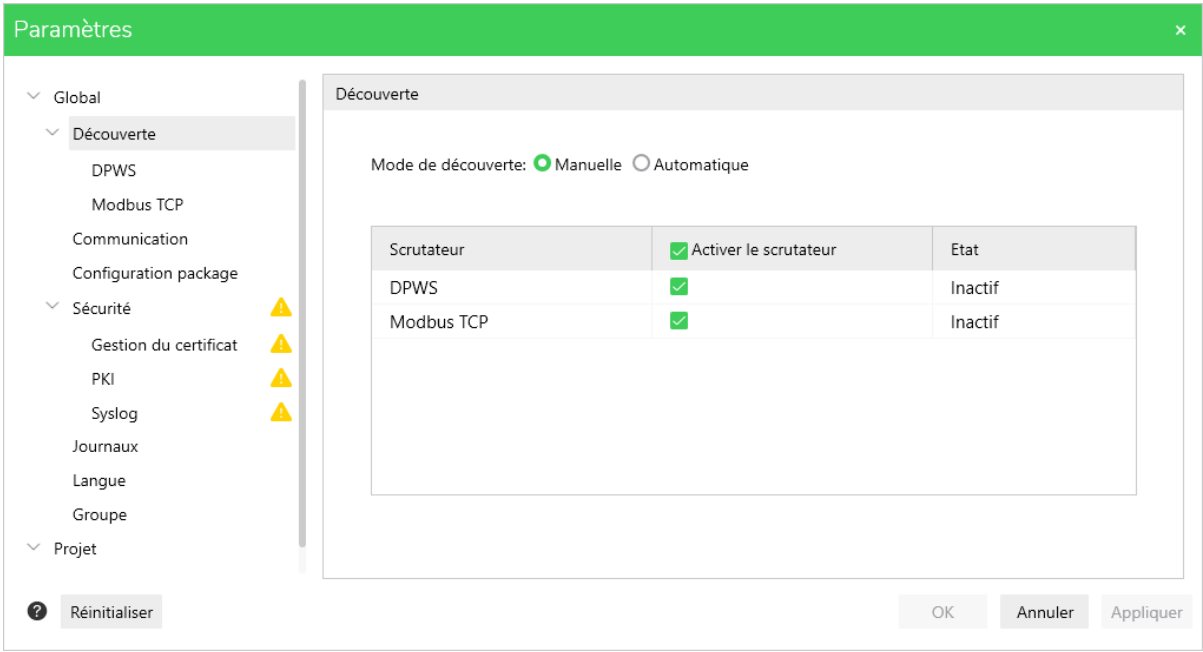
Sélectionnez les références commerciales de votre choix et cliquez sur **OK** pour ouvrir le projet.

Configuration de l'outil EcoStruxure Automation Device Maintenance

Configuration du mode de découverte des équipements

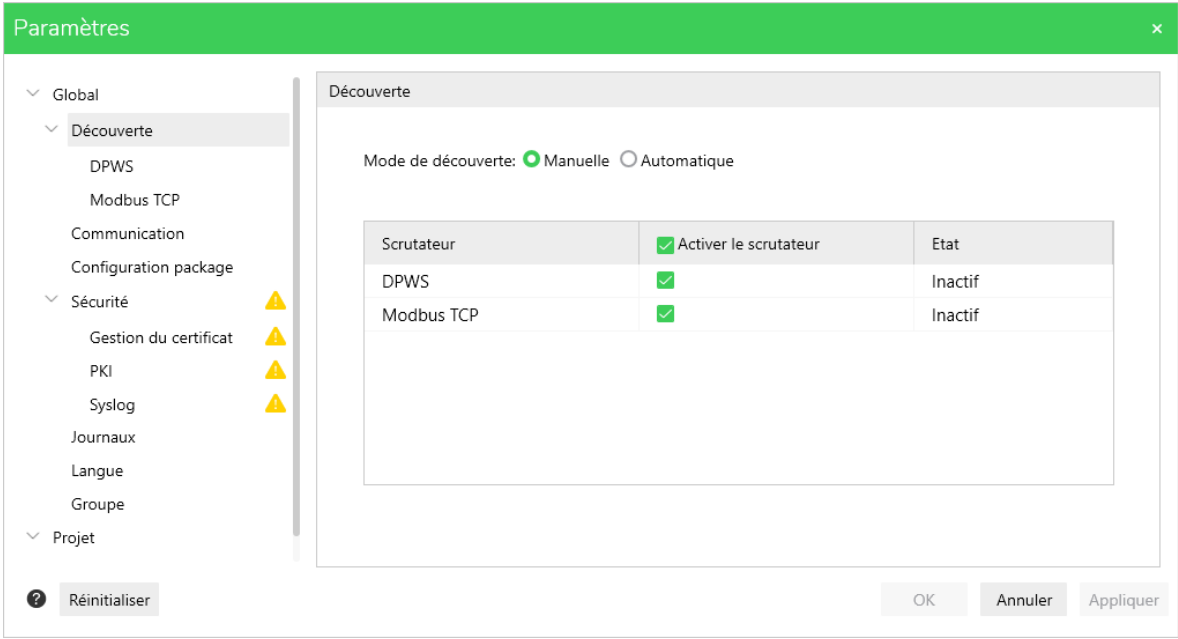
Configuration du mode de découverte automatique

Vous pouvez sélectionner le mode de découverte **Automatique** ou **Manuelle**. Si la découverte est définie sur **Automatique**, l'outil envoie régulièrement des informations via le réseau en arrière-plan et reçoit des informations des équipements qui répondent.

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	<p>Cliquez sur l'option Découverte.</p> 
3	Sélectionnez le mode Automatique .
4	Sélectionnez les scrutateurs à utiliser lors de la découverte. Utilisez ce paramètre pour empêcher la scrutation des équipements que vous souhaitez éviter.
5	Cliquez sur Appliquer puis sur OK .

Configuration du mode de découverte manuel

Vous pouvez sélectionner le mode de découverte manuel (**Manuelle**) pour détecter les équipements reliés au réseau lorsque cela est nécessaire.

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Cliquez sur l'option Découverte . 
3	Sélectionnez le mode Manuel .
4	Sélectionnez les scrutateurs à utiliser lors de la découverte. Utilisez ce paramètre pour empêcher la scrutation des équipements que vous souhaitez éviter.
5	Cliquez sur Appliquer puis sur OK .

Configuration du scrutateur Modbus TCP

Présentation

Le scrutateur **Modbus TCP** envoie des requêtes Modbus de code de fonction 43 à toutes les adresses IP d'une plage définie par une **Adresse IP de début** et une **Dernière adresse IP**.

Vous pouvez configurer les paramètres **Modbus TCP** suivants :

Élément	Valeur par défaut	Description
Section Adresse IP :		
Paramètre Nom de plage	–	Nom (facultatif) de la plage d'adresses.
Paramètre Adresse IP de début	127.0.0.1	Première adresse de la plage de scrutation d'adresses.
Paramètre Dernière adresse IP	127.0.0.1	Dernière adresse de la plage de scrutation d'adresses.
Bouton Importer	–	<p>Cliquez sur le bouton Importer pour importer un fichier de configuration disponible au format .csv (voir un exemple de fichier de configuration ci-après, page 34).</p> <p>NOTE: Cette commande remplace les paramètres de configuration actuels. Prenez soin de sauvegarder vos paramètres au préalable.</p> <p>Résultat : Une boîte de dialogue Windows Ouvrir un fichier s'ouvre et vous permet de rechercher le fichier csv sur votre réseau. Cliquez sur Ouvrir pour importer les paramètres de configuration contenus dans le fichier. Pour appliquer les nouveaux paramètres, cliquez sur Appliquer ou sur OK.</p>
Bouton + Ajouter	–	<p>Cliquez sur le bouton + Ajouter pour créer une nouvelle plage d'adresses.</p> <p>Résultat : Une nouvelle ligne est ajoutée au tableau, avec :</p> <p>Nom de plage = Par défaut</p> <p>Adresse IP de début = 127.0.0.1</p> <p>Dernière adresse IP = 127.0.0.1</p>
Case à cocher	–	Sélectionnez ou désélectionnez une case à cocher pour inclure ou exclure la plage pour la scrutation Modbus.
Bouton Corbeille	–	Cliquez sur le bouton de la corbeille pour supprimer la plage sélectionnée, c'est-à-dire la ligne correspondante du tableau.
Section Paramètres avancés :		
Paramètre Premier port	502	Premier port de la plage de scrutation de ports.
Paramètre Dernier port	502	Dernier port de la plage de scrutation de ports.
Paramètre Temporisation	4 000	Temps d'attente maximal entre l'envoi d'un ping à l'équipement et la réception de la réponse.
Paramètre ID d'unité	255	ID d'unité Modbus utilisé pour accéder à l'équipement.

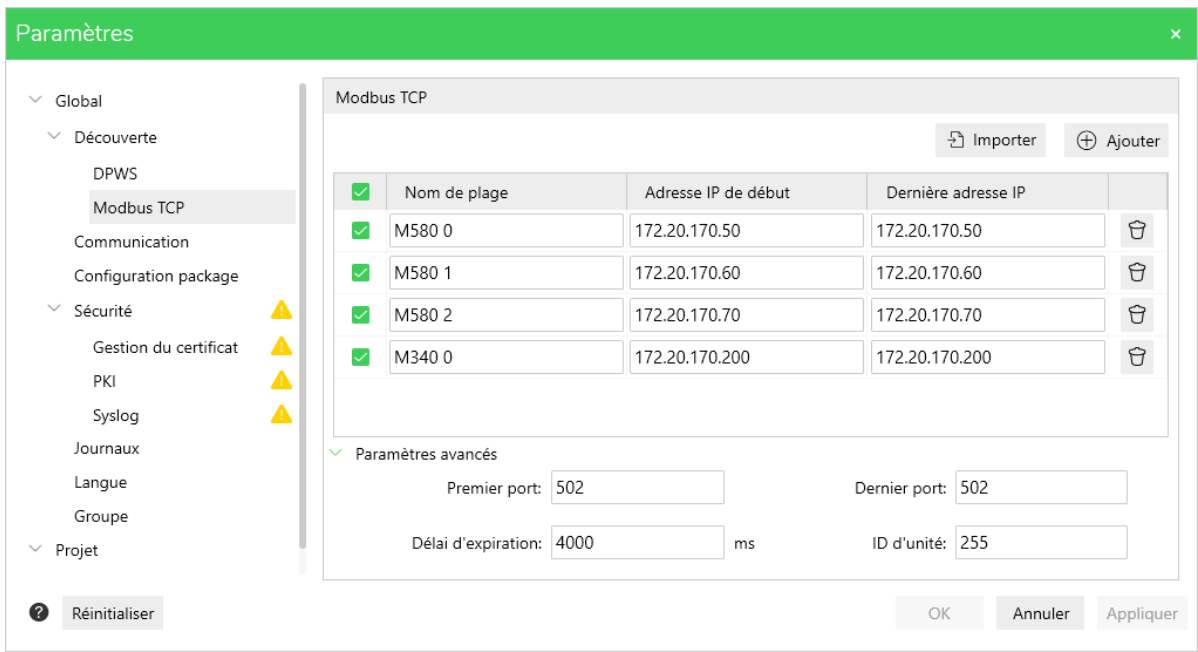
Exemple de fichier d'importation de configuration

Le format du fichier de configuration .csv doit être conforme à l'exemple suivant :

```
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
```

Configuration du scrutateur Modbus TCP

Pour configurer le scrutateur **Modbus TCP**, procédez comme suit :

Étape	Action
1	Développez le menu Découverte sur la page Paramètres .
2	Sélectionnez le noeud Modbus TCP .
3	Dans la vue Modbus TCP de droite, cliquez sur le bouton Ajouter pour créer une nouvelle plage d'adresses.
4	<p>Cliquez sur le bouton Importer pour importer un fichier de configuration ou configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • Nom de plage • Adresse IP de début • Dernière adresse IP • Premier port • Dernier port • Timeout • ID d'unité  <p>The screenshot shows the 'Paramètres' dialog box. On the left is a sidebar with a tree view containing: Global, Découverte (expanded), DPWS, Modbus TCP (selected), Communication, Configuration package, Sécurité (with warning icons), Gestion du certificat (with warning icon), PKI (with warning icon), Syslog (with warning icon), Journaux, Langue, Groupe, and Projet. The main panel is titled 'Modbus TCP' and contains an 'Importer' button and an 'Ajouter' button. Below these is a table with 4 rows, each with a checked checkbox, a 'Nom de plage', an 'Adresse IP de début', a 'Dernière adresse IP', and a trash icon. The rows are: M580 0 (172.20.170.50), M580 1 (172.20.170.60), M580 2 (172.20.170.70), and M340 0 (172.20.170.200). Below the table is a 'Paramètres avancés' section with input fields for 'Premier port' (502), 'Dernier port' (502), 'Délai d'expiration' (4000 ms), and 'ID d'unité' (255). At the bottom are buttons for 'Réinitialiser', 'OK', 'Annuler', and 'Appliquer'.</p>
5	Cliquez sur Appliquer pour appliquer les paramètres Modbus TCP ou cliquez sur OK pour appliquer toutes les modifications des paramètres d'application et fermer la boîte de dialogue Paramètres .

Configuration du scrutateur DPWS

Présentation

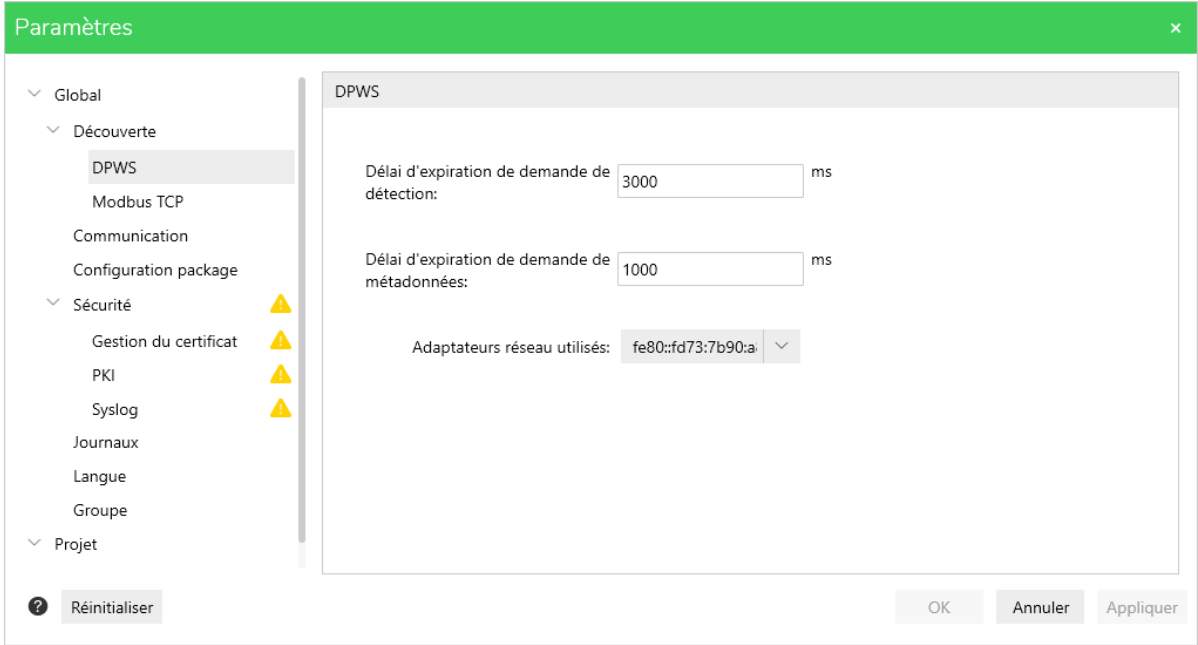
Le scrutateur **DPWS** est une implémentation côté client de la norme **DPWS** qui permet de détecter les équipements conformes à DPWS.

Pour plus d'informations sur les normes DPWS, consultez <http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>.

