



EcoStruxure Panel Server

Guide de cybersécurité

Concentrateur d'appareils sans fil et passerelle Modbus, enregistreur de données et serveur d'énergie

EcoStruxure propose une architecture et une plateforme compatible IdO

DOCA0211FR-14
01/2026



Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document 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 document 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 document 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 document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, 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.

Table des matières

Consignes de sécurité.....	5
À propos du document	6
Introduction à la cybersécurité.....	9
Caractéristiques de l'équipement.....	10
Recommandations de cybersécurité	12
Fonctions de l'appareil	14
Sécurité du réseau.....	16
Sécurité des applications cloud	19
Sécurité physique de l'équipement	20
Recommandations de sécurité pour la maintenance	22
Glossaire	25

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.

À propos du document

Portée de ce document

Ce guide fournit des informations sur la cybersécurité de EcoStruxure™ Panel Server en vue d'aider les concepteurs et les utilisateurs de système à mettre en place un environnement sécurisé d'exploitation du produit.

Ce guide n'aborde pas la question générique de la sécurisation de votre réseau de technologie opérationnelle ou de votre réseau Ethernet d'entreprise. Pour une présentation générale des menaces de cybersécurité et des moyens de protection disponibles, reportez-vous aux Informations générales sur la cybersécurité, page 6.

NOTE: Dans ce guide, le terme **sécurité** fait référence à la cybersécurité.

Note de validité

Les informations contenues dans ce document sont pertinentes pour EcoStruxure Panel Server avec le micrologiciel de version 002.005.000 ou supérieure.

Informations en ligne

Les informations indiquées dans ce guide peuvent être mises à jour à tout moment. Schneider Electric recommande de disposer en permanence de la version la plus récente, disponible sur le site www.se.com/ww/en/download.

Les caractéristiques techniques des équipements décrits dans ce guide sont également fournies en ligne. Pour accéder aux informations en ligne, accédez à la page d'accueil Schneider Electric à l'adresse www.se.com.

Informations relatives à la cybersécurité générale

Ces dernières années, le nombre croissant de machines en réseau et d'usines de production a entraîné une augmentation correspondante du potentiel de cybermenaces, telles que les accès non autorisés, les violations de données et les perturbations opérationnelles. Vous devez donc envisager toutes les mesures de cybersécurité possibles pour protéger les ressources et les systèmes contre de telles menaces.

Pour garantir la sécurité et la protection de vos produits Schneider Electric, il est dans votre intérêt d'appliquer les meilleures pratiques relatives à la cybersécurité telles que décrites dans le document *Cybersecurity Best Practices*.

Schneider Electric fournit des informations supplémentaires et une assistance :

- Abonnez-vous à la *newsletter* sur la sécurité de Schneider Electric.
- Consultez la page Web *Cybersecurity Support Portal* pour :
 - obtenir des notifications de sécurité.
 - signaler les vulnérabilités et incidents.
- Consultez la page Web *Schneider Electric Cybersecurity and Data Protection Posture* pour :
 - accéder à la position sur la cybersécurité.
 - en savoir plus sur la cybersécurité dans l'académie de cybersécurité.
 - découvrir les services de cybersécurité de Schneider Electric.

Informations de cybersécurité liées au produit

⚠ AVERTISSEMENT

RISQUES POUVANT AFFECTER LA DISPONIBILITÉ, L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DU SYSTÈME

- Désactivez les ports/services inutilisés pour réduire le risque d'attaques malveillantes.
- Protégez les équipements en réseau par plusieurs niveaux de cyberdéfense (pare-feu, segmentation du réseau, détection des intrusions et protection du réseau).
- Respectez les pratiques recommandées en matière de cybersécurité (par exemple : moindre privilège, séparation des tâches) pour réduire les risques d'intrusion, la perte ou l'altération des données et journaux, ou l'interruption des services.

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

Langues disponibles du document

Ce document est disponible dans les langues suivantes :

- Anglais (DOCA0211EN) langue d'origine
- Français (DOCA0211FR)
- Allemand (DOCA0211DE)
- Italien (DOCA0211IT)
- Portugais (DOCA0211PT)
- Espagnol (DOCA0211ES)

Documents connexes à consulter

Titre du document	Numéro de référence
<i>EcoStruxure Panel Server - Guide utilisateur</i>	DOCA0172EN DOCA0172DE DOCA0172ES DOCA0172FR DOCA0172IT DOCA0172PT
<i>Bonnes pratiques de cybersécurité</i>	7EN52-0390
<i>EcoStruxure Power - Guide for Designing and Implementing a Cyber Secure Digital Power System - Technical Guide</i>	ESXP2TG003EN

Vous pouvez télécharger ces publications ainsi que d'autres informations techniques depuis notre site Web à l'adresse www.se.com/ww/en/download/.

Informations concernant la terminologie inclusive/sensible

Schneider Electric s'efforce de mettre constamment à jour ses communications et ses produits pour respecter ses engagements en matière de terminologie inclusive/sensible. Il se peut malgré tout que nos contenus présentent encore des termes jugés inappropriés par certains clients.

Les marques

QR Code est une marque déposée de DENSO WAVE INCORPORATED au Japon et dans d'autres pays.

Introduction à la cybersécurité

Gamme principale EcoStruxure

EcoStruxure est une architecture et une plateforme interopérable de Schneider Electric ouverte, plug-and-play et compatible IdO destinée aux foyers, bâtiments, centres de données, infrastructures et industries. L'innovation à tous les niveaux, des produits connectés au contrôle périphérique, en passant par les applications, les analyses et les services.

Introduction

La cybersécurité vise à protéger votre réseau de communication et tous les équipements qui y sont connectés, contre les attaques susceptibles de perturber les opérations (disponibilité), de modifier des informations (intégrité) ou de divulguer des informations confidentielles (confidentialité). Son objectif consiste à augmenter les niveaux de protection des informations et des actifs physiques contre le vol, la corruption, l'utilisation abusive ou les accidents, tout en maintenant l'accès pour les utilisateurs cibles. La cybersécurité revêt de nombreux aspects, comme la conception de systèmes sécurisés, la restriction de l'accès à l'aide d'outils physiques et numériques, l'identification des utilisateurs, ainsi que la mise en œuvre de procédures de sécurité et de bonnes pratiques.

Consignes Schneider Electric

En plus des recommandations fournies dans ce guide qui concernent spécifiquement Panel Server, vous devez adopter l'approche de défense en profondeur de Schneider Electric en matière de cybersécurité et appliquer les informations générales sur la cybersécurité, page 6.

Politiques et règles de cybersécurité Schneider Electric

Schneider Electric suit un processus de cycle de développement sécurisé (SDL, Secure Development Lifecycle), un cadre de développement essentiel qui assure que les produits respectent des processus de conception sécurisés à toutes les étapes de leur cycle de vie. Le processus SDL de Schneider Electric est conforme à la norme IEC 62443-4-1.

Le processus SDL inclut les éléments suivants :

- Pratiques SDL appliquées au développement interne tout au long de la chaîne logistique.
- Examen de sécurité final obligatoire avant le lancement des produits.
- Formation en sécurité du personnel participant au développement des produits.

Caractéristiques de l'équipement

Présentation

EcoStruxure Panel Server est équipé de fonctions de sécurité. Ces fonctions sont prédéfinies et peuvent être modifiées selon les besoins de votre installation. Panel Server doit être configuré par du personnel qualifié, car la désactivation ou la modification de paramètres affecte la sécurité globale de Panel Server et de votre réseau.

Ce guide est à utiliser en conjonction avec le document DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7 qui décrit en détail la configuration des fonctions et paramètres de Panel Server.

Interfaces de EcoStruxure Panel Server

Le tableau suivant récapitule les architectures de communication disponibles avec Panel Server, par modèle :

Caractéristique		EcoStruxure Panel Server														
		Entry	Universal								Advanced					
		PAS400	PAS600 HW : V1.0	PAS600 HW : V2.0	PAS600T HW : V1.0	PAS600L HW : V1.0	PAS600L HW : V2.0	PAS600LWD HW : V2.0	PAS600PWD HW : V2.0	PAS800 HW : V1.0	PAS800 HW : V2.0	PAS800L HW : V1.0	PAS800L HW : V2.0	PAS800P HW : V1.0	PAS800P HW : V2.0	
Ethernet 10/100BASE-T	Un port RJ45	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	
	Deux ports RJ45	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Connectivité Modbus TCP/IP en amont		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Connectivité Wi-Fi en amont		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Connectivité Modbus TCP/IP en aval		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Connectivité IEEE 802.15.4 en aval		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Connectivité Modbus-SL en aval		-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Deux entrées numériques (pour WAGES (eau, air, gaz, électricité, vapeur))		-	-	-	-	✓	✓	✓	-	-	-	✓	✓	-	-	
Antenne externe Wi-Fi		-	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Antenne externe IEEE 802.15.4		-	-	✓	-	-	✓	-	-	✓	✓	✓	✓	✓	✓	
Point d'accès Wi-Fi		✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	
Notification des alarmes par email		-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓	
Publication sur un serveur SFTP ou HTTPS		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Convention

EcoStruxure Panel Server est désigné ci-après sous le nom Panel Server.