Vous pouvez configurer les paramètres **DPWS** suivants :

Paramètre	Valeur par défaut	Description
Délai d'expiration de demande de détection	3000 ms	Temps d'attente maximal entre l'envoi d'une demande de détection et la réception des réponses de concordance des équipements.
Délai d'expiration de demande de métadonnées	1000 ms	Temps d'attente maximal entre l'envoi d'une demande de métadonnées et la réception de la réponse de l'équipement.
Adaptateurs réseau utilisés	–	Liste des adaptateurs réseau à utiliser pour l'envoi de la demande d'analyse DPWS .

Suivez les étapes pour configurer le scrutateur **Modbus** :

Étape	Action
1	Développez le menu Découverte sur la page Paramètres .
2	<p>Sélectionnez DPWS et entrez les détails suivants :</p> <ul style="list-style-type: none"> • Délai d'expiration de demande de détection • Délai d'expiration de demande de métadonnées • Adaptateurs réseau utilisés 
3	Cliquez sur Appliquer puis sur OK .

Configuration des paramètres de communication

Présentation

Vous pouvez configurer les paramètres suivants pour la communication entre EcoStruxure Automation Device Maintenance et les équipements :


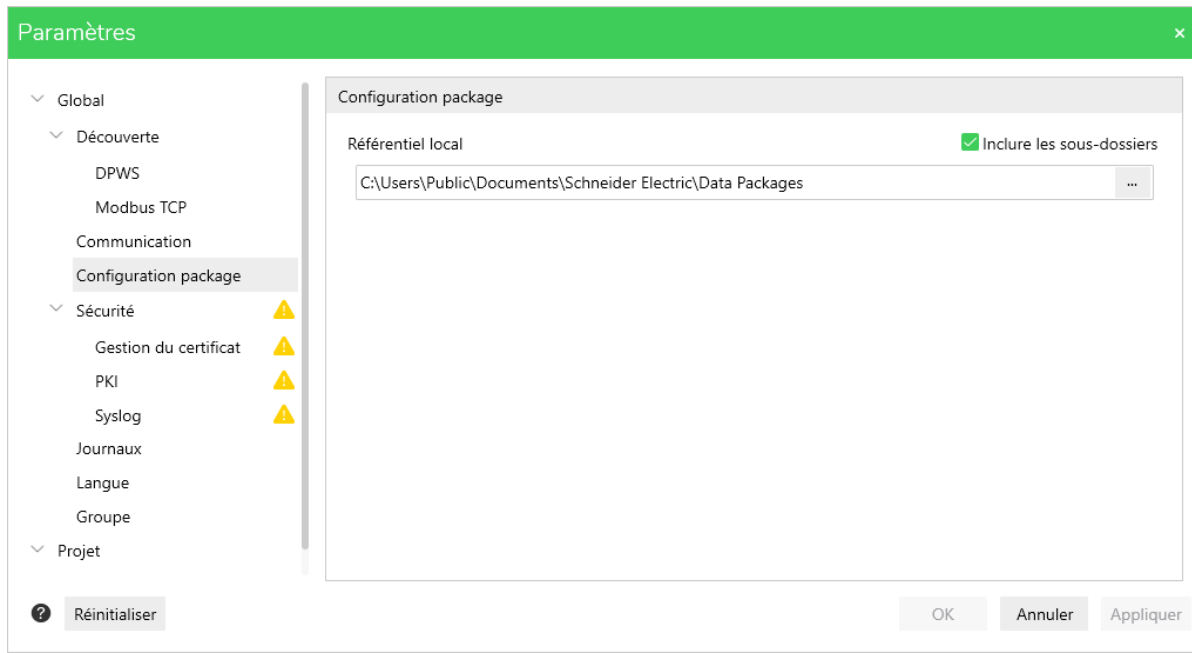
Paramètre	Valeur par défaut	Description
Section Temporisation :		
Timeout	6000 ms	Temps d'attente maximum de la réponse après l'envoi par EcoStruxure Automation Device Maintenance d'une demande (par exemple, mise à jour de micrologiciel, définition de la configuration IP). Pour les temporisations qui s'appliquent aux demandes de détection, consultez <i>Scrutateur Modbus TCP</i> , page 34 et <i>Scrutateur DPWS</i> , page 36.
Section Interrogation automatique de l'état des équipements : Ces paramètres définissent la fréquence d'envoi de requêtes d'interrogation aux équipements détectés afin de maintenir le statut de l'équipement, page 21 à jour :		
Fréquence (priorité élevée) :	3000 ms	L'interrogation de priorité élevée est utilisée lorsque des mises à jour de micrologiciel sont effectuées. Elle permet d'accélérer la détection de l'équipement après son redémarrage.
Fréquence (priorité faible) :	10 000 ms	L'interrogation de faible priorité (cycles moins fréquents) est utilisée pour le fonctionnement normal.

Configuration des emplacements de package

Vous pouvez configurer le chemin des packages de micrologiciel disponibles dans l'outil. Cela permet de mettre à jour les versions de micrologiciel des équipements. Par ailleurs, la référence commerciale spécifique fournie par chaque package de données est ajoutée à la liste **Référence commerciale** dans la boîte de dialogue **Ajouter un appareil**, page 23.

Modification de l'emplacement de package

Pour changer l'emplacement d'un package, procédez comme suit :




Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d'accueil.
2	Sélectionnez l'option Paramètres de package .
3	Sélectionnez le chemin d'accès pour modifier l'emplacement du Référentiel local .
4	<p>Cliquez sur l'icône  et sélectionnez le dossier de destination pour modifier le chemin.</p> 
5	Cliquez sur Appliquer puis sur OK .

Affichage des fichiers journaux

Vous pouvez afficher les journaux stockés et analyser les informations détaillées relatives à l'équipement sélectionné.

Procédez comme suit pour consulter les journaux :

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d'accueil.
2	Sélectionnez l'option Journaux .
3	Configurez la création de journaux : Active/Inactive .
4	Sélectionnez le chemin d'accès du nouvel emplacement du fichier journal.

Étape	Action
5	<p> Cliquez sur l'icône  et sélectionnez le dossier de destination pour modifier le chemin.</p> <div><div>Paramètres</div><div><div><div>Global</div><div>Découverte</div><div>DPWS</div><div>Modbus TCP</div><div>Communication</div><div>Configuration package</div><div>Sécurité</div><div>Gestion du certificat</div><div>PKI</div><div>Syslog</div><div>Journaux</div><div>Langue</div><div>Groupe</div><div>Projet</div></div><div><div>Journaux</div><div><div>Actif</div><div>Inactif</div><div>C:\Users\AdminUser\AppData\Local\Temp\AutomationDeviceMaintenance.log</div><div>...</div><div></div><div> Le fichier journal contient des données sensibles. Supprimez-le après l'avoir utilisé ou stockez-le dans un endroit sécurisé.</div></div></div><div><div>Réinitialiser</div><div>OK</div><div>Annuler</div><div>Appliquer</div></div></div><p>NOTE: Pour plus d'informations sur la notification de cybersécurité, reportez-vous à la section Recommandation pour améliorer la cybersécurité, page 68.</p></div>
6	Cliquez sur Appliquer , puis sur OK .

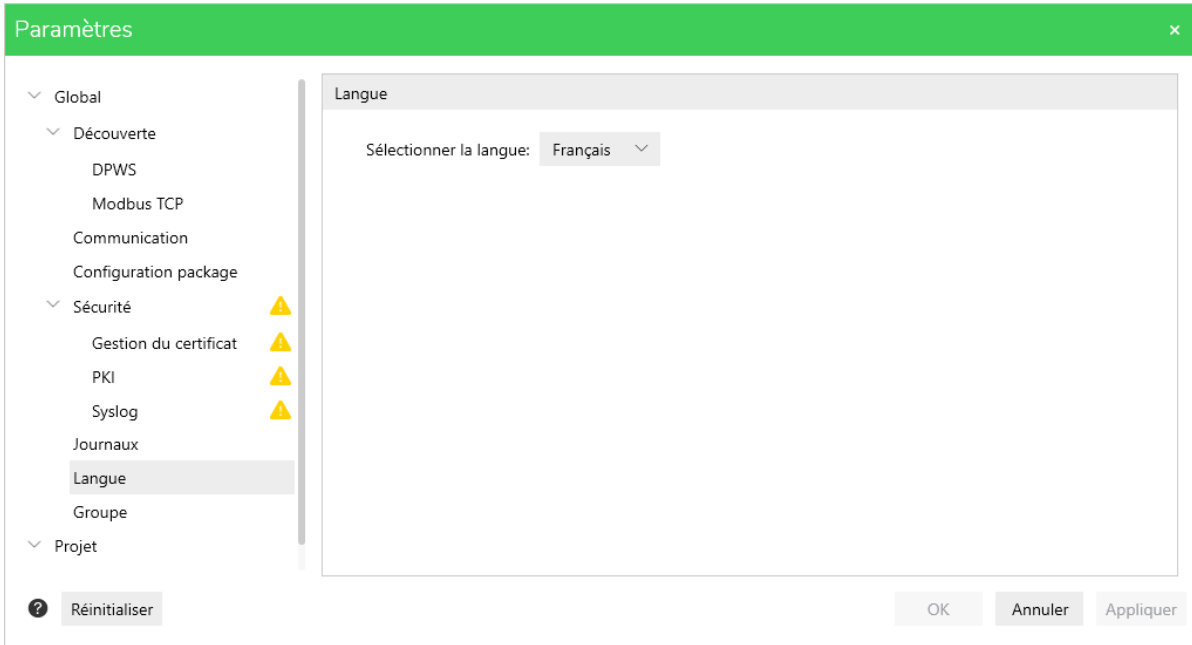
Configuration de la langue

Vous pouvez sélectionner la langue d'affichage du contenu de l'outil EcoStruxure Automation Device Maintenance.

Langues prises en charge :

- Anglais
- Allemand
- Français
- Espagnol
- Italien
- Chinois

Pour définir la langue, procédez comme suit :

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Sélectionnez l'option Langue .
3	<p>Cliquez sur la liste déroulante Sélectionner la langue pour sélectionner la langue souhaitée.</p> 
4	<p>Cliquez sur Appliquer puis sur OK.</p> <p>NOTE: Redémarrez EcoStruxure Automation Device Maintenance pour appliquer les changements de langue.</p>

Réinitialisation des paramètres d'application

Présentation

Les boîtes de dialogue du menu **Paramètres** contiennent un bouton **Réinitialiser** dans le coin inférieur gauche.

Cliquez sur le bouton **Réinitialiser** pour rétablir les valeurs par défaut de tous les paramètres d'application que vous avez configurés à l'aide du menu **Paramètres**.

Configuration des fonctions de sécurité

Présentation

Les recommandations et les solutions de cybersécurité sont en constante évolution. Dès sa conception, Schneider Electric intègre les toutes dernières connaissances et techniques pour rendre les produits plus résilients aux cyberattaques. L'approche intégrant la sécurité dans la conception permet de mettre en œuvre des mécanismes qui limitent les menaces, réduisent les vulnérabilités exploitables et protègent contre les vols de données et les cyberattaques évitables.

NOTE:

Pour sécuriser vos produits Schneider Electric, vous avez tout intérêt à appliquer les recommandations de cybersécurité mentionnées dans le document *Recommandations de cybersécurité* disponible sur le [Schneider Electric website](#).

L'augmentation rapide de l'interconnexion des machines et des usines s'accompagne d'un accroissement tout aussi rapide des menaces potentielles. Il convient donc d'envisager toutes les mesures de sécurité possibles.

Des mesures de sécurité sont nécessaires pour protéger les données et les canaux de communication contre les intrusions.

NOTE: Avant de configurer les fonctions de sécurité, consultez votre administrateur de la sécurité pour vous assurer que vous utilisez les paramètres appropriés.

Fonctions de sécurité

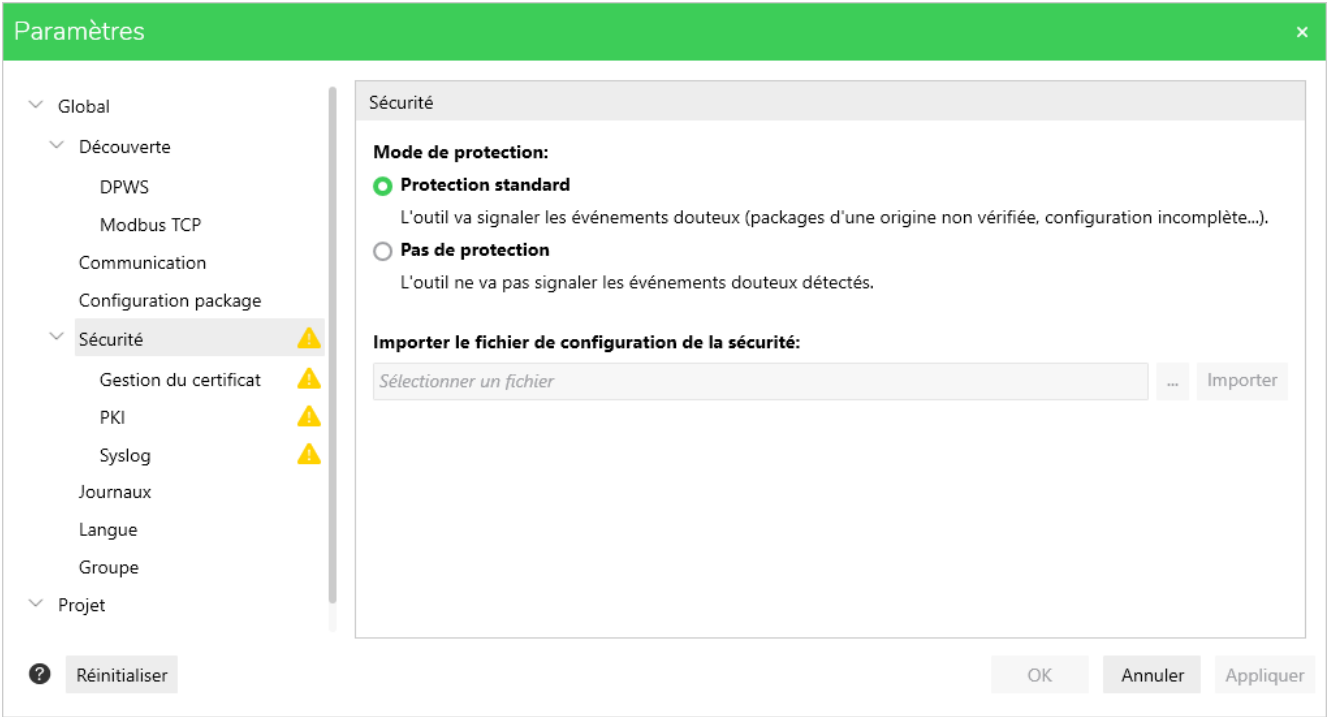
Présentation

EcoStruxure Automation Device Maintenance prend en charge les fonctions de sécurité suivantes :

- Communication cryptée utilisant des certificats numériques dans une infrastructure à clé publique (PKI).
- Gestion des packages de données Schneider Electric sécurisés (SEDPS) signés numériquement.
- Protocole réseau Syslog.

Activation/désactivation du mode de protection

Si vous travaillez au sein d'un réseau protégé et n'utilisez pas de fonctions de sécurité, les notifications concernant les fonctions de sécurité (les points d'exclamation jaunes, par exemple) peuvent être désactivées via l'option **Sécurité** de la page **Paramètres**.



Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Sélectionnez l'option Sécurité .
3	Sélectionnez l'option permettant d'activer le mode de protection et d'afficher les notifications concernant les fonctions de sécurité.

Importation d'un fichier de configuration de sécurité

EcoStruxure Automation Device Maintenance permet d'importer les paramètres de configuration de la sécurité que vous avez configurés globalement pour votre réseau au sein de l'application l'EcoStruxure Cybersecurity Admin Expert. Si ces paramètres sont disponibles sous forme de fichier, procédez comme suit pour importer ce fichier :

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Sélectionnez l'option Sécurité .
3	Dans la section Importer le fichier de configuration de la sécurité , cliquez sur le bouton Importer pour accéder au fichier de configuration de la sécurité.
4	Cliquez sur Ouvrir pour importer les paramètres de configuration de la sécurité contenus dans le fichier.

Pour mettre à jour le fichier de configuration de la sécurité, utilisez le **Centre de mise à jour** comme expliqué dans le chapitre **Mise à jour du fichier de configuration de la sécurité**, page 71.

Gestion des certificats

Présentation

Des certificats numériques sont nécessaires pour la communication sécurisée via les protocoles respectifs (HTTPS par exemple) dans une infrastructure à clé publique (PKI).

Dans le contexte de TLS, les certificats peuvent être utilisés pour vérifier l'identité des partenaires de communication. Ces certificats sont envoyés pendant l'établissement d'une connexion (transfert TLS). L'envoi du certificat est facultatif pour le client (en l'occurrence, le certificat d'application de EcoStruxure Automation Device Maintenance), sauf si le serveur demande le certificat client. Par contre, le serveur envoie systématiquement son certificat. Uniquement si le résultat de la vérification du certificat est positif une connexion avec le partenaire de communication peut être établie.

EcoStruxure Automation Device Maintenance prend en charge les modes d'approbation de certificat suivants :

- Mode d'approbation manuel : Vous pouvez approuver/désapprouver manuellement les certificats des participants à une communication sécurisée. Le statut d'approbation est géré dans les onglets **Certificats approuvés** / **Certificats non approuvés** de la boîte de dialogue **Gestion de certificat**, page 46.
- Mode d'approbation par liste d'autorisation : Vous pouvez importer une liste d'autorisation avec le fichier de configuration de la sécurité, page 42. EcoStruxure Automation Device Maintenance approuve ensuite automatiquement les certificats de cette liste.
- Mode d'approbation par autorité de certification (CA) / inscription : EcoStruxure Automation Device Maintenance approuve automatiquement les certificats inscrits avec les certificats d'autorité de certification qui sont disponibles dans le dossier **Autorités de certification racines de confiance** du **magasin de certificats** Windows.

Remarques à propos de l'utilisation de certificats

Tenez compte des remarques suivantes si vous utilisez des certificats pour des communications sécurisées :

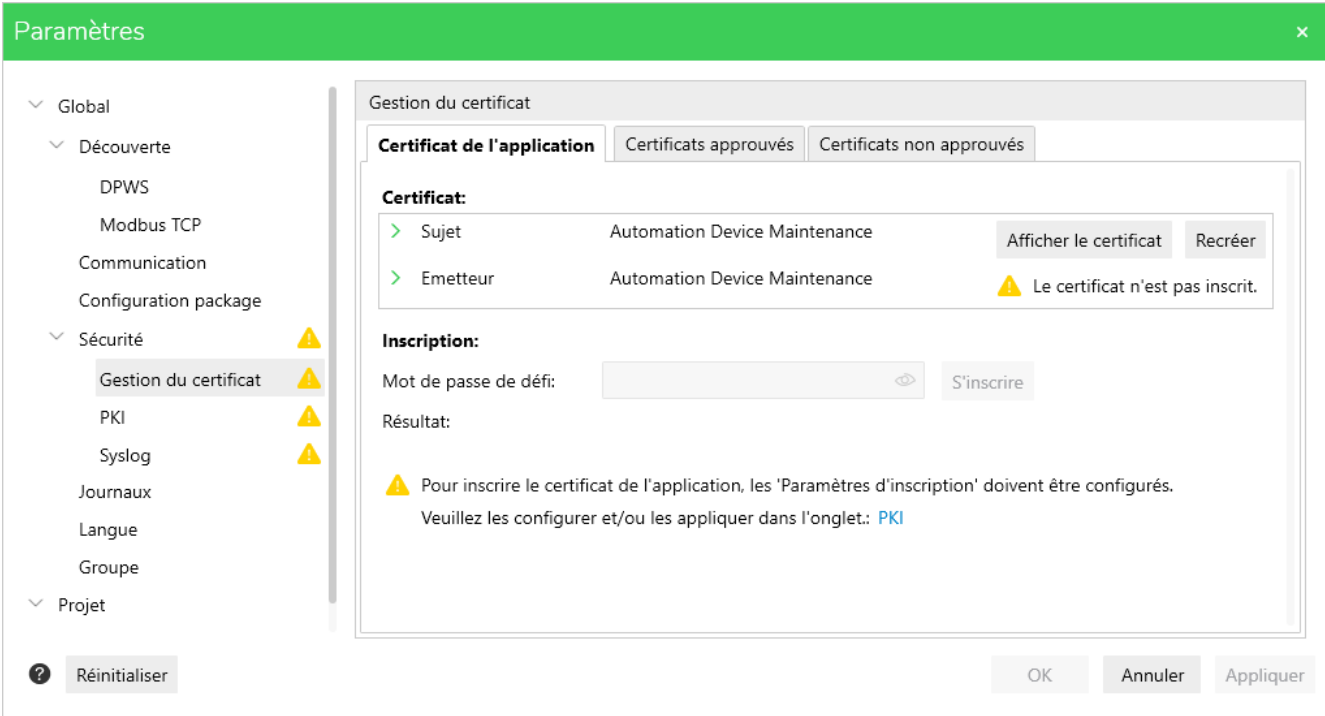
- Les certificats ayant une période de validité limitée, il convient de les gérer et de les mettre à jour régulièrement, et ce tout au long du cycle de vie de votre machine ou de votre système de contrôle.
- Les paramètres de date et d'heure de votre PC Windows sont utilisés pour vérifier si le certificat est toujours valide. Vérifiez à intervalles réguliers ces paramètres dans Windows **Démarrer > Paramètres > Heure et langue > Date et heure**.
- Si votre PC exécutant EcoStruxure Automation Device Maintenance est hors ligne en permanence, vous devez mettre à jour la **liste de révocation de certificats** (CRL) manuellement à intervalles réguliers. Pour cela, connectez-vous à votre point de distribution de CRL, téléchargez la dernière CRL et installez-la sur votre PC.
Pour connaître l'URL correcte du point de distribution de CRL, consultez votre administrateur de sécurité.
- Vous pouvez également déclarer des certificats comme non approuvés dans EcoStruxure Automation Device Maintenance, par exemple à l'aide de la boîte de dialogue **Gestion des certificats**, page 46.

Boîte de dialogue Gestion des certificats

Après l'installation initiale, un certificat d'application auto-signé par défaut est disponible pour EcoStruxure Automation Device Maintenance.

La boîte de dialogue **Gestion des certificats** propose les options suivantes pour le certificat d'application :

- Recréation du certificat d'application auto-signé et attribution de propriétés individuelles (voir [Recréation du certificat d'application auto-signé](#), page 44).
- Inscription du certificat d'application pour affecter une signature numérique d'une autorité de certification (CA) et créer une chaîne de confiance (voir [Inscription du certificat d'application](#), page 45).
- Gestion de l'état d'approbation des certificats numériques des partenaires de communication (voir [Gestion de l'état d'approbation des certificats](#), page 46).



Recréation du certificat d'application auto-signé

Pour recréer le certificat d'application par défaut et attribuer vos propriétés individuelles, procédez comme suit :

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Sélectionnez l'option Sécurité > Gestion des certificats .
3	Dans l'onglet Certificat de l'application , cliquez sur le bouton Recréer . Résultat : La boîte de dialogue Créer un certificat s'ouvre.
4	Entrez les propriétés à attribuer au certificat et cliquez sur le bouton OK . Résultat : Le certificat EcoStruxure Automation Device Maintenance auto-signé est présenté aux autres participants à la communication avec les propriétés que vous avez définies.

Inscription du certificat d'application

Pour créer une chaîne de confiance, le certificat d'application EcoStruxure Automation Device Maintenance doit être inscrit et signé numériquement par une autorité de certification.

Pour inscrire le certificat, commencez par configurer les **Paramètres d'inscription** comme indiqué dans l'option **Paramètres > Sécurité > PKI**, page 48.

Ensuite, inscrivez le certificat d'application pour EcoStruxure Automation Device Maintenance en procédant comme suit :

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Sélectionnez l'option Sécurité > Gestion des certificats .
3	Dans l'onglet Certificat d'application , vérifiez que le certificat d'application est toujours auto-signé et pas encore inscrit : <ul style="list-style-type: none"> Dans la section Certificat, les éléments Sujet et Emetteur présentent le même contenu : Automation Device Maintenance. La notification Le certificat n'est pas inscrit s'affiche sur la ligne Emetteur.
4	Entrez votre mot de passe pour l'autorité de certification dans la zone de texte Mot de passe de défi . Ce mot de passe permet d'autoriser la demande d'inscription. Pour plus d'informations, consultez l'administrateur de votre réseau industriel.
5	Cliquez sur Inscrire . Résultat : EcoStruxure Automation Device Maintenance envoie à l'autorité de certification une demande de signature de certificat à partir du certificat d'application, avec le mot de passe de défi. Si le mot de passe est incorrect, un message Échec de l'inscription est renvoyé. NOTE : Cette procédure remplace le certificat d'application auto-signé par défaut par un nouveau certificat signé. Le remplacement ne peut pas être annulé.
6	Vérifiez que le processus a abouti : <ul style="list-style-type: none"> Résultat : Inscription terminée s'affiche dans l'onglet Certificat d'application. Dans l'onglet Général de la boîte de dialogue Informations sur le certificat, l'entrée Emetteur contient désormais le nom de l'autorité de certification, par exemple <i>INT-DEV-SUB-CA</i>. L'onglet Chemin de certification de la boîte de dialogue Informations sur le certificat indique l'autorité de certification racine et les autorités de certification subordonnées dans une structure hiérarchique qui dépend de votre configuration PKI. Le certificat d'entité qui apparaît en bas de la structure hiérarchique est le certificat de EcoStruxure Automation Device Maintenance, avec les entrées suivantes : <ul style="list-style-type: none"> CN (Common Name) = Automation Device Maintenance O (Organization) = Schneider Electric

Gestion de l'état d'approbation des certificats

Les onglets **Certificats approuvés** et **Certificats non approuvés** de la boîte de dialogue **Gestion des certificats** permettent de gérer l'état d'approbation des certificats disponibles dans EcoStruxure Automation Device Maintenance.

Dans les deux onglets, chaque certificat est répertorié avec les informations suivantes :

Composant	Description
Sujet	Fournit des informations générales sur le certificat : <ul style="list-style-type: none"> • CN = Nom commun • OU = Unité d'organisation
Nom de l'équipement	Indique le nom de l'équipement tel qu'il est affiché dans la LISTE D'EQUIPEMENTS de l'onglet Equipement/Chargement . Si le certificat n'appartient à aucun équipement, la mention n/a est indiquée.
Point final de service	Les informations sur le point final de service sont fournies pour les équipements qui sont utilisés dans la présente session EcoStruxure Automation Device Maintenance. Si le certificat n'appartient à aucun équipement, la mention n/a est indiquée.
Action	Permet d'ouvrir la boîte de dialogue Informations sur le certificat via le lien Afficher le certificat .
État des certificats	Indique l'état du certificat : <ul style="list-style-type: none"> • Approuvé • Non approuvé

Vous pouvez effectuer les actions suivantes sur les certificats :

- Pour annuler l'approbation des certificats, sélectionnez un ou plusieurs certificats dans l'onglet **Certificats approuvés** et cliquez sur le bouton **Rejeter**.
- Pour approuver des certificats, sélectionnez un ou plusieurs certificats dans l'onglet **Certificats non approuvés** et cliquez sur le bouton **Approuver**. Pour approuver temporairement les certificats sélectionnés, choisissez l'option **Approuver cette session**.
- Pour supprimer des certificats, sélectionnez-les dans l'onglet **Certificats approuvés** ou **Certificats non approuvés** et cliquez sur le bouton **Supprimer**.


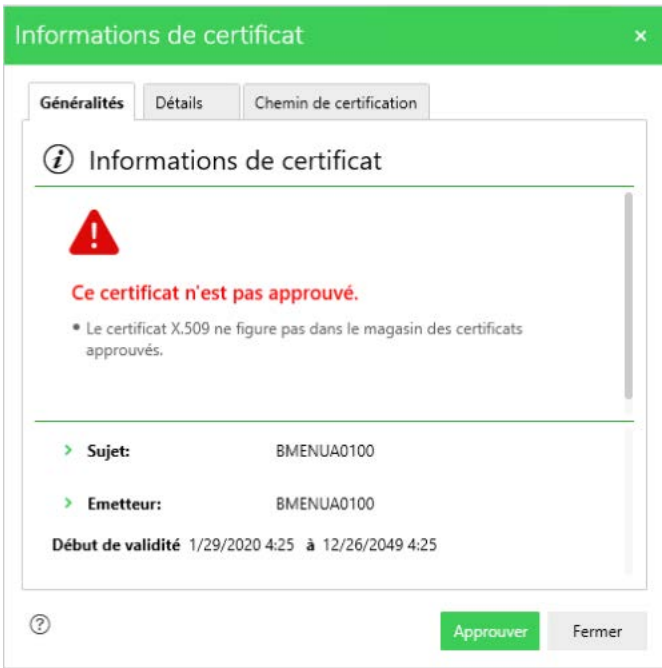
NOTE: Les certificats des équipements utilisés dans la présente session EcoStruxure Automation Device Maintenance ne peuvent pas être supprimés directement. Les certificats sont temporairement déplacés vers la liste **Certificats non approuvés** et seront supprimés lors de la fermeture de EcoStruxure Automation Device Maintenance.

NOTE: L'exécution de cette commande supprime les certificats sélectionnés sur le PC Windows. Ils seront également supprimés du **magasin de certificats** Windows.


Gestion de l'état d'approbation des certificats dans l'onglet Equipement/Chargement

Vous pouvez approuver et désapprouver les certificats des équipements dans l'onglet **Equipement/Chargement**.

Pour approuver un certificat d'équipement dans l'onglet **Equipement/Chargement**, procédez comme suit :

Étape	Action
1	<p>Cliquez sur l'icône Certificat d'équipement  correspondant à l'équipement.</p>  <p>NOTE: Vous pouvez approuver le certificat de serveur temporairement.</p>
2	Cochez l'option Approuver provisoirement le certificat de l'équipement pour la session en cours
3	Cliquez sur Certificat d'équipement approuvé .

Pour désapprouver un certificat d'équipement dans l'onglet **Equipement/Chargement**, procédez comme suit :

Étape	Action
1	Cliquez sur l'icône Certificat d'équipement  correspondant à l'équipement.
2	Cliquez sur Certificat d'équipement non approuvé .

Gestion de l'infrastructure à clé publique (PKI)

Paramètres d'inscription du certificat d'application

Si l'option **Sécurité** est activée dans la boîte de dialogue **Sécurité** de la page **Paramètres**, la boîte de dialogue **PKI** vous permet de configurer la connexion à l'autorité de certification (CA) pour inscrire le certificat de l'application .
EcoStruxure Automation Device Maintenance.

Paramètres

Global

Découverte

DPWS

Modbus TCP

Communication

Configuration package

Sécurité

Gestion du certificat

PKI

Syslog

Journaux

Langue

Groupe

Projet

PKI

Paramètres d'inscription:

URL d'inscription:

ID de l'émetteur:

Délai d'expiration:

Vérifier la signature uniquement:

Vérifier la connexion

Réinitialiser

OK

Annuler

Appliquer

Composant	Description
URL d'inscription	Entrez l'URL (Uniform Resource Locator) de l'autorité de certification (CA) qui émettra le certificat.
ID de l'émetteur	Entrez l'identifiant de l'émetteur de votre autorité de certification.
Timeout	Entrez une temporisation (en millisecondes) correspondant à vos débits de transfert Internet. Valeur par défaut : 10 000 ms
Vérifier la signature uniquement	Si cette option n'est pas sélectionnée, le certificat de l'autorité de certification doit être disponible en tant que certificat approuvé dans le magasin de certificats Windows. Pour vérifier uniquement les signatures numériques, sélectionnez cette option.
Bouton Vérifier la connexion	Cliquez sur le bouton Vérifier la connexion pour établir une connexion au site Web de l'autorité de certification.
Bouton Afficher le certificat	Une fois la connexion à l'autorité de certification établie, le bouton Afficher le certificat s'affiche. Cliquez sur ce bouton pour ouvrir la boîte de dialogue Informations sur le certificat et vérifier les attributs du certificat afin de vous assurer que vous êtes connecté à l'autorité de certification appropriée.

Si la connexion au site Web de l'autorité de certification a été établie, sélectionnez l'option **Sécurité > Gestion du certificat** et poursuivez l'inscription du certificat d'application.