Protocoles pris en charge

EcoStruxure Panel Server prend en charge les protocoles suivants :

- DHCP pour l'adressage IP du réseau
- DNS pour la résolution de nom réseau
- DPWS pour la détection réseau
- HTTPS (TLS v1.2) pour la configuration via les outils de configuration et les pages Web intégrées
- IEEE 802.15.4 pour la communication sans fil utilisant la bande ISM de radiofréquences 2,4 GHz (non disponible pour les modèles Wired by Design)
- Modbus TCP et Modbus-SL pour les communications avec d'autres équipements de technologie opérationnelle (OT)
- NTP pour la synchronisation horaire
- RSTP pour autoriser des topologies en anneau Ethernet robustes pour les applications critiques
- SFTP pour la publication de fichiers CSV sur un serveur SFTP
- Client VPN pour l'accès à distance (ouvert sur le Centre de Contact Client Schneider Electric)
- WPA2 et WPA pour la communication Wi-Fi (non disponible pour les modèles Wired by Design)

Fonctionnalités de sécurité

EcoStruxure Panel Server prend en charge les fonctions de sécurité suivantes :

- Seul un micrologiciel signé numériquement par Schneider Electric peut être installé sur Panel Server.
- Lors de chaque démarrage, la signature numérique est validée avant l'exécution du micrologiciel pour confirmer que son intégrité n'a pas été altérée.
- Les mots de passe utilisateur sont stockés sous une forme hachée et salée (SHA256).
- Vous pouvez effacer toutes les informations de Panel Server à l'aide du bouton Redémarrer.
- L'équipement est doté d'une horloge interne et mémorise la date et l'heure pendant plusieurs mois hors tension.
- La clé d'authenticité de Panel Server est stockée sur une puce Common Criteria haute sécurité CC EAL6+.

Recommandations de cybersécurité

Votre appareil est conçu pour être utilisé dans un environnement protégé qui met en œuvre une stratégie de défense en profondeur.

Pour sécuriser votre appareil, vous devez prendre des mesures spécifiques à chaque étape du cycle de vie du projet.

NOTE: Les recommandations décrites ci-dessous ne constituent pas une liste exhaustive des mesures de cybersécurité possibles. Il s'agit d'un point de départ pour améliorer la sécurité de votre appareil dans un environnement protégé. Consultez des experts en cybersécurité pour planifier, configurer, exploiter, maintenir et mettre hors service votre appareil en fonction de vos besoins.

Le tableau suivant énumère les actions que nous vous recommandons d'effectuer pour sécuriser votre appareil dans un environnement protégé, à chaque phase du cycle de vie :

Phase du cycle de vie	Action recommandée	Actions de défense en profondeur
Planification	Sensibilisation à la cybersécurité, page 6.	Utilisez les ressources disponibles pour accroître vos connaissances en matière de cybersécurité.
	Examinez les considérations relatives à la défense en profondeur des systèmes. Suivez les recommandations de ce guide.	Prenez connaissance des mesures de sécurité qui sont attendues de l'environnement externe dans lequel l'appareil va être utilisé. Il s'agit notamment (mais pas seulement) des aspects suivants : • Sécurité du site et de l'emplacement des appareils • Sécurité du réseau
	Examinez les fonctionnalités de sécurité des appareils. Voir <i>Fonctionnalités de sécurité</i> dans DOCA0172**, Guide utilisateur de Panel Server, page 7.	Comprenez comment les fonctionnalités de sécurité des appareils peuvent être utilisées dans un environnement protégé.
	Examinez les risques liés à la sécurité et les solutions de contrôle disponibles. Voir <i>Fonctionnalités de sécurité</i> dans DOCA0172**, Guide utilisateur de Panel Server, page 7.	Comprenez les risques de sécurité connus et les contrôles permettant de les réduire.
Installation et configuration	Vérifiez l'état de l'étiquette anti-falsification avant d'installer l'appareil, page 20.	Une étiquette inviolable empêche toute modification de l'appareil avant son installation.
	Suivez scrupuleusement les instructions d'installation, page 20.	Contribue à réduire les risques d'accès physique non autorisé.
	Modifiez le mot de passe par défaut lors de la première connexion. Voir <i>Gestion des utilisateurs</i> dans DOCA0172**, Guide utilisateur de Panel Server, page 7.	Contribue à réduire les risques d'accès non autorisé. Les paramètres par défaut de compte utilisateur sont souvent à l'origine de l'accès non autorisé d'utilisateurs malveillants.
	Modifiez le mot de passe d'utilisateur de Panel Server et le mot de passe de point d'accès Wi-Fi. Voir <i>Gestion des utilisateurs et Point d'accès Wi-Fi</i> dans DOCA0172**, Guide utilisateur de Panel Server, page 7.	Créez des mots de passe forts en respectant les instructions. Les paramètres par défaut de compte utilisateur et les mots de passe faibles sont souvent à l'origine de l'accès non autorisé d'utilisateurs malveillants.
	Désactivez les protocoles et les ports non utilisés, page 14.	Désactivez les protocoles et ports de communication inutiles et inutilisés, par exemple : Wi-Fi, point d'accès Wi-Fi, IEEE.802.15.4.
Exploitation	Cryptez les fichiers de sauvegarde de configuration, page 20.	Utilisez des mots de passe forts pour crypter les fichiers de sauvegarde de configuration. Les fichiers non protégés et les mots de passe faibles peuvent favoriser l'accès non autorisé d'utilisateurs malveillants.
	Gérez l'accès aux domaines, page 19.	Limitez l'accès aux domaines connus et requis, en fonction de vos besoins.
	Signalez tout incident ou vulnérabilité de cybersécurité, page 6.	Signalez toute activité suspecte, tout incident de cybersécurité ou toute vulnérabilité sur la page Web Cybersecurity Support Portal de Schneider Electric.
Maintenance	Maintenez le micrologiciel à jour. Voir <i>Mise à jour du micrologiciel</i> dans	Mettez à jour votre micrologiciel vers la plus récente version pour bénéficier des derniers correctifs de sécurité.