Activation de la journalisation des messages Syslog


Présentation

La boîte de dialogue **Syslog** vous permet d'activer la fonction syslog et de configurer EcoStruxure Automation Device Maintenance en tant que client syslog. EcoStruxure Automation Device Maintenance fournit ensuite un sous-ensemble des messages de journal qu'il génère au serveur syslog correspondant en utilisant les paramètres syslog configurés dans cette boîte de dialogue.

The screenshot shows a software interface with a green header bar labeled "Paramètres". On the left is a sidebar menu with categories: "Global", "Découverte" (containing DPWS, Modbus TCP, Communication, Configuration package), "Sécurité" (containing Gestion du certificat, PKI, Syslog, Journaux, Langue, Groupe), and "Projet". The "Sécurité" category is expanded, and "Syslog" is selected, highlighted with a grey background and a yellow warning triangle. Below the menu is a "Réinitialiser" button with a question mark icon. The main area is titled "Syslog" and contains the following controls: a "Syslog:" label followed by radio buttons for "Activer" and "Désactiver" (which is selected and accompanied by a yellow warning triangle), a text field for "Adresse du serveur:" containing "127.0.0.1", a text field for "Port:" containing "6514", radio buttons for "Protocole réseau:" with "UDP", "TCP", and "TLS" (which is selected), and a "Vérifier la connexion" button. At the bottom right are "OK", "Annuler", and "Appliquer" buttons.

Activation de la journalisation des messages Syslog

Procédez comme suit pour activer la fonction syslog et pour configurer la connexion au serveur syslog :

Étape	Action
1	Cliquez sur le menu Paramètres au centre de la partie supérieure de la page d' accueil .
2	Sélectionnez l'option Sécurité > Syslog .
3	Sélectionnez l'option Activer pour activer la fonction syslog.
4	Dans la zone de texte Adresse du serveur , entrez l'adresse IP de votre serveur syslog.
5	Entrez le port sur lequel le serveur surveille les messages syslog en provenance des clients.
6	Sélectionnez l'option Protocole réseau : <ul style="list-style-type: none">• UDP (User Datagram Protocol)• TCP (Transmission Control Protocol)• TLS (Transport Layer Security)
7	<p>Pour les connexions TCP ou TLS, vous pouvez éventuellement cliquer sur le bouton Vérifier la connexion pour vérifier la connexion au serveur syslog.</p> <p>Résultats :</p> <p>Pour les connexions TCP : Un message s'affiche pour indiquer si une connexion au serveur a été établie.</p> <p>Pour les connexions TLS :</p> <ul style="list-style-type: none">• Un message s'affiche pour indiquer si une connexion au serveur a été établie.• Une icône indique si le certificat du serveur syslog est déjà déclaré comme approuvé. Si le certificat n'est pas approuvé, cliquez sur l'icône  pour ouvrir la boîte de dialogue Informations de certificat qui vous permet de vérifier le certificat et de le déclarer comme approuvé. <p>NOTE: Comme UDP est basé sur un modèle de communication sans connexion, EcoStruxure Automation Device Maintenance ne peut pas fournir de solution pour vérifier la connexion. Vous devez vérifier manuellement la réception des messages syslog sur le serveur que vous avez spécifié.</p>

Package de données

Onglet Package de données

Types de package de données pris en charge

Les types de fichiers suivants sont pris en charge :

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

Packages de données sécurisés

EcoStruxure Automation Device Maintenance prend en charge les packages de données *.sedps (Schneider Electric Data Package Secure) signés numériquement : Lorsque le mode de protection est activé, EcoStruxure Automation Device Maintenance vérifie que ce package provient d'une origine vérifiée et affiche des notifications de sécurité si la signature n'est pas correcte. Pour une description générale de la gestion des certificats, reportez-vous au chapitre [Gestion des certificats](#), page 43.

Si le mode de protection est activé, page 42, les règles suivantes s'appliquent :

- Les fichiers de package suivants sont signalés par l'icône de notification jaune dans la liste des packages de l'onglet **Package de données** et le message **Impossible de vérifier la chaîne de confiance du package** s'affiche à droite :
 - Fichiers de package non signés.
 - Fichiers de package auto-signés.
 - Fichiers de package utilisant un certificat racine qui n'est pas approuvé.
- Ces packages sont également signalés par l'icône de notification jaune dans l'onglet **Equipement/Chargement**.
- Si vous tentez une mise à jour de micrologiciel avec l'un de ces packages de données, le processus est suspendu et le message **La chaîne d'approbation du package sélectionné ne peut pas être vérifiée. Ce téléchargement peut endommager l'équipement. Voulez-vous continuer ?** s'affiche dans la zone de notification, page 67. Lisez attentivement le message et évaluez les risques. Une fois le message confirmé, le processus se poursuit.
- Si vous tentez de mettre à jour le micrologiciel avec l'un de ces packages de données, les erreurs détectées s'affichent dans la fenêtre **Journaux**, page 68.

AVIS

EQUIPEMENTS ENDOMMAGES

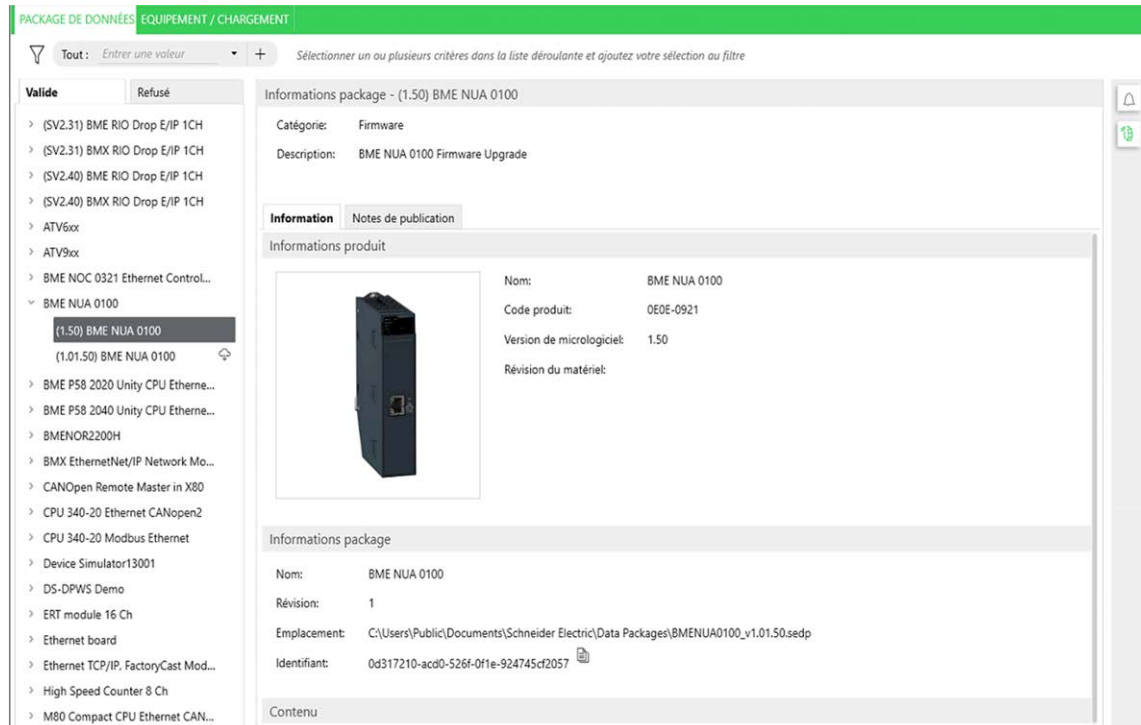
Vérifiez scrupuleusement que le package de données provient d'une source approuvée, car le téléchargement d'un package de données falsifié peut endommager votre équipement.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Présentation de l'onglet Package de données

Vous pouvez consulter le contenu de la bibliothèque de packages de données pour plus d'informations sur les différents packages.

La partie gauche de l'onglet affiche la liste des packages de données regroupés par famille d'équipement. La partie droite de l'onglet affiche les détails concernant le package sélectionné.



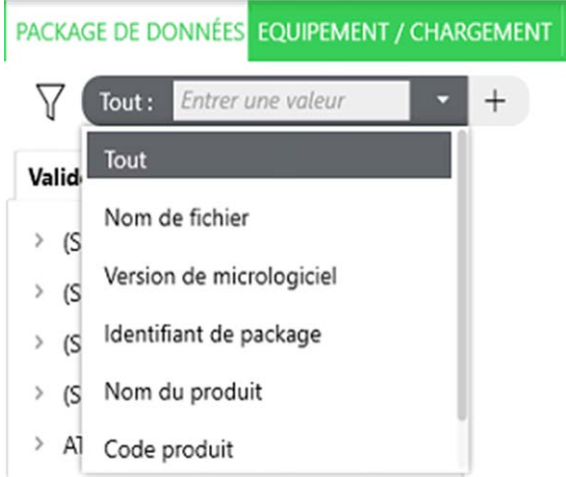
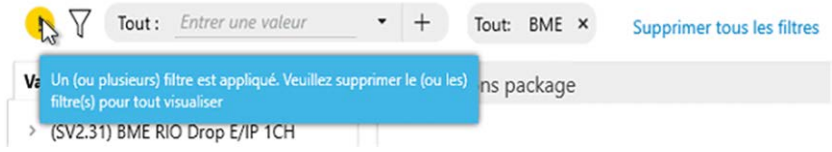
Liste des packages de données

La liste de packages de données affichée à gauche comprend deux onglets :

- L'onglet **Valide** répertorie les packages de données disponibles localement sur votre PC, regroupés par famille d'équipements.
- L'onglet **Refusé** répertorie les packages de données que vous avez téléchargés sur votre PC mais qui - pour une raison ou une autre - n'ont pas pu être traités. Il est possible que le fichier des packages de données ait été endommagé pendant le téléchargement. Il peut donc être utile de le télécharger une deuxième fois. Si cela ne résout pas le problème, demandez l'aide de votre service Schneider Electric.

Filtrage de la liste de packages de données

Pour réduire le nombre de packages de données affichés dans la liste, vous pouvez appliquer des critères de filtrage :

Étape	Action
1	<p>Entrez une chaîne dans le champ de texte Tout. Pour limiter la recherche à une propriété de package de données particulière, vous pouvez ouvrir la liste et sélectionner un critère de recherche.</p> 
2	<p>Cliquez sur le bouton "plus" à droite de la liste de recherche pour lancer l'opération.</p> <p>Résultat : La liste des packages de données affiche les entrées correspondant au critère de recherche que vous avez saisi. Une icône jaune s'affiche à gauche de la zone de recherche pour indiquer qu'un filtre est appliqué et que la liste est donc limitée aux packages de données répondant au critère de recherche.</p> 
3	<p>Répétez les étapes 1 et 2 pour définir un autre filtre. Les filtres fonctionnent par accumulation (opérateur booléen ET).</p> <p>Résultat : La liste des packages de données affiche les entrées qui répondent aux deux critères de recherche.</p>
4	<p>Pour supprimer un critère de filtrage, cliquez sur le bouton "croix" correspondant.</p> <p>Pour supprimer tous les filtres que vous avez définis, cliquez sur le lien Effacer tous les filtres. Vous revenez ainsi à la liste complète des packages de données.</p>

Informations package

Le volet **Informations package** qui s'affiche à droite fournit des informations sur le package de données que vous avez sélectionné dans la liste de gauche.

Dans la partie supérieure, vous trouvez les informations suivantes :

- **Catégorie**
- **Description**

L'onglet **Informations** affiche les détails suivants :

- Section **Informations produit** :
 - Image - Si le package de données en contient une.
 - **Nom**
 - **Code produit**
 - **Version de micrologiciel**
 - **Révision du matériel**
- Section **Informations package** :
 - **Nom**
 - **Révision**
 - **Emplacement**
 - **Identifiant** : Le bouton **Copier dans le Presse-papiers** vous permet de copier la chaîne d'identification dans le presse-papiers de votre PC.
- Section **Contenu** : Fournit le contenu du package de données sous forme de liste.

L'onglet **Notes de publication** n'a de contenu que si le package de données sélectionné contient un document marqué en tant que `ReleaseNotes`. En l'absence d'un tel document, l'onglet est vide pour le package considéré.


Equipement/Chargement

Onglet Equipement/Chargement

Présentation

EcoStruxure Automation Device Maintenance affiche un ensemble de propriétés d'équipement (nom d'appareil, point final de service, version de micrologiciel) dans l'onglet **Equipement/Chargement**.

NOTE: Les informations affichées dans cet onglet ne sont mises à jour automatiquement que si le mode de détection est défini sur **Automatique**.

Cliquez sur l'icône  dans la barre d'outils pour afficher les dernières valeurs.

PACKAGE DE DONNÉES

EQUIPEMENT / CHARGEMENT

LISTE D'EQUIPEMENTS

+

Ajouter

🔌

Connexion

🔌

Déconnexion

↻

Centre de mise à jour

🔍

Masquer

🗑


Supprimer

▼

<input type="checkbox"/>	Etat	Nom d'équipement Référence commerciale	Point final de service Numéro de série	Versio...	Version d...	Mode	Informations du centre de mise à jour	Extensions	Actions
<input type="checkbox"/>	Groupe par défaut de l'équipement (7)								
<input checked="" type="checkbox"/>	<div><div></div><div></div></div>	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-	-	-	<div><div>🔔</div><div>🔄</div><div>📄</div><div>▶</div><div>🔍</div><div>🔒</div><div>⋮</div></div>
<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>
<input type="checkbox"/>	<div><div></div><div></div></div>	ATV930U07M3_b3a CR: ATV930U07M3	mbap://fe80::280:f4ff:feb3:aa7d:502 SN: 4030000HL704004007	3.5IE94B04	-	-	-	-	<div><div>🔔</div><div>🔄</div><div>📄</div><div>▶</div><div>🔍</div><div>🔒</div><div>⋮</div></div>

Pour plus d'informations sur les détails affichés pour les équipements, reportez-vous au chapitre Equipement/Chargement, page 21.

Détails disponibles après connexion

Une fois que vous avez réussi à vous connecter à un équipement et que l'état de ce dernier est devenu vert, cliquez sur le bouton  pour accéder aux commandes suivantes :

Commande	Description
Optique	L'équipement émet un signal optique pour vous aider à l'identifier dans un rack de matériels parmi les équipements qui prennent en charge cette fonctionnalité.
Optique et acoustique	L'équipement émet un signal optique et acoustique pour vous aider à l'identifier dans un rack de matériels parmi les équipements qui prennent en charge cette fonctionnalité.
Propriétés	<p>Ouvre une nouvelle boîte de dialogue Propriétés qui fournit des informations complémentaires sur l'équipement dans différents onglets :</p> <ul style="list-style-type: none"> L'onglet Informations affiche des informations générales sur l'équipement : <ul style="list-style-type: none"> ID produit Nom du produit Version de micrologiciel Révision du matériel ID matériel Adresse MAC L'onglet Etat de l'équipement affiche des informations sur le statut actuel de l'équipement. L'onglet Configuration affiche des informations sur les paramètres de configuration de l'équipement. Si l'équipement le prend en charge, il est possible de modifier les paramètres de configuration dans cet onglet. <p>NOTE: Les modifications des paramètres de configuration peuvent nécessiter un redémarrage de l'équipement, ce qui risque de mettre le contrôleur à l'état STOP. Les effets sont indiqués par des messages affichés dans la zone de notification. Lisez attentivement chaque message et confirmez après avoir évalué les risques. Une fois que vous avez confirmé chaque message, le processus se poursuit.</p> <p>Les informations affichées dans la boîte de dialogue Propriétés dépendent de l'équipement concerné. Pour plus d'informations, consultez la documentation de l'équipement.</p>

Regroupement d'équipements dans la LISTE D'EQUIPEMENTS

Présentation

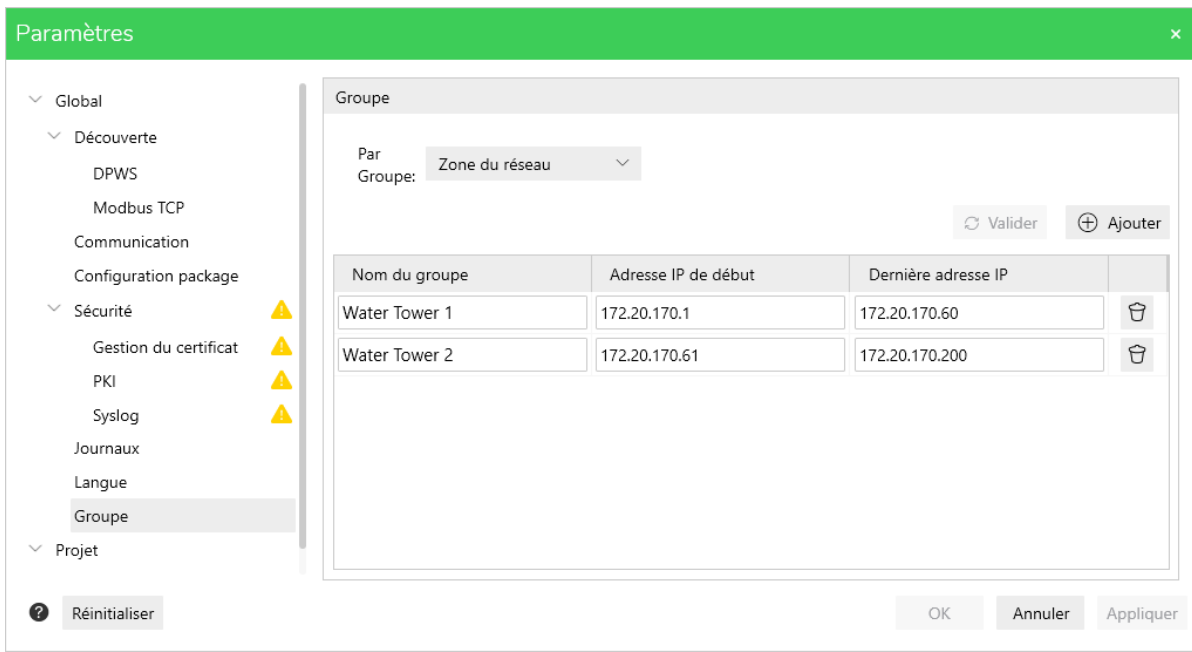
EcoStruxure Automation Device Maintenance permet de structurer les équipements affichés dans la **LISTE D'EQUIPEMENTS** en créant des groupes.

EcoStruxure Automation Device Maintenance V3.0 prend en charge le regroupement d'après les adresses IP des équipements en définissant des plages d'adresses IP. Des critères de regroupement supplémentaires pourront être ajoutés dans les versions ultérieures du logiciel EcoStruxure Automation Device Maintenance.

NOTE: Cette fonction de regroupement concerne exclusivement les adresses IPv4. La norme IPv6 n'est pas prise en charge par EcoStruxure Automation Device Maintenance V3.0.

Création de groupes

Procédez comme suit pour regrouper des équipements :

Étape	Action
1	Sélectionnez l'option Groupe dans la page Paramètres .
2	Développez la liste Grouper par et sélectionnez l'option Zone du réseau .
3	Cliquez sur le bouton + Ajouter pour créer une nouvelle plage d'adresses. Résultat : Un tableau contenant une ligne vide s'affiche.
4	Dans la cellule Nom de groupe , entrez un nom pour votre groupe d'équipements.
5	Dans la cellule Adresse IP de début , entrez la première adresse IP de la plage d'adresses définissant le groupe d'équipements.
6	Dans la cellule Dernière adresse IP , entrez la dernière adresse IP de la plage d'adresses définissant le groupe d'équipements. 
7	Cliquez sur le bouton + Ajouter pour créer un autre groupe. Ou Cliquez sur Appliquer pour appliquer les paramètres du groupe . Ou Cliquez sur OK pour appliquer toutes les modifications apportées aux paramètres de l'application et fermer la boîte de dialogue Paramètres .

Suppression d'équipement

Présentation








Vous pouvez supprimer des équipements en les masquant de façon temporaire ou permanente dans l'onglet **Liste d'équipements** du menu **Équipement/Chargement**.

Vous pouvez effectuer les actions suivantes :

- Masquer un équipement actif
- Supprimer un équipement actif
- Supprimer un équipement masqué




Masquer un équipement actif

Pour masquer un équipement actif, procédez comme suit :

Étape	Action
1	<p>Cliquez sur l'onglet Équipement/Chargement.</p> <p>Les équipements actifs détectés sont répertoriés dans l'onglet Liste d'équipements.</p>
2	<p>Dans Équipement/Chargement :</p> <ul style="list-style-type: none"> Sélectionnez un équipement en cliquant sur une cellule dans la ligne de l'équipement. OU Sélectionnez plusieurs équipements en cochant les cases situées à gauche de chaque ligne ou en sélectionnant l'ensemble du groupe.
3	<p>Les icônes suivantes sont activées pour les équipements sélectionnés :</p> <ul style="list-style-type: none">  Hide  Dispose
4	<p>Cliquez sur l'icône  Hide.</p> <p>Le message Masquer l'équipement s'affiche.</p> <div> <div>Masquer l'équipement</div> <div>×</div> </div> <p> Souhaitez-vous déplacer les équipements sélectionnés dans la LISTE DES ÉQUIPEMENTS MASQUÉS ?</p> <p><small>Vous pouvez réactiver le ou les équipements masqués dans la LISTE DES ÉQUIPEMENTS MASQUÉS.</small></p> <p>    </p>
5	<p>Cliquez sur Oui pour continuer.</p> <p>L'équipement sélectionné est déplacé dans l'onglet Liste des équipements masqués.</p> <p>NOTE: Vous pouvez réactiver les équipements masqués dans la liste Liste des équipements masqués.</p>





Afficher un équipement masqué

Pour afficher un équipement masqué, procédez comme suit :

Étape	Action
1	<p>Cliquez sur l'onglet Équipement/Chargement.</p> <p>Les équipements masqués sont répertoriés dans l'onglet Liste des équipements masqués.</p>
2	<ul style="list-style-type: none"> Sélectionnez un équipement en cliquant sur une cellule dans la ligne de l'équipement. OU Sélectionnez plusieurs équipements en cochant les cases situées à gauche de chaque ligne ou en sélectionnant l'ensemble du groupe.
3	<p>Les icônes suivantes sont activées pour les équipements sélectionnés :</p> <ul style="list-style-type: none">  Unhide  Dispose
4	<p>Cliquez sur l'icône  Unhide .</p> <p>L'équipement sélectionné est déplacé dans l'onglet Liste d'équipements.</p>






Supprimer un équipement actif

Pour supprimer un équipement actif, procédez comme suit :

Étape	Action
1	<p>Cliquez sur l'onglet Equipement/Chargement.</p> <p>Les équipements actifs détectés sont répertoriés dans l'onglet Liste d'équipements.</p>
2	<ul style="list-style-type: none">• Sélectionnez un équipement en cliquant sur une cellule dans la ligne de l'équipement.OU• Sélectionnez plusieurs équipements en cochant les cases situées à gauche de chaque ligne ou en sélectionnant l'ensemble du groupe.
3	<p>Les icônes suivantes sont activées pour les équipements sélectionnés :</p> <div><div> Hide</div><div>•</div><div> Dispose</div><div>•</div></div>
4	<div><div> Dispose</div><p>Cliquez sur l'icône  .</p><p>Le message Mettre l'équipement au rebut s'affiche.</p><div><div>Mettre l'équipement au rebut</div><div>×</div></div><div><div>!</div><div>Souhaitez-vous supprimer définitivement les équipements sélectionnés ?</div></div><div><div>La mise au rebut d'un équipement est irréversible. Il se peut qu'un équipement mis au rebut soit à nouveau détecté et reste accessible sur le réseau, si la découverte automatique est sélectionnée.</div></div><div><div>?</div><div>Oui</div><div>Non</div></div></div>
5	<p>Cliquez sur Oui pour continuer.</p> <p>NOTE: Si vous choisissez oui l'équipement est supprimé de façon permanente. Pour réintégrer l'équipement dans l'outil, il doit être ajouté manuellement ou détecté par la fonction de découverte.</p>

Supprimer un équipement masqué

Pour supprimer un équipement masqué, procédez comme suit :

Étape	Action
1	<p>Cliquez sur l'onglet Équipement/Chargement.</p> <p>Les équipements masqués sont répertoriés dans l'onglet Liste des équipements masqués.</p>
2	<ul style="list-style-type: none"> Sélectionnez un équipement en cliquant sur une cellule dans la ligne de l'équipement. OU Sélectionnez plusieurs équipements en cochant les cases situées à gauche de chaque ligne ou en sélectionnant l'ensemble du groupe.
3	<p>Les icônes suivantes sont activées pour les équipements sélectionnés :</p> <div>  Unhide </div> <p>.</p> <div>  Dispose </div> <p>.</p>
4	<div>  Unhide </div> <p>Cliquez sur l'icône .</p> <p>Le message Mettre l'équipement au rebut s'affiche.</p> <div> <div>Mettre l'équipement au rebut</div> <div>×</div> </div> <div>  <p>Souhaitez-vous supprimer définitivement les équipements sélectionnés ?</p> <p>La mise au rebut d'un équipement est irréversible. Il se peut qu'un équipement mis au rebut soit à nouveau détecté et reste accessible sur le réseau, si la découverte automatique est sélectionnée.</p> <div>  <div> <div>Oui</div> <div>Non</div> </div> </div> </div>
5	<p>Cliquez sur Oui pour continuer.</p> <p>NOTE: Si vous choisissez Oui, l'équipement est supprimé de façon permanente de l'outil, et il ne peut pas être récupéré.</p>

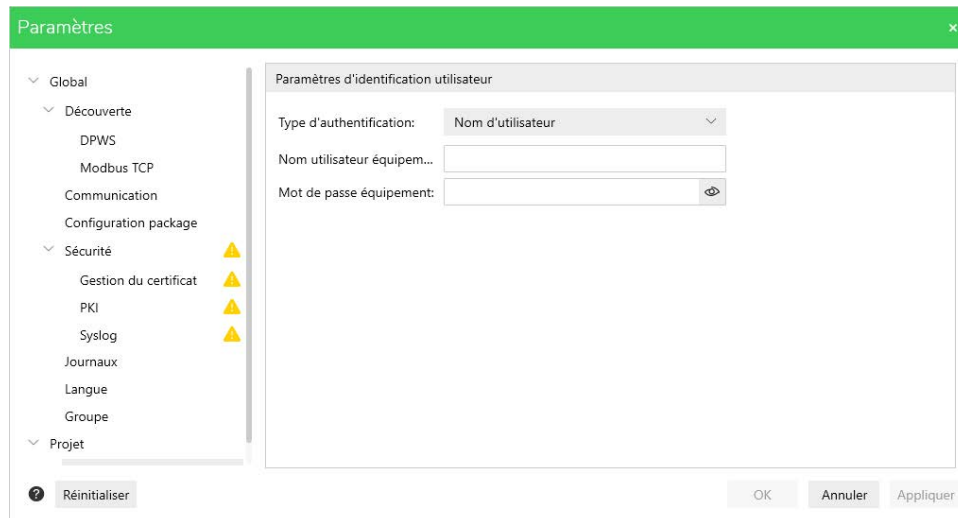
Gestion des identifiants d'utilisateur

Présentation

EcoStruxure Automation Device Maintenance permet d'entrer des informations d'identification pour l'accès autorisé aux équipements, au niveau global du projet et au niveau de chaque équipement.

Gestion globale des identifiants d'utilisateur


Pour gérer les identifiants d'utilisateur au niveau global du projet, accédez à la page **Paramètres** et sélectionnez l'option **Projet > Paramètres d'identification utilisateur**.



Sélectionnez **Type d'authentification > Nom d'utilisateur** ou **Type d'authentification > Personnalisé** et entrez les informations d'identification requises. Cliquez sur **Ok** pour enregistrer les informations d'identification. L'icône **Définir les identifiants de connexion** des équipements concernés dans la page **Équipement/Chargement** devient jaune et vous pouvez cliquer sur l'icône

Connecter  ou le bouton **Connexion**  pour vous connecter sans saisir à nouveau les identifiants.

Gestion des identifiants d'utilisateur par équipement

Pour gérer les identifiants d'utilisateur pour chaque équipement individuellement, ouvrez la page **Équipement/Chargement** et cliquez sur l'icône **Définir les identifiants de connexion**  dans la ligne du tableau correspondant à l'équipement :

Définir les identifiants de connexion

Nom d'équipement: ATV930U07M3_b3a

Type d'authentification:

Nom d'utilisateur

Nom utilisateur équipem...

MyDeviceUserName

Mot de passe équipement:

••••••••••

👁



?

Enregistrer et connecter

Enregistrer

Supprimer

Vous pouvez cliquer sur **Enregistrer et connecter** pour enregistrer les informations d'identification et établir une connexion à l'équipement. Une fois la connexion établie, l'icône **Définir les identifiants de connexion** devient verte. Sinon, vous pouvez cliquer sur **Enregistrer** pour enregistrer les informations d'identification de l'équipement en vue d'une connexion ultérieure. Dans ce cas, l'icône **Définir les identifiants de connexion** devient jaune et vous pouvez

cliquer sur l'icône **Connecter**  ou sur le bouton  **Connexion** pour vous connecter sans saisir à nouveau les identifiants.

Paramètres des identifiants d'utilisateur

Les paramètres affichés sont spécifiques à l'équipement et exigent les identifiants requis pour la connexion à cet équipement. Pour plus d'informations, consultez la documentation de l'équipement.













Trois mots de passe sont nécessaires pour se connecter aux contrôleurs Modicon M340, Modicon M580 ou Momentum. Pour plus d'informations sur le mot de passe de protection de l'application, le mot de passe du stockage des données et le mot de passe de protection du micrologiciel, reportez-vous aux chapitres appropriés du document *EcoStruxure Control Expert Operating Modes or the legacy Unity Pro Operating Modes* manual. Les liens permettant de télécharger les versions traduites de ce manuel sont fournis dans la liste de documents à consulter de la présente aide en ligne, page 10.

Accès aux extensions

Présentation

Un équipement modulaire figurant dans la **LISTE D'EQUIPEMENTS** de l'onglet **Equipement/Chargement** fournit un lien qui vous permet d'accéder aux différentes extensions de cet équipement.

Exemple d'équipement modulaire :

PACKAGE DE DONNÉES EQUIPEMENT / CHARGEMENT									
LISTE D'EQUIPEMENTS									
	Etat	Nom d'équipement Référence commerciale	Point final de service Numéro de série	Versio...	Version d...	Mode	Informations du centre de mise à jour	Extensions	Actions
Groupe par défaut de l'équipement (7)									
<input checked="" type="checkbox"/>	●	ATV630EIP CR: ATV630U07M3	mbapz/172.20.170.209-502 SN: 4004000HL44718401Y	2.6IE94B13	-	STOP		Extensions	     
<input type="checkbox"/>	●	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196-443 SN: 4002000HL64197000N	3.5IE94B04	-	-			     

Si l'équipement le prend en charge, le lien **Extensions** ([Extensions](#)) ouvre un nouvel onglet **Extensions** et présente les équipements modulaires regroupés par **Extension**.

PACKAGE DE DONNÉES

EQUIPEMENT / CHARGEMENT

EXTENSIONS

ATV630EIP

ATV630EIP

CR: ATV630U07M3

mbapz/172.20.170.209-502



SN: 4004000HL44718401Y

Version de micrologiciel: 2.6IE94B13

Centre de mise à jour

0

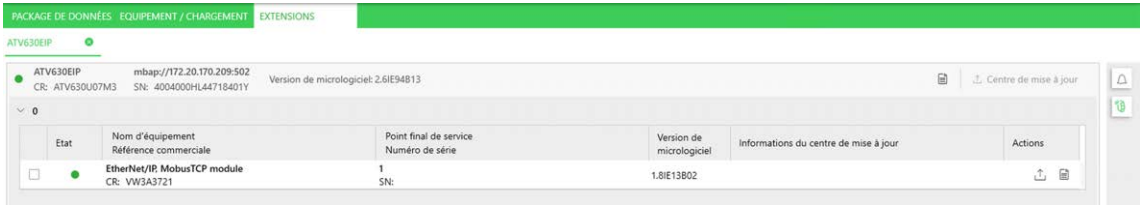
	Etat	Nom d'équipement Référence commerciale	Point final de service Numéro de série	Versio...	Version de micrologiciel	Informations du centre de mise à jour	Actions
<input type="checkbox"/>	<div></div>	EtherNet/IP, ModbusTCP module CR: VV3A3721	1 SN:		1.8IE13B02		<div></div> <div></div>

Les deux onglets permettent d'accéder à la boîte de dialogue **Centre de mise à jour** (via l'icône **Centre de mise à jour**  ou le bouton **Centre de mise à jour**  **Centre de mise à jour**) qui vous permet de sélectionner le package de données du micrologiciel via le bouton **Firmware**.