Phase du cycle de vie	Action recommandée	Actions de défense en profondeur
	DOCA0172**, Guide utilisateur de Panel Server, page 7.	
	Surveillez le journal d'audit pour détecter tout comportement inattendu. Voir <i>Journaux de diagnostic</i> dans DOCA0172**, Guide utilisateur de Panel Server, page 7.	Surveillez les journaux d'audit pour détecter toute activité inattendue et pour identifier la cause des violations de cybersécurité qui pourraient conduire à un incident de cybersécurité.
	Vérifiez régulièrement l'état de l'étiquette anti-falsification, page 20.	Une étiquette inviolable empêche toute modification de l'appareil.
	Vérifiez qu'il n'existe pas d'appareils inconnus parmi les appareils connectés, page 18.	Localisez et supprimez les appareils inconnus afin de protéger le système contre les violations de cybersécurité.
	Maintenez la sécurité de votre réseau à jour.	Contribue à réduire votre surface d'attaque et à limiter le risque de vulnérabilité.
	Effectuer des audits de sécurité	Permet de vérifier l'état de sécurité de votre système.
Mise hors service	Restaurer les réglages d'usine de l'appareil. Voir <i>Recommandations de sécurité pour la mise hors service</i> dans DOCA0172**, Guide utilisateur de Panel Server, page 7.	Contribue à prévenir les fuites de données.

Fonctions de l'appareil

Mise à jour du firmware

Mettez à jour l'EcoStruxure Panel Server vers la dernière version du firmware pour bénéficier des fonctions et correctifs de sécurité les plus récents. Afin d'assurer l'intégrité et l'authenticité du firmware exécuté sur l'EcoStruxure Panel Server, tous les firmwares conçus pour l'EcoStruxure Panel Server sont signés à l'aide de l'infrastructure de clé publique (PKI) Schneider Electric. Pour que l'infrastructure PKI fonctionne correctement, la date de l'appareil doit être synchronisée (consultez la section [Date et heure](#), page 14).

Pour être tenu informé des mises à jour de sécurité, demandez à recevoir les notifications de sécurité (*Security Notifications*) sur le portail d'assistance à la cybersécurité de Schneider Electric.

Date et heure

Il est important de synchroniser la date et l'heure pour les raisons suivantes :

- Pour éviter les erreurs dans les certificats et les signatures numériques dans le EcoStruxure Panel Server
- Pour fournir un horodatage exact dans les journaux d'audit et favoriser ainsi la sécurité des analyses

Pour plus d'informations sur la date et l'heure, consultez la documentation DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

Désactivation des fonctions inutilisées

L'EcoStruxure Panel Server vous permet de désactiver les ports et services inutilisés pour réduire le risque d'attaques malveillantes.

Il est recommandé de désactiver les éléments suivants :

- Activation Wi-Fi et infrastructure Wi-Fi. Le Wi-Fi peut être désactivé de façon permanente si nécessaire.
- Point d'accès Wi-Fi (activé par défaut). Lorsque le point d'accès est désactivé, le bouton situé sur la face avant du Panel Server ne permet pas de déclencher l'activation du point d'accès. La désactivation de l'activation Wi-Fi désactive également le point d'accès Wi-Fi et interrompt toute connexion active.
- IEEE 802.15.4 (par défaut non actif). Le protocole IEEE 802.15.4 peut être désactivé de façon permanente.
- Services de passerelle Modbus (actifs par défaut). Peuvent être désactivés sur chaque interface (Ethernet 1, Ethernet 2 et/ou Wi-Fi) dans les pages Web du Panel Server.
- DPWS (protocole de découverte sur IP v4/6) (actif par défaut)
- RSTP (Rapid Spanning Tree Protocol) (par défaut non actif)

NOTE: Wi-Fi et IEEE 802.15.4 ne sont pas disponibles en mode natif sur les modèles Wired by Design (WD), lesquels ne disposent pas de chipset sans fil.

Pour plus d'informations sur la désactivation des fonctions inutilisées de l'EcoStruxure Panel Server, consultez le document DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

Ports TCP

Les ports TCP suivants sont utilisés dans le produit EcoStruxure Panel Server:

- Port 443 : HTTPS
- Port 502 : Modbus
- Port 5357 : DPWS (peut être modifié)

NOTE: Panel Server n'intègre aucun serveur SSH.

Journaux d'audit

L'EcoStruxure Panel Server génère des journaux d'audit qui enregistrent divers événements, comme les tentatives de connexion non valides et les mises à jour du firmware.

Les journaux ne contiennent aucune information personnelle.