Pour les équipements qui ne peuvent pas charger les extensions à la demande via un clic sur le lien **Extensions**, exécutez la procédure décrite dans la section suivante pour accéder aux extensions individuelles.


Accès manuel aux extensions

Pour les équipements qui ne peuvent pas charger les extensions à la demande via un clic sur le lien **Extensions**, procédez comme suit :

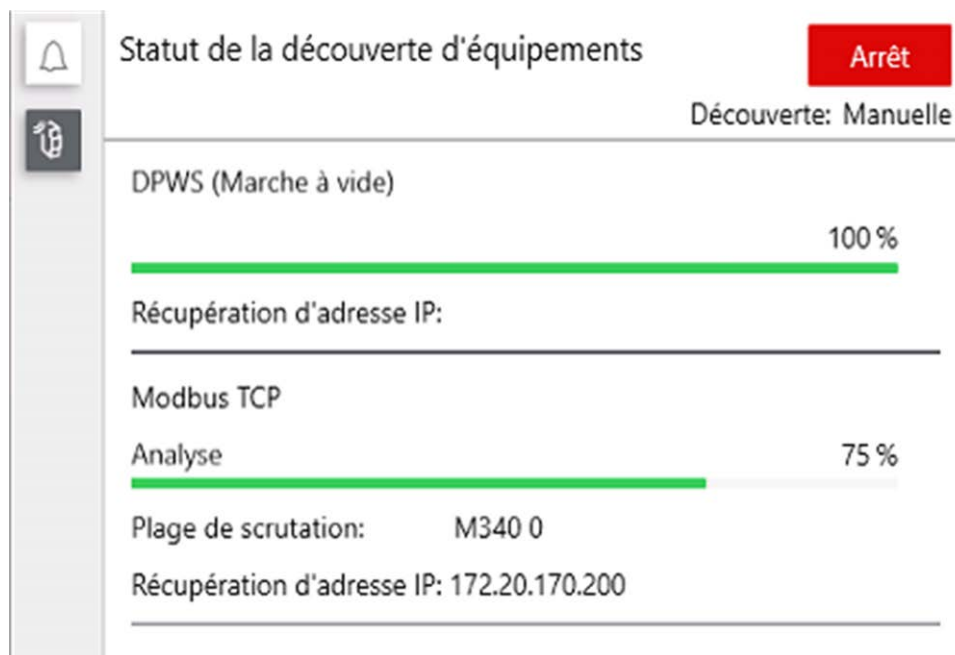
Étape	Action
1	<p>Cliquez sur le lien Extensions de l'équipement modulaire.</p> <p>Résultat : L'onglet Extensions s'ouvre. Si l'équipement ne peut pas charger les extensions à la demande suite à un clic sur le lien Extensions, un bouton Ajouter est disponible.</p>
2	<p>Cliquez sur le bouton Ajouter ou sur le lien Aucun module trouvé. Pour ajouter un module, cliquez ici.</p> <p>Résultat : La boîte de dialogue Ajouter un module s'ouvre.</p>
3	<p>Dans la boîte de dialogue Ajouter un module, configurez les paramètres d'accès aux extensions de l'équipement :</p> <ul style="list-style-type: none">• Numéro du Rack• Numéro du Logement
4	<p>Cliquez sur le bouton OK pour lancer la scrutation de découverte.</p> <p>Une fois les extensions détectées, l'onglet Extensions s'affiche.</p> 
5	<p>Fermez l'onglet Extensions.</p>

Surveillance du statut de la découverte d'équipements

Présentation

Lorsque le processus de découverte d'équipements s'exécute, vous pouvez en extraire le statut en cliquant sur le bouton  dans l'onglet **Équipement/Chargement**.

La vue **Statut de la découverte d'équipements** s'affiche sur le côté droit :



Elle fournit les informations suivantes :


- Informations d'avancement pour chaque scrutateur.
- Si des plages différentes sont configurées pour un scrutateur, les informations d'avancement sont fournies pour chaque plage individuellement (par exemple, pour le scrutateur Modbus TCP, page 34).

Le bouton **Démarrage/Arrêt** permet de lancer une découverte manuelle ou d'arrêter une découverte en cours directement depuis cette vue.

Affichage / confirmation des messages

Présentation

Certains processus exécutés par EcoStruxure Automation Device Maintenance nécessitent des interactions avec l'utilisateur. Chaque fois qu'une confirmation est requise, le processus (mise à jour de micrologiciel par exemple) s'arrête temporairement et un message s'affiche dans la zone de notification. Lisez attentivement chaque message et confirmez après avoir évalué les risques. Une fois que vous avez confirmé chaque message, le processus se poursuit.

Pour ouvrir la zone de notification, cliquez sur le bouton  dans l'onglet **Equipement/Chargement**.

PACKAGE DE DONNÉES

EQUIPEMENT / CHARGEMENT

LISTE D'EQUIPEMENTS

Ajouter

Connexion

Déconnexion

Centre de mise à jour

Masquer

Supprimer

<input type="checkbox"/>	Etat	Nom d'équipement Référence commerciale	Point final de service Numéro de série	Versio...	Version d...	Mode	Informations du centre de mise à jour
<input checked="" type="checkbox"/>	●	BME NOC0321 CR: BME NOC0321	ftp://172.20.170.62:21 SN:	01.06 IR 2	Confirmation requise	Micrologiciel sélectionné	
<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]:5... SN: 18c23639	3.5IE94802	-	-	
<input type="checkbox"/>	●	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94802	-	-	

Zone de notification

Astuce sur la sécurité

☒

BME NOC0321
ftp://172.20.170.62:21

Avant de transférer les données vers l'automate, vérifiez l'adresse de l'automate et l'adresse MAC affichées dans l'onglet Firmware afin de vous assurer que vous êtes connecté au bon équipement. Le transfert de données vers un équipement incorrect peut entraîner une situation dangereuse.

Souhaitez-vous poursuivre le transfert des données ?

Confirmer

Rejeter

Sommaire

Mise à jour

Annuler

Deux types de messages peuvent s'afficher dans la zone de notification :

- Messages de confirmation : Sélectionnez le message en activant la case à cocher, puis cliquez sur **Confirmer** pour confirmer le message et reprendre le processus en cours ou cliquez sur **Rejeter** pour arrêter le processus.
- Messages de notification : Sélectionnez le message en activant la case à cocher, puis cliquez sur **OK** pour confirmer et reprendre le processus en cours.

L'option **Ne pas afficher les notifications** permet de désactiver l'affichage des messages de notification. Si vous sélectionnez cette option, les processus seront exécutés automatiquement sans observer de pauses pour des interactions avec l'utilisateur, en partant de l'hypothèse que les messages sont confirmés.

NOTE: Activez cette option uniquement si vous travaillez en mode maintenance et si l'opérateur a vérifié l'état de sécurité de votre machine ou de votre environnement de processus.

Affichage des journaux


Vous pouvez afficher les journaux stockés et analyser les informations détaillées relatives à l'équipement sélectionné.


Les informations consignées dans le journal sont visibles dans les sections suivantes :

- Pour chaque équipement de la page **Équipement/Chargement**
- Pour l'ensemble du projet dans la fenêtre **Journaux**

NOTE: La fenêtre **Journaux** affiche les erreurs détectées, les avertissements détectés et les messages d'information.

Pour afficher les journaux propres à l'équipement sélectionné, procédez comme suit :

Éta-pe	Action
1	Accédez à la page Équipement/Chargement .
2	<p>Cliquez sur l'icône Journal d'équipement  correspondant à un équipement.</p> <p>Résultat : Une petite vue Infos journaux s'ouvre directement dans le tableau situé sous la ligne de l'équipement. Si nécessaire, utilisez la barre de défilement à droite pour voir toutes les entrées du journal.</p>

Pour masquer la vue **Infos journaux** d'un équipement, cliquez à nouveau sur l'icône **Journal d'équipement** .

Recommandation pour améliorer la cybersécurité

Le fichier journal contient des données généralement sensibles, du type :


- Adresses d'équipement
- Noms d'équipement
- Détails sur la topologie du réseau
- Détails sur la configuration du réseau

Il est stocké sur le disque dur de votre PC. Supprimez-le dès que vous n'en avez plus besoin ou stockez-le dans un emplacement protégé contre tout accès non autorisé.

Centre de mise à jour

Présentation

La boîte de dialogue **Centre de mise à jour** vous permet de configurer les paramètres à utiliser pour une mise à jour de micrologiciel ou du fichier de configuration de la sécurité. Ces paramètres de configuration peuvent être appliqués à un équipement particulier ou à plusieurs équipements à la fois.

- Pour effectuer des mises à jour sur un équipement particulier, cliquez sur l'icône **Centre de mise à jour**  sur la ligne de tableau correspondant à cet équipement dans l'onglet **Équipement/Chargement**.
- Pour effectuer des mises à jour simultanément sur différents équipements du projet, sélectionnez les équipements dans l'onglet **Équipement/Chargement**

et cliquez sur le bouton **Centre de mise à jour**  **Centre de mise à jour** dans la barre de boutons.

Boîte de dialogue Centre de mise à jour

Les deux actions ouvrent la boîte de dialogue **Centre de mise à jour** qui propose les options suivantes :

- **Firmware** : Permet de configurer les paramètres de mise à jour de micrologiciel pour les équipements sélectionnés. Pour plus d'informations, reportez-vous à la section *Mise à jour du micrologiciel*, page 69.
- **Sécurité** : Permet de configurer les paramètres de mise à jour du fichier de configuration de la sécurité pour les équipements sélectionnés. Pour plus d'informations, reportez-vous à la section *Mise à jour du fichier de configuration de la sécurité*, page 71.
- **Réinitialiser** : Permet de réinitialiser les paramètres de mise à jour pour les équipements sélectionnés.

Pour confirmer les paramètres et fermer la boîte de dialogue **Centre de mise à jour**, cliquez sur le bouton **Enregistrer**. La configuration que vous avez effectuée est indiquée dans les cellules **Informations du centre de mise à jour** des équipements dans l'onglet **Équipement/Chargement**, page 21.

Pour exécuter le processus de mise à jour tel que configuré, cliquez sur le bouton **Mise à jour**.

Mise à jour du micrologiciel

Présentation

EcoStruxure Automation Device Maintenance permet de mettre à jour le micrologiciel des équipements affichés dans l'onglet **Équipement/Chargement**.



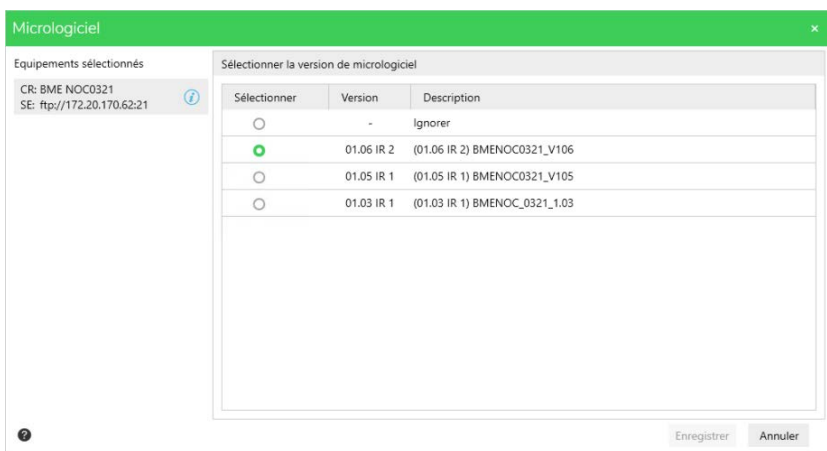
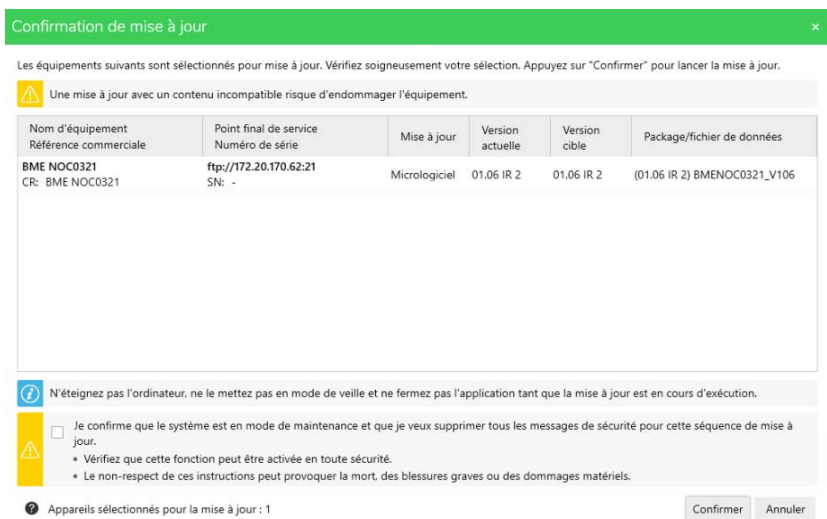
Pour mettre à jour le micrologiciel des équipements modulaires, vous pouvez accéder aux différentes extensions décrites dans le chapitre *Accès aux extensions*, page 64.

Vous pouvez sélectionner des packages de données pour plusieurs extensions et/ou modules de rack. EcoStruxure Automation Device Maintenance mettra à jour le micrologiciel de tous ces équipements simultanément.

NOTE: Si vous effectuez une mise à jour simultanée pour le contrôleur et les modules, veillez à ne pas redémarrer le contrôleur tant que la mise à jour des modules est en cours d'exécution. Voir le message *Danger* ci-dessous.

Mise à jour du micrologiciel

Procédez comme suit pour mettre à jour le micrologiciel :

Étape	Action
1	Accédez à la page Equipement/Chargement .
2a	Pour effectuer des mises à jour sur un équipement particulier, cliquez sur l'icône Centre de mise à jour  sur la ligne correspondant à cet équipement.
2b	Pour mettre à jour simultanément plusieurs équipements du projet, cochez les cases appropriées ou cochez la case correspondant à l'ensemble du groupe et cliquez sur le bouton Centre de mise à jour  Centre de mise à jour dans la barre de boutons.
3	Dans la boîte de dialogue Centre de mise à jour , cliquez sur le bouton Firmware .
4	Dans la boîte de dialogue Firmware , sélectionnez le package de données de micrologiciel pour chaque équipement. 
5	Cliquez sur Enregistrer pour enregistrer la configuration de mise à jour du micrologiciel et fermer la boîte de dialogue Firmware . Résultat : Les cellules Informations du centre de mise à jour des équipements dans l'onglet Equipement/Chargement , page 21 affichent le texte Micrologiciel sélectionné .
6	Cliquez sur le bouton Mise à jour dans l'onglet Equipement/Chargement pour lancer la mise à jour. Résultat : La boîte de dialogue Confirmation de mise à jour s'affiche. 
7	Dans la boîte de dialogue Confirmation de mise à jour , examinez attentivement la liste des équipements sélectionnés pour la mise à jour et vérifiez les paramètres que vous avez définis.

Étape	Action
8	<p>Cliquez sur le bouton Confirmer pour lancer la mise à jour.</p> <p>Résultat : La mise à jour du micrologiciel démarre. Chaque fois qu'une interaction utilisateur est nécessaire, le processus s'arrête temporairement et un message s'affiche dans la zone de notification, page 67. Lisez attentivement chaque message et confirmez après avoir évalué les risques. Une fois que vous avez confirmé chaque message, le processus se poursuit.</p>
9	<p>Une fois le processus terminé, cliquez sur le bouton Résumé, page 19 en bas de la fenêtre EcoStruxure Automation Device Maintenance pour afficher la boîte de dialogue Résumé de la mise à jour. Elle fournit des informations sur l'état de la mise à jour pour chaque équipement, indiquant notamment la version précédente et la version cible, ainsi que le package/fichier de données.</p>

AVIS

EQUIPEMENTS ENDOMMAGÉS

N'éteignez pas le PC, ne fermez pas l'application et assurez-vous que le PC ne passe pas en mode de veille pendant l'exécution de la mise à jour de micrologiciel car l'interruption du processus peut endommager l'appareil.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Vous pouvez éventuellement cocher la case **Je confirme que le système est en mode de maintenance et que je veux supprimer tous les messages de sécurité pour cette séquence de mise à jour**. Cela permettra d'éviter la mise en pause du processus.

NOTE: Activez cette option uniquement si vous travaillez en mode maintenance et si l'opérateur a vérifié l'état de sécurité de votre machine ou de votre environnement de processus.

Une fois le processus terminé, vous pouvez éventuellement (pour les contrôleurs) cliquer sur l'icône **Démarrer l'équipement** dans l'onglet **Équipement/Chargement**, page 21 pour démarrer l'équipement.

NOTE: Effectuez un test de démarrage avant d'utiliser un équipement de commande électrique et d'automatisation en mode d'exploitation normale après une installation ou une mise à jour. Pour plus d'informations, reportez-vous à la section **Démarrage et test**, page 7.

Mise à jour du fichier de configuration de la sécurité



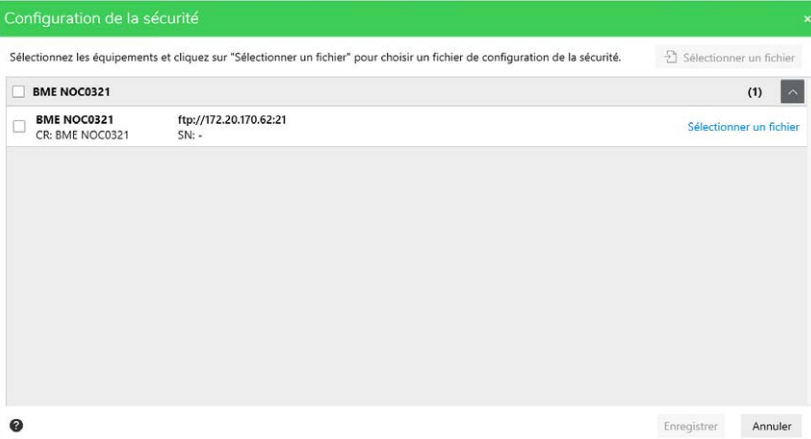
Présentation

EcoStruxure Automation Device Maintenance permet de mettre à jour le fichier de configuration de la sécurité qui contient les paramètres de configuration de la sécurité que vous avez configurés globalement pour votre réseau dans l'application EcoStruxure Cybersecurity Admin Expert.

NOTE: Le nouveau fichier de configuration de la sécurité peut attribuer de nouvelles informations d'identification aux équipements. Ces nouveaux identifiants seront indispensables pour toute connexion ultérieure.

Mise à jour du fichier de configuration de la sécurité

Procédez comme suit pour mettre à jour le fichier de configuration de la sécurité :

Étape	Action
1	Accédez à la page Equipement/Chargement .
2a	Pour effectuer des mises à jour sur un équipement particulier, cliquez sur l'icône Centre de mise à jour  sur la ligne correspondant à cet équipement.
2b	Pour mettre à jour simultanément plusieurs équipements du projet, cochez les cases appropriées ou cochez la case correspondant à l'ensemble du groupe et cliquez sur le bouton Centre de mise à jour  Centre de mise à jour dans la barre de boutons.
3	Dans la boîte de dialogue Centre de mise à jour , cliquez sur le bouton Sécurité .
4	<p>Dans la boîte de dialogue Configuration de la sécurité, sélectionnez un équipement et cliquez sur le lien Sélectionner un fichier correspondant ou sélectionnez plusieurs équipements et cliquez sur le bouton Sélectionner un fichier dans la partie supérieure de la boîte de dialogue.</p>  <p>Résultat : Une boîte de dialogue d'ouverture de fichier Windows s'affiche et vous permet de rechercher sur votre réseau le fichier de configuration de la sécurité.</p>
5	<p>Sélectionnez le fichier de configuration de la sécurité et cliquez sur le bouton Ouvrir.</p> <p>Résultat : La boîte de dialogue Configuration de la sécurité affiche les équipements contenant les fichiers sélectionnés.</p>
6	<p>Cliquez sur le bouton Enregistrer pour enregistrer la configuration et fermer la boîte de dialogue Configuration de la sécurité.</p> <p>Résultat : Les cellules Informations du centre de mise à jour des équipements dans l'onglet Equipement/Chargement, page 21 affichent le texte Configuration de sécurité sélectionnée.</p>
7	<p>Cliquez sur le bouton Mise à jour dans l'onglet Equipement/Chargement pour lancer la mise à jour.</p> <p>Résultat : La boîte de dialogue Confirmation de mise à jour s'affiche.</p>
8	Dans la boîte de dialogue Confirmation de mise à jour , examinez attentivement la liste des équipements sélectionnés pour la mise à jour et vérifiez les paramètres que vous avez définis.
9	<p>Cliquez sur le bouton Confirmer pour lancer la mise à jour.</p> <p>Résultat : Le processus de mise à jour démarre. Chaque fois qu'une action de l'utilisateur est nécessaire, le processus s'arrête temporairement et un message s'affiche dans la zone de notification, page 67. Lisez attentivement chaque message et confirmez après avoir évalué les risques. Une fois que vous avez confirmé chaque message, le processus se poursuit.</p>

AVIS

EQUIPEMENTS ENDOMMAGÉS

N'éteignez pas le PC, ne fermez pas l'application et assurez-vous que le PC ne passe pas en mode de veille pendant l'exécution de la mise à jour de micrologiciel car l'interruption du processus peut endommager l'appareil.

Le non-respect de ces instructions peut provoquer des dommages matériels.

Vous pouvez éventuellement cocher la case **Je confirme que le système est en mode de maintenance et que je veux supprimer tous les messages de sécurité pour cette séquence de mise à jour**. Cela permettra d'éviter la mise en pause du processus.

NOTE: Activez cette option uniquement si vous travaillez en mode maintenance et si l'opérateur a vérifié l'état de sécurité de votre machine ou de votre environnement de processus.

Cybersécurité

Introduction

La cybersécurité est une branche de l'administration de réseau qui s'occupe des attaques ciblant les systèmes informatiques ou émanant d'ordinateurs via des réseaux informatiques, qui peuvent entraîner des perturbations accidentelles ou intentionnelles. Son objectif est de mieux protéger les informations et les actifs physiques contre le vol, les dommages, une utilisation abusive ou des accidents, tout en les maintenant accessibles à leurs utilisateurs.

Aucune approche, à elle seule, ne peut garantir la cybersécurité. Schneider Electric recommande une approche de défense en profondeur. Conçu par National Security Agency (NSA), cette approche définit des couches sur le réseau avec des fonctions de sécurité, des équipements et des processus. Ses composants de base sont les suivants :

- Evaluation des risques
- Plan de sécurité élaboré en fonction des résultats de l'évaluation des risques
- Campagne de formation en plusieurs phases
- Séparation physique des réseaux industriels des réseaux d'entreprise avec une zone dite démilitarisée (DMZ) et utilisation de parefeu et du routage pour créer d'autres zones de sécurité
- Contrôle des accès au système
- Renforcement des équipements
- Surveillance et maintenance du réseau

Ce chapitre définit les éléments qui vous aident à configurer un système moins vulnérable aux cyber-attaques. Pour plus d'informations sur l'approche de défense en profondeur, reportez-vous à la note technique *système Comment... Réduire la vulnérabilité aux cyber-attaques* sur [Schneider Electric website](#).

Qu'est-ce que la cybersécurité ?

Présentation

Les cyber-menaces désignent des actions volontaires ou non, susceptibles de perturber le fonctionnement normal des systèmes et réseaux informatiques. Ces actions peuvent être déclenchées dans les locaux ou à l'extérieur de l'entreprise. Les défis de l'environnement de contrôle en matière de sécurité sont les suivants :

- Diversité des limites physiques et logiques.
- Multiplicité des sites et ampleur des zones géographiques.
- Effets négatifs de la sécurité sur la disponibilité des processus.
- Vulnérabilité accrue aux vers et virus qui contaminent les systèmes de contrôle à partir des systèmes commerciaux, à mesure que les communications entre ces systèmes s'ouvrent.
- Vulnérabilité accrue aux logiciels malveillants provenant de périphériques USB, des ordinateurs portables de fournisseurs et de techniciens de maintenance, et du réseau de l'entreprise.
- Impact direct des systèmes de contrôle sur les systèmes physiques et mécaniques.

Sources des cyberattaques

Mettez en œuvre un plan de cybersécurité qui tient compte des multiples sources potentielles de cyberattaques et d'accidents :

Source	Description
Interne	<ul style="list-style-type: none">• Comportement inapproprié d'un employé ou d'un sous-traitant• Employé ou sous-traitant mécontent
Opportuniste externe (attaque non ciblée)	<ul style="list-style-type: none">• Script kiddies*• Pirates occasionnels• Créateurs de virus
Volontaires externes (attaque ciblée)	<ul style="list-style-type: none">• Groupes criminels• Activistes• Terroristes• Services d'états étrangers
Accidentelles	
* Terme désignant les pirates qui utilisent des scripts malveillants créés par des tiers, sans connaître nécessairement le fonctionnement de ces scripts ou leur impact potentiel sur un système.	

Une cyberattaque peut cibler délibérément un système de contrôle pour atteindre plusieurs objectifs, notamment :

- Perturber le processus de production en bloquant ou en retardant le flux d'informations.
- Endommager, désactiver ou arrêter des équipements pour perturber la production ou l'environnement.
- Modifier ou désactiver les systèmes de sécurité pour causer des dommages volontairement.

Techniques utilisées par les pirates pour accéder aux systèmes

Un pirate contourne les défenses périmétriques pour accéder au réseau du système de contrôle. Les points d'accès courants sont les suivants :

- Accès commuté à des équipements terminaux distants (RTU).
- Points d'accès des fournisseurs (comme les points d'accès du support technique).
- Solutions réseau contrôlées par informatique.
- Réseau privé virtuel d'entreprise (VPN).
- Liens à des bases de données.
- Parefeu mal configurés.
- Services homologues.

Certifications liées à la cybersécurité

Les consignes de cybersécurité développées par Schneider Electric s'appuient sur les recommandations suivantes :

- Achilles
- ISA Secure

Pour poser des questions, consulter les actualités ou signaler des problèmes de vulnérabilité

Pour poser une question sur la cybersécurité, obtenir les dernières actualités de Schneider Electric ou signaler des problèmes de vulnérabilité, visitez notre [website](#).

Consignes Schneider Electric

Introduction

Votre système PC peut exécuter une grande variété d'applications destinées à améliorer la sécurité dans votre environnement de contrôle. Les paramètres par défaut du système doivent être reconfigurés en fonction des recommandations de Schneider Electric concernant le renforcement de la protection des équipements.

Les consignes suivantes décrivent les procédures relatives à Windows. Elles sont fournies à titre d'exemple. Les exigences ou procédures de votre système d'exploitation et de votre application peuvent être différentes.

Sécurisation renforcée des postes de travail d'ingénierie

Les clients ont le choix entre différents PC commerciaux pour leurs postes de travail d'ingénierie. Les principales techniques de sécurisation renforcée sont les suivantes :

- Gestion des mots de passe forts
- Gestion des comptes utilisateur
- Méthodes du droit minimum appliqué aux applications et comptes utilisateur
- Suppression ou désactivation des services superflus
- Suppression des droits de gestion à distance
- Gestion systématique des correctifs

Désactiver les cartes d'interface réseau inutilisées

Vérifiez que les cartes d'interface réseau non requises par l'application sont désactivées. Par exemple, si votre système compte deux cartes et que l'application n'en utilise qu'une, vérifiez que l'autre (Connexion au réseau local 2) est désactivée.

Pour désactiver une carte réseau dans Windows :

Étape	Action
1	Ouvrez Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte .
2	Cliquez avec le bouton droit de la souris sur la connexion non utilisée. Sélectionnez Désactiver .

Configurer la connexion au réseau local

Différents paramètres réseau de Windows permettent de renforcer la sécurité pour la mettre au niveau de la protection renforcée recommandée par Schneider Electric.

Sur un système Windows, vous pouvez accéder à ces paramètres en ouvrant **Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte > Connexion au réseau local (x)**.

Cette liste montre des exemples de modification de la configuration que vous pouvez effectuer sur votre système via l'écran **Propriétés de la connexion au réseau local** :

- Désactivez toutes les piles IPv6 sur leurs cartes réseau respectives. (Cet exemple de système ne requiert pas la plage d'adresses IPv6, et la désactivation des piles IPv6 limite la vulnérabilité aux risques potentiels liés à la sécurité IPv6.
- Désactivez **Partage de fichiers et d'imprimantes Réseaux Microsoft**.

L'approche de protection renforcée de Schneider Electric inclut également les recommandations suivantes :

- Ne définissez que des adresses, masques de sous-réseau et passerelles IPv4 statiques.
- N'utilisez pas DHCP ou DNS dans la salle de contrôle.

Gérer le pare-feu Windows

Les recommandations de Schneider Electric pour le renforcement de la protection comprennent l'activation du pare-feu hôte Windows sur tous les PC du système. Activez les pare-feux pour tous les profils publics et privés définis.

Il est recommandé aux utilisateurs de définir des règles de pare-feu qui refusent les connexions provenant ou à destination d'hôtes externes inconnus ou non approuvés.

Désactiver Remote Desktop Protocol

Les recommandations de l'approche de défense en profondeur de Schneider Electric incluent la désactivation du protocole RDP (Remote Desktop Protocol), sauf si votre application requiert le protocole RDP.

Exécutez les étapes suivantes pour désactiver le protocole sur les systèmes Windows 10 :

Étape	Action
1	Cliquez avec le bouton droit de la souris sur le bouton Windows Démarrer et exécutez la commande Système .
2	Dans le menu Paramètres , exécutez la commande Bureau à distance .
3	Dans la vue Bureau à distance , désactivez l'option Activer le Bureau à distance (basculez sur la valeur Désactivé).

Pour les autres systèmes d'exploitation Windows, exécutez des procédures équivalentes.

Mise à jour des stratégies de sécurité

Mettez à jour les stratégies de sécurité sur les ordinateurs de votre système en utilisant `gpupdate` dans une fenêtre de commande. Pour plus d'informations, consultez la documentation Microsoft relative à `gpupdate`.

Désactiver LANMAN et NTLM

Le protocole Microsoft LAN Manager (LANMAN ou LM) et son successeur NT LAN Manager (NTLM) présentent des vulnérabilités. Leur utilisation est donc déconseillée dans les applications de contrôle.

Pour désactiver LM et NTLM sur un système Windows, procédez comme suit :

Étape	Action
1	Dans une fenêtre de commande, exécutez <code>secpol.msc</code> pour ouvrir la fenêtre Stratégie de sécurité locale .
2	Ouvrez Paramètres de sécurité > Stratégies locales > Options de sécurité .
3	Sélectionnez Envoyer réponse NTLMv2 uniquement. Refuser LM et NTLM dans le champ Sécurité réseau : Niveau d'authentification du gestionnaire de réseau local .
4	Cochez l'option Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe .
5	Dans une fenêtre de commande, entrez <code>gpupdate</code> pour valider la stratégie de sécurité modifiée.

Gestion des mises à jour

Avant le déploiement, mettez à jour les systèmes d'exploitation de tous les ordinateurs à l'aide des utilitaires disponibles dans la page **Windows Update** de Microsoft. Pour accéder à cet outil dans Windows, sélectionnez **Démarrer > Tous les programmes > Windows Update**.

Vérification de la signature numérique

Vérification de l'intégrité de EcoStruxure Automation Device Maintenance après téléchargement

Après avoir téléchargé le fichier exécutable de EcoStruxure Automation Device Maintenance à partir du site Web Schneider Electric, vérifiez son intégrité en exécutant les étapes suivantes :

Étape	Action
1	Cliquez avec le bouton droit sur le fichier <code>AutomationDeviceMaintenance.exe</code> et sélectionnez la commande Propriétés dans le menu contextuel.
2	Dans la boîte de dialogue AutomationDeviceMaintenance.exe Propriétés , sélectionnez l'onglet Signatures numériques .
3	Dans la liste de signatures , sélectionnez l'entrée Schneider Electric USA, INC. et cliquez sur le bouton Détails pour afficher les détails de la signature numérique .
4	Assurez-vous que la boîte de dialogue Détails de la signature numérique indique que cette signature numérique est correcte .