Pour détecter des comportements inattendus (tels que des redémarrages fréquents, une mise à jour incorrecte du firmware ou des tentatives de connexion non valides), il est recommandé de surveiller régulièrement les journaux d'audit. Pour plus d'informations sur les journaux de diagnostic, consultez DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

Mise au rebut de l'appareil

L'EcoStruxure Panel Server contient des informations confidentielles configurées pendant la mise en service, ainsi que des valeurs de données récentes et des journaux. Ces informations concernent notamment la topologie d'appareils Modbus, les réseaux sans fil, les mots de passe Wi-Fi ou les consommations d'énergie mesurées.

Rétablissez les paramètres d'usine avant de mettre l'EcoStruxure Panel Server au rebut. Vous devez pouvoir redémarrer physiquement l'EcoStruxure Panel Server durant cette procédure. Pour rétablir les paramètres d'usine de l'EcoStruxure Panel Server, consultez la documentation DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

Sécurité du réseau

Introduction

EcoStruxure Panel Server n'est pas conçu pour être directement exposé au réseau Internet public. Il doit être protégé avec la méthode NAT (Network Address Translation) au minimum ou, de préférence, par plusieurs pare-feu. Consultez les sites Web suivants pour en savoir plus :

- Services de conseil en cybersécurité Schneider Electric
- National Institute of Standards and Technology (NIST)
- Agence européenne de la cyber-sécurité (ENISA)

Segmentation réseau

EcoStruxure Panel Server est une passerelle. Il crée un pont entre différents réseaux. La segmentation du réseau permet d'assurer la cybersécurité. Pour améliorer la segmentation du réseau, Panel Server Universal et Advanced disposent de deux ports Ethernet. Ils peuvent être exploités séparément, avec un port dédié aux technologies de l'information (IT) et un port dédié aux technologies opérationnelles (OT). La segmentation du réseau vous permet de maintenir la segmentation des réseaux OT et IT, car les paquets réseau ne sont pas transmis d'un côté à l'autre.

Il est recommandé de configurer le réseau en mode segmenté (pour plus d'informations sur les paramètres réseau, reportez-vous à DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7).

Vous pouvez ainsi connecter Panel Server à :

- Des équipements OT en aval via Modbus TCP sur un port Ethernet.
- Des PC IT en amont avec SCADA et applications logicielles de mise en service sur l'autre port Ethernet.

HTTPS et Modbus sont disponibles sur les interfaces Ethernet de Panel Server (ETH1, ETH2) et le Wi-Fi.

Le tableau suivant présente la configuration par défaut pour chaque interface :

Interface		Modbus
Ethernet en topologie commutée		Activé
Ethernet en topologie séparée	Port ETH1	Activé
	Port ETH2	Désactivé
Infrastructure Wi-Fi		Désactivé
Point d'accès Wi-Fi		Non disponible

Il est recommandé de désactiver le service Modbus sur les réseaux où il n'est pas utilisé. Pour plus d'informations sur l'activation des services, reportez-vous à DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

Certificat de serveur Web du produit

Pour prendre en charge les communications sécurisées HTTPS, EcoStruxure Panel Server est équipé d'un certificat X.509v3 par défaut. Ce certificat assure l'intégrité et la confidentialité des communications HTTPS.

Les navigateurs Web reconnaissent seulement les certificats destinés à des sites publics. Comme Panel Server est installé sur un réseau local (LAN), ils ne

peuvent pas faire la distinction entre deux Panel Servers. C'est pourquoi un message de sécurité s'affiche dans le navigateur Web lors de la connexion à Panel Server.

Une connexion câblée directe permet de sécuriser le chemin de communication avec Panel Server. Pour plus d'informations sur le premier accès aux pages Web EcoStruxure Panel Server via un PC, reportez-vous à DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

Empreinte de la clé du serveur SFTP

Si vous publiez vos données sur un serveur SFTP, assurez-vous que l'empreinte de la clé qui s'affiche lors de la configuration de l'adresse du serveur, correspond à la clé SFTP de votre serveur.

Si vous renouvelez la clé SFTP sur votre serveur, Panel Server ne pourra plus envoyer les fichiers, car la connexion ne sera pas authentifiée. Vous devrez reconfigurer la publication pour que Panel Server enregistre la nouvelle empreinte de clé SFTP.

Réseau sans fil

Les protocoles radio sont vulnérables aux attaques physiques. Lors d'une attaque par refus de service, par exemple, le signal radio peut être brouillé grâce à un émetteur puissant situé à proximité.

Par conséquent, il est recommandé d'adapter la sécurité physique du système en fonction du niveau de criticité des informations qui dépendent de protocoles radio. Pour cela, les réseaux sans fil (Wi-Fi et IEEE 802.15.4) peuvent être désactivés de façon permanente dans Panel Server. Si vous êtes sûr de ne jamais avoir besoin de réseaux sans fil (Wi-Fi et IEEE 802.15.4), et dans ce cas uniquement, vous pouvez les désactiver définitivement. Pour plus d'informations sur la désactivation définitive et simultanée des réseaux sans fil, reportez-vous à DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7.

NOTE: Les modèles Wired by Design (WD) de Panel Server permettent la conformité aux stratégies excluant le sans-fil puisqu'ils ne contiennent pas de chipset sans fil.

Recommandations :

- Utilisez le code d'installation pour détecter les équipements sans fil. Pour plus d'informations, reportez-vous à DOCA0172** *EcoStruxure Panel Server - Guide utilisateur*, page 7
- Procédez à la mise en service d'équipements sans fil IEEE 802.15.4 dans un endroit sécurisé contre les émetteurs radio non fiables, comme une salle d'administrateur.

Pour le réseau Wi-Fi, il est recommandé d'utiliser WPA2 (Wi-Fi Protected Access version 2).

NOTE: Le protocole TKIP (Temporal Key Integrity Protocol) n'est pas pris en charge.

Accès à distance (VPN)

Panel Server fournit une fonction d'accès à distance qui permet au Centre de contact client (CCC) de Schneider Electric de se connecter aux pages Web de Panel Server.

L'accès n'est pas activé par défaut et nécessite que le pare-feu active la connexion. Pour plus d'informations, reportez-vous à Points de terminaison attendus, page 19.

La fonction d'accès à distance s'appuie sur un VPN de couche 3 qui, par conception, ne fournit pas l'accès au réseau mais seulement à Panel Server. En outre, seul le protocole HTTPS est autorisé à être tunnelisé via ce VPN.

Équipements connectés

Il est recommandé de vérifier régulièrement la liste des équipements connectés au réseau IEEE 802.15.4 de Panel Server. Si la liste contient un équipement connecté inconnu, localisez-le et supprimez-le. Vous pouvez aussi recréer le réseau et ne reconnecter que les équipements identifiés.

Sécurité des applications cloud

Sécurité des données en mouvement

Les applications cloud EcoStruxure de Schneider Electric mettent en oeuvre les pratiques recommandées suivantes :

- Toutes les communications vers et depuis EcoStruxure Panel Server avec des systèmes Schneider Electric internes ou des systèmes tiers externes sont cryptées à l'aide du protocole HTTPS (le niveau minimum requis est TLS 1.2).
- Les certificats impliqués dans ces sessions cryptées utilisent l'algorithme de hachage sécurisé SHA 256. Cela s'applique aux communications entre application Panel Server et serveurs de plateformes cloud Microsoft Azure.

Sécurité des données au repos

Schneider Electric suit les pratiques recommandées pour créer des solutions sécurisées et limiter le risque de compromission importante des données tout en protégeant la confidentialité, le contrôle et l'autonomie des données de chaque client individuellement.

Tous les identifiants et jetons de système à système sont stockés et cryptés dans les plateformes cloud Microsoft Azure.

Points de terminaison attendus

Schneider Electric recommande de n'autoriser l'accès qu'aux domaines absolument nécessaires.

Le tableau suivant répertorie les noms de domaine et les protocoles utilisés lorsque le Panel Server se connecte au cloud.

Nom de domaine	Protocole	Description
cbBootStrap.gl.StruXureWareCloud.com	HTTPS (port TCP 443)	Utilisé lors de la première connexion de Panel Server au cloud (ou après une restauration des paramètres d'usine) pour authentifier et enregistrer le Panel Server.
etp.prod.StruXureWareCloud.com	HTTPS (port TCP 443)	Permet de télécharger une mise à jour de firmware.
cnm-ih-na.Azure-devices.net	HTTPS (port TCP 443)	Utilisé pour la communication de Panel Server avec les services cloud de Schneider Electric tels que la configuration, les données ou les alarmes.
RemoteShell.rsp.Schneider-Electric.com	HTTPS (port TCP 443)	Permet au centre de contact client de Schneider Electric d'accéder à distance aux pages Web de votre Panel Server via le VPN.
cnmdapiappstna.Blob.Core.Windows.net	HTTPS (port TCP 443)	Permet à Panel Server de télécharger des journaux et des fichiers de diagnostic sur demande du centre de contact client de Schneider Electric.
cnmiothubappstna.Blob.Core.Windows.net/file-upload	HTTPS (port TCP 443)	Permet à Panel Server de télécharger une topologie vers les services cloud de Schneider Electric.
time.gl.StruXureWareCloud.com	NTP (port UDP 123)	Le serveur NTP permet à l'horloge du Panel Server de rester synchronisée.

NOTE: Les noms de domaine ne sont pas sensibles à la casse.

Sécurité physique de l'équipement

Étiquette de garantie

EcoStruxure Panel Server dispose d'une étiquette de garantie qui assure la sécurité physique de l'équipement. Elle doit être propre et ne présenter aucun signe d'altération (comme des accrocs, des déchirures ou des rayures). Schneider Electric déconseille d'utiliser un équipement dont l'intégrité physique a été visiblement altérée.