Vous pouvez alors double-cliquer sur le fichier `.exe` pour démarrer EcoStruxure Automation Device Maintenance.

Vérification des composants lors du démarrage

Au démarrage de EcoStruxure Automation Device Maintenance, chaque bibliothèque de liens dynamiques (DLL) chargée est analysée pour vérifier si elle

sûre ou non. Il s'agit d'une fonctionnalité de sécurité intégrée contre les cyberattaques et pour la consolidation du niveau de confiance.

Que faire si des composants non approuvés sont détectés

Si des composants non approuvés sont détectés, le lancement de EcoStruxure Automation Device Maintenance est abandonné et un message s'affiche pour indiquer qu'une exception a été détectée.

Dans ce cas, vous disposez des options suivantes :

- Réinstallez EcoStruxure Automation Device Maintenance.
- Si vous avez le moindre soupçon de cyber-attaque à l'origine du problème, consultez la page [Schneider Electric Cybersecurity services portal](#) pour obtenir des conseils ou une assistance supplémentaires.

Pour identifier le composant à l'origine du problème, vous pouvez utiliser un outil de débogage tel que WinDbg : Démarrez l'outil de débogage, lancez EcoStruxure Automation Device Maintenance et recherchez dans le fichier journal les entrées indiquant qu'il est impossible de déterminer la validité de la signature de code d'une DLL.

Fichiers nécessitant une désinstallation manuelle

Présentation

Lorsque vous désinstallez EcoStruxure Automation Device Maintenance de votre PC, les fichiers de programme sont automatiquement supprimés, mais certains fichiers propres à l'utilisateur doivent être gérés individuellement afin d'éviter les problèmes de cybersécurité.

Fichier de paramètres EcoStruxure Automation Device Maintenance

Le fichier de paramètres EcoStruxure Automation Device Maintenance *AutomationDeviceMaintenanceSettings.emes* est créé par EcoStruxure Automation Device Maintenance pour stocker la configuration que vous avez effectuée dans la boîte de dialogue **Paramètres** (par exemple, plages de scrutation ou paramètres de détection Modbus TCP). Il n'est pas supprimé de votre PC lors de la désinstallation de EcoStruxure Automation Device Maintenance, mais vous devez le supprimer manuellement.

Supprimez-le du dossier *%APPDATA%\Schneider Electric\Automation Device Maintenance* à l'aide de l'Explorateur Windows ou d'autres outils de système de fichiers.

Certificats

Le certificat EcoStruxure Automation Device Maintenance et les **Certificats approuvés** et **Certificats non approuvés** gérés dans la boîte de dialogue **Paramètres**, sous **Sécurité > Gestion des certificats** (voir aussi [Boîte de dialogue Gestion des certificats](#), page 44), sont supprimés sur le PC Windows lors de la désinstallation de EcoStruxure Automation Device Maintenance. Ils sont également supprimés du magasin de certificats Windows.

Packages de données

Les packages de données, page 20 qui ont été enregistrés localement ne sont pas supprimés du PC avec la désinstallation de EcoStruxure Automation Device Maintenance. Par défaut, les packages de données sont stockés dans le dossier *%PUBLIC%\Public Documents\Schneider Electric\Data Packages*. Vous pouvez configurer votre chemin d'accès individuel dans la boîte de dialogue **Paramètres > Paramètres de package**, page 37.

Supprimez manuellement le dossier (par défaut ou configuré) à l'aide de l'Explorateur Windows ou d'autres outils de système de fichiers.

Fichiers de projet EcoStruxure Automation Device Maintenance

Les fichiers de projet EcoStruxure Automation Device Maintenance ne sont pas supprimés de votre PC lors de la désinstallation de EcoStruxure Automation Device Maintenance. Recherchez les fichiers portant l'extension **.emep* et supprimez-les manuellement ou stockez-les en vue d'une utilisation ultérieure dans un endroit sûr où aucun accès non autorisé n'est possible.

Fichiers journaux

Les fichiers journaux qui ont été enregistrés localement dans le chemin indiqué dans la boîte de dialogue **Paramètres > Journaux**, page 38 ne sont pas supprimés du PC lors de la désinstallation de EcoStruxure Automation Device Maintenance. Supprimez le dossier manuellement à l'aide de l'Explorateur Windows ou d'autres outils de système de fichiers ou stockez les fichiers journaux en vue d'une utilisation ultérieure dans un endroit sûr où aucun accès non autorisé n'est possible.


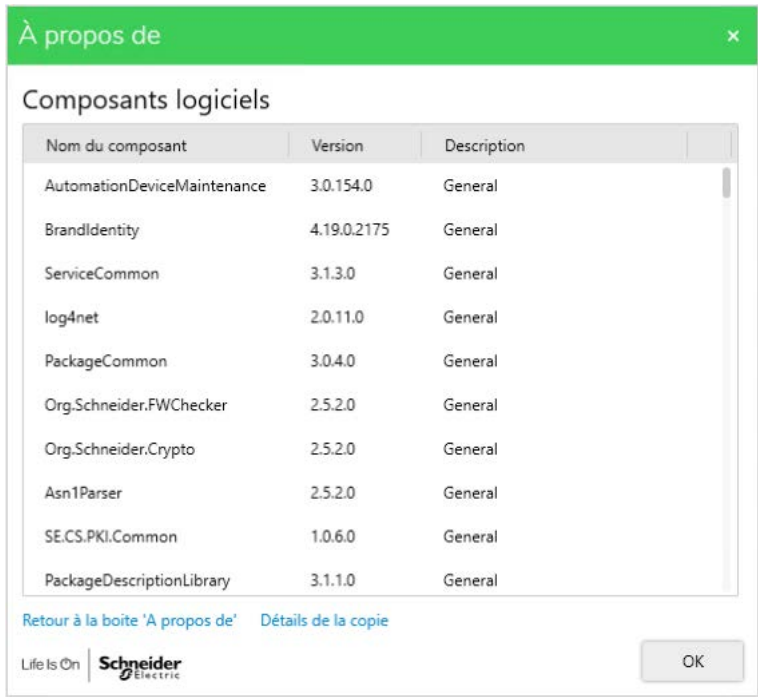
Composants utilisés par EcoStruxure Automation Device Maintenance

Présentation

EcoStruxure Automation Device Maintenance fournit une vue d'ensemble des composants et des versions présentes. Si une exception est détectée, cette liste de composants et de versions peut vous aider à identifier le composant à l'origine du problème.

Extraction d'une liste de composants

Pour extraire une liste des composants chargés par EcoStruxure Automation Device Maintenance, procédez comme suit :

Étape	Action
1	<p>Cliquez sur le bouton À propos  dans la barre d'outils.</p> <p>Résultat : La boîte de dialogue À propos s'ouvre.</p>
2	<p>Cliquez sur le lien Composants logiciels.</p> <p>Résultat : La boîte de dialogue Composants logiciels s'ouvre.</p> 
3	<p>Cliquez sur le lien Détails de la copie pour copier la liste des composants et des versions dans le presse-papiers.</p> <p>Vous pouvez alors coller le contenu dans un fichier *.txt où vous pourrez facilement effectuer des opérations de recherche sur des composants spécifiques et les versions correspondantes.</p>

Glossaire

A

Adresse IP:

Adresse d'un équipement selon les spécifications du protocole IP. L'adresse peut être au format IPv4 ou IPv6.

C

Certificat de l'équipement:

Certificat de clé publique X.509 utilisé par l'outil et l'équipement pour établir une voie de communication sécurisée (par exemple : HTTPs).

D

Découverte d'équipements:

Détection d'équipements et services proposés par ces équipements sur un réseau informatique.

DHCP: Dynamic Host Configuration Protocol.

DNS: Abréviation de Domain Name System.

DPWS:

Profil d'équipement pour les services Web, spécification standard pour la découverte et la description des équipements prenant en charge les services web.

F

Famille d'équipements:

Groupe d'équipements de types similaires, chaque famille d'équipements est identifiée par un ID de produit.

H

HTTP:

Hypertext Transfer Protocol (protocole de transfert hypertexte)

HTTPs:

Hypertext Transfer Protocol Secure (protocole de transfert hypertextuel sécurisé) également appelé HTTP sur TLS.

I

ICS: Acronyme de Industrial Control and Systems

ID produit:

Identification du produit et de la famille de produits à laquelle appartient l'équipement.

IEC:

Acronyme de *International Electrotechnical Commission*, Commission Electrotechnique Internationale (CEI). Organisation internationale non gouvernementale à but non lucratif, qui rédige et publie les normes internationales en matière d'électricité, d'électronique et de domaines connexes.

IP:

Internet Protocol (protocole Internet).

ISO: Organisation internationale de normalisation

N

NEMA:

Acronyme de *National Electrical Manufacturers Association*, Association nationale de fabricants de produits électriques. Norme de performance des différentes classes de boîtiers électriques. Les normes NEMA traitent de la résistance à la corrosion, de la capacité de protection contre la pluie, la submersion, etc. Pour les pays membres de l'IEC (CEI), la norme IEC 60529 classifie le degré de protection contre la pénétration de corps étrangers dans les boîtiers.

O

OPC UA:

Acronyme de « OPC Unified Architecture », architecture unifiée OPC. OPC UA est une norme d'interopérabilité qui régit l'échange sécurisé et fiable de données dans le domaine des automatismes industriels. Il s'agit d'un protocole de communication indépendant des plates-formes qui utilise le modèle serveur/client. La connexion entre le client et le serveur est généralement basée sur le protocole de couche de transport fiable TCP (Transmission Control Protocol).

Pour plus d'informations sur les technologies OPC, en particulier sur la norme OPC UA, consultez le site Web officiel de l'OPC Foundation à l'adresse <https://opcfoundation.org>.

P

Package de données, Package de micrologiciel:

Un package de données est un fichier qui permet l'échange de contenu entre l'outil et les équipements. Il peut être au format SEDP. Un package de données contient le ou les packages du micrologiciel, et il peut contenir également la configuration, les applications des automates, etc.

PLC:

Acronyme de *programmable logic controller*, Logic Controller programmable. Ordinateur industriel utilisé pour automatiser des processus de fabrication et autres processus électromécaniques. Les PLCs diffèrent des ordinateurs courants par le fait qu'ils sont conçus pour utiliser plusieurs tableaux d'entrées et de sorties et pour accepter des conditions de choc, de vibration, de température et d'interférences électriques plus rudes.

POU:

Acronyme de *program organization unit*, unité organisationnelle de programme. Déclaration de variables dans le code source et jeu d'instructions correspondant. Les POU facilitent la réutilisation modulaire de programmes logiciels, de fonctions et de blocs fonction. Une fois déclarées, les POU sont réutilisables.

S

SEDP:

Schneider Electric Data Package, format de fichier standardisé pour l'échange de contenu entre les outils logiciels et les équipements.

T

TCP:

Transmission Control Protocol (protocole de contrôle de transmissions)

TLS:

Transport Layer Security (sécurité de la couche de transport)

U

UDP: User Datagram Protocol.

URL:

Uniform Resource Locator (localisateur uniforme de ressource)

Index

A	
accès aux extensions	64
affichage	21
ajouter un équipement	23
appareils modulaires	64
application des modifications	26
approuver un certificat	43
AutomationDeviceMaintenanceSettings.emes (fichier)	79
Autorité de certification	43
avertissement enregistrer, effacer	26
B	
barre d'outils à propos, aide, découverte	19
boîte de dialogue Connexion équipement	61
boîte de dialogue de connexion	61
Boîte de dialogue Projet modifié	27
bouton Appliquer	26
bouton Copier dans le presse-papiers	54
bouton OK	26
C	
CA	43
carte mémoire SD	21
Centre de mise à jour	68
certificat valider, approuver, désapprouver, supprimer	43
certificat d'équipement approuvé, non approuvé	21
Certificat de l'application	43
certificats	43
communication HTTP/HTTPS	23
communication Modbus TCP	23
composants et versions	80
configuration découverte, Modbus, paramètre de package, langue, certificat	25
emplacements de package	37
langue, changer	40
Modbus TCP	34
paramètres de communication	37
scrutateur DPWS	36
configuration système requise matériel, logiciel, protocoles de communication, résolution d'écran, cybersécurité	16
configurer découverte	32
Confirmation de mise à jour (boîte de dialogue)	69
connexion pour la mise à jour du micrologiciel	69
copie de l'identifiant	54
cybersécurité	74
bureau à distance	77
cartes d'interface réseau	76
certifications	74
connexion au réseau local	77
consignes	76
introduction	74
LANMAN / NTLM	78
pare-feu	77
D	
découverte automatique, manuelle	32
manuelle, automatique	25
découverte d'équipements Modbus, DPWS (profil d'équipement pour les services Web)	15
désapprouver un certificat	43
désinstallation	79
DLL non approuvée	78
données micrologiciel, configuration	52
E	
écran de bienvenue package de données, équipement/chargement, barre d'outils	18
emplacement de package ajouter	38
équipement mise à jour, options de configuration, identifiants	61
équipement/chargement nom d'équipement, état, package de données	21
équipements pris en charge	15
erreur enregistrer, effacer	26
erreur, avertissement	19
exception	78
extensions	64
F	
fichier csv pour importation	34
fichier de configuration de la sécurité	41, 71
fichier de configuration, importation	34
fichiers de package fwp	51
fichiers de package ldx	51
fichiers de package sécurisés sedps	51
fichiers de package sedp	51
fichiers de package sedps	51
fichiers de projet avec équipements non identifiés	31
fichiers de projet provenant d'un autre ordinateur	30
Firmware (boîte de dialogue)	69
fonctions de sécurité	41
fréquence d'interrogation	37
G	
Gestion du certificat	43
Groupe , option	56
I	
icône d'actualisation	26
identifiant copie	54
identifiants	25, 61, 69
importation d'un fichier de configuration	34
importation de fichier csv	34
Importer le fichier de configuration de la sécurité	41
information enregistrer, effacer	26
informations	

package, produit	52
informations sur les composants	80
Infrastructure à clé publique (PKI)	48
inscrire un certificat d'application	43
installation	
procédure, assistant d'installation, installation,	
contrat de licence	17
interrogation, fréquence	37

J

journaux	
affichage	68

L

logiciel	
fonctionnalités, packages de micrologiciel pris en	
charge	15

M

matériel	
UC, RAM, disque dur	16
messages de confirmation	67
messages de notification	67
micrologiciel	
mise à jour, équipement/chargement, package de	
données	69
version, informations de mise à niveau,	
avancement	21
mise à jour du fichier de configuration de la	
sécurité	71
mise à jour du micrologiciel	69
Modbus TCP	
ID unité, temporisation ping, port	34
modifications dans la page Paramètres	26
modules en rack	64
mots de passe	61, 69

N

non approuvée, DLL	78
nouveau projet	27

O

onglet Equipement/Chargement	55
Onglet Extensions	64

P

package de données	51
nom du package, informations sur le package	20
package de données rejeté	52
package de données valide	52
package de micrologiciel	
informations sur le package, nom de package	18
PKI	48
projet	
enregistrer	28
nouveau	27
ouvrir	29
ouvrir, enregistrer	19
protocoles de communication	16

R

Référentiel local	37
regroupement d'équipements	56
réinitialisation des paramètres d'application	40
Résumé de la mise à jour (boîte de dialogue)	69
retirer un certificat	43

S

scrutateur DPWS	
demande de détection, demande de métadonnées,	
adaptateurs réseau	36
statut de la découverte d'équipements	66
suppression de fichiers	79
supprimer un certificat	43
surveillance du statut de la découverte	
d'équipements	66
syslog	49

T

TCP	49
temporisation	
paramètres de communication	37
TLS	49

U

UDP	49
-----------	----

Z

zone de notification	67
----------------------------	----

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Les normes, spécifications et conceptions pouvant changer de temps à autre, veuillez demander la confirmation des informations figurant dans cette publication.

© 2022 Schneider Electric. Tous droits réservés.

EIO0000004048.04