Installation

Afin d'assurer la sécurité physique de l'équipement, il est recommandé d'effectuer l'installation suivante :

- Installez EcoStruxure Panel Server dans une armoire protégée de manière appropriée en fonction du niveau de risque de votre installation (un cadenas ou une clé, par exemple).
- Si EcoStruxure Panel Server est monté dans un tableau de distribution, installez ce dernier dans une pièce sécurisée (par une porte verrouillée ou une caméra, par exemple).

NOTE: La sécurité physique de l'équipement inclut la protection du code QR. Le code QR donne accès au code d'équipement de Panel Server, lequel doit être considéré comme une information d'identification confidentielle de l'équipement. Il est utilisé :

- Lors de la revendication sécurisée de l'équipement pour les applications cloud
- Comme mot de passe pour la connexion au point d'accès Wi-Fi

Gestion des mots de passe

Pour protéger l'équipement contre les attaques malveillantes, modifiez le mot de passe utilisateur Panel Server et le mot de passe du point d'accès Wi-Fi via les pages Web Panel Server.

Le mot de passe utilisateur et le mot de passe SupportUser doivent respecter les règles suivantes :

- Entre 8 et 50 caractères
- Doivent contenir au moins trois des types de caractères suivants :
 - Majuscules
 - Minuscules
 - Chiffres
 - Caractères spéciaux (limités à l'espace et !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~)

Le mot de passe du point d'accès Wi-Fi doit respecter les règles suivantes :

- Entre 8 et 32 caractères
- Doit contenir au moins un caractère de chacun des types suivants :
 - Majuscules
 - Minuscules
 - Chiffres
- Peut contenir des caractères spéciaux (limités à l'espace et !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~)

Fonction de sauvegarde

Lors du téléchargement d'un fichier de sauvegarde, cryptez le fichier avec un mot de passe fort, composé des éléments suivants :

- Entre 6 et 32 caractères
- Doit contenir au moins un caractère de chacun des types suivants :
 - Majuscules
 - Minuscules
- Caractères spéciaux (limités à l'espace et !"#\$%&'()*+,-./:;<=>?@[^_`{|}~)

Recommandations de sécurité pour la maintenance

Opérations de maintenance

Il est recommandé de réaliser régulièrement les opérations suivantes pendant toute la durée de vie de l'EcoStruxure Panel Server :

- Vérifier la sécurité physique de l'EcoStruxure Panel Server (consulter la section [Etiquette de garantie](#), page 20)
- S'assurer que le firmware est à jour (vous devez être abonné aux [notifications de sécurité](#), page 14)
- Vérifier qu'il n'existe pas d'appareils inconnus parmi les [appareils connectés](#), page 18
- Consulter les [journaux d'audit](#), page 15 pour identifier d'éventuels comportements inattendus (tentatives de connexion non valides et redémarrages fréquents, par exemple)
- Vérifier la date et l'heure, page 14 pour éviter toute dérive d'horloge
- Vérifier que tous les services et fonctionnalités inutiles sont désactivés, page 14.

Vérification des fonctions de sécurité

Les tests suivants vous permettent de vérifier que les fonctions de sécurité fonctionnent comme prévue via les pages Web EcoStruxure Panel Server.

Authentification Web

1. Essayez de vous connecter aux pages Web d'EcoStruxure Panel Server sans mot de passe ou entrez un mot de passe incorrect.
Résultat : EcoStruxure Panel Server ne vous donne pas accès aux pages Web.
2. Répétez cette action 9 fois de plus.
Résultat : EcoStruxure Panel Server se verrouille pendant 10 minutes.
3. Réessayez encore 5 fois.
Résultat : EcoStruxure Panel Server se verrouille pendant 60 minutes.

Autorisation Web

1. Connectez-vous aux pages Web EcoStruxure Panel Server.
2. Placez un signet sur une page Web (par exemple, **Paramètres**)
3. Ouvrez une fenêtre de navigation privée dans votre navigateur et ouvrez la page Web précédemment marquée d'un signet.
Résultat : Vous ne pouvez pas accéder à la page Web, mais vous êtes redirigé vers la page de connexion.

Historique

1. Après avoir effectué une partie ou l'ensemble des tests précédents, accédez à la page Web des journaux.
2. Téléchargez les fichiers journaux.

3. Vérifiez que les tentatives infructueuses de connexion figurent dans les journaux.

Mise à jour du micrologiciel

1. Accédez à la page Web **Mise à jour du firmware**.
2. Téléchargez un fichier aléatoire (par exemple, une image ou un document texte).
Résultat : EcoStruxure Panel Server signale que la signature est erronée.
3. Accédez aux journaux d'audit.
4. Vérifiez que l'échec de mise à jour du micrologiciel est consigné dans les journaux.

Désactivation des services

1. Pour accéder au menu permettant de désactiver les services, sélectionnez **Paramètres > Communication réseau > DPWS**.
2. Connectez un PC exécutant le système d'exploitation Windows sur le même réseau local.
3. Cliquez sur Réseau dans l'Explorateur de fichiers.

Résultat : EcoStruxure Panel Server n'est pas repéré et n'apparaît donc pas dans la liste des équipements du réseau.

Désactivation des services sans fil

Pour accéder aux menus permettant de désactiver temporairement les services sans fil :

- Pour le Wi-Fi, accédez à **Paramètres > Communication réseau > Wi-Fi**, cliquez sur le curseur **Activation du Wi-Fi** et enregistrez vos modifications.

Résultat : Dans votre interface de gestion de point d'accès WiFi, il n'y a aucun EcoStruxure Panel Server connecté.

- Pour IEEE 802.15.4, accédez à **Paramètres > Appareils sans fil > Configuration réseau**, cliquez sur le curseur **Activation du sans-fil** et enregistrez vos modifications.

Résultat : Tous les appareils sans fil répertoriés dans **Paramètres > Appareils sans fil > Appareils sans fil** présentent un état **Non connecté** au bout d'un certain temps qui dépend de l'appareil sans fil (consultez la documentation de l'appareil pour plus d'informations).

Glossaire

C

Code d'installation:

Code unique de 36 caractères associé à un équipement Modbus, qui vous permet de lancer une détection de l'équipement avec une sécurité renforcée depuis Panel Server.

D

DHCP (Dynamic Host Configuration Protocol):

Protocole de gestion de réseau utilisé sur les réseaux IP (Internet Protocol) pour attribuer automatiquement des adresses IP et d'autres paramètres de communication aux équipements connectés au réseau à l'aide d'une architecture client-serveur.

DPWS - Device Profile for Web Services:

Ensemble minimal de contraintes d'implémentation qui permet d'activer la messagerie, la découverte, la description et les événements de services Web sécurisés sur des équipements limités en ressources.

H

HTTP - Hypertext Transfer Protocol:

Protocole réseau qui gère la distribution des fichiers et données sur le Web.

HTTPS - Hypertext Transfer Protocol Secure:

Variante du protocole de transfert web standard (HTTP) qui ajoute une couche de sécurité sur les données en transit via une connexion par protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security).

I

IEEE 802.15.4:

Norme définie par l'IEEE et utilisée par EcoStruxure Panel Server pour communiquer avec des équipements sans fil.

IP - Internet Protocol:

Les adresses IP servent à identifier les équipements connectés à l'intranet de l'entreprise ou à Internet.

IT - Information Technology, signifiant technologie de l'information:

Désigne le réseau informatique et les systèmes d'information de l'entreprise, par opposition au réseau de technologie opérationnelle (OT).

L

LAN - Local Area Network, signifiant réseau local.:

Désigne l'intranet ou le réseau informatique de l'entreprise.

M

Modbus TCP/IP:

Protocole qui assure la communication client/serveur entre des équipements et TCP/IP, et qui permet les communications sur une connexion Ethernet.

N

NTP (Network Time Protocol):

Protocole réseau conçu pour la synchronisation d'horloge entre systèmes informatiques sur des réseaux de données à commutation de paquets et à temps de latence variable.

O

OT - Operational technology, signifiant technologie opérationnelle.:

Désigne les systèmes matériels et logiciels utilisés par l'entreprise pour surveiller et contrôler directement les processus et équipements de production, également appelés réseau de contrôle industriel (IC). L'abréviation OT est souvent utilisée pour désigner le réseau opérationnel de l'entreprise, par opposition à son réseau informatique.

P

PKI - Public key infrastructure, signifiant infrastructure de clé publique.:

Définit un ensemble de services utilisés pour générer et authentifier des signatures numériques. Une infrastructure de clé publique est conçue pour garantir la confidentialité, l'intégrité et l'authenticité des informations.

R

RSTP (Rapid Spanning Tree Protocol):

Protocole réseau qui favorise la haute disponibilité et la topologie sans boucle dans les réseaux Ethernet.

S

SCADA - Supervisory control and data acquisition:

Désigne les systèmes conçus pour obtenir des données en temps réel sur les processus et équipements de production en vue de les surveiller et de les contrôler à distance.

SDL – Cycle de développement sécurisé:

Cadre de développement de produits qui garantit que les produits suivent des processus de conception sécurisés à toutes les étapes de leur cycle de vie.

SFTP - Secure File Transfer Protocol:

Version sécurisée du protocole de transfert de fichiers (FTP) qui facilite l'accès aux données et le transfert de données via un flux de données SSH (Secure Shell).

Stratégie de sécurité:

Paramètres de sécurité appliqués à l'ensemble du système sécurisé. En général, une stratégie de sécurité renvoie à l'utilisation de normes. Il permet de définir la configuration de sécurité commune à l'ensemble des équipements.

T

TCP/IP - Transmission control protocol/Internet protocol:

Désigne la suite de protocoles utilisés pour les communications sur Internet.

V**VPN - Virtual private network, signifiant réseau privé virtuel.:**

Un VPN permet d'établir un « tunnel » sécurisé/privé entre un point d'accès externe authentifié et le réseau d'entreprise sécurisé.

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.

© 2026 Schneider Electric. Tous droits réservés.

DOCA0211FR-